Sicurezza delle piattaforme Apple

Maggio 2024

Indice

Introduzione alla sicurezza delle piattaforme Apple

La sicurezza è al centro di tutte le piattaforme di Apple. Facendo affidamento sull'esperienza della creazione del sistema operativo mobile più avanzato al mondo, Apple ha creato delle architetture di sicurezza che soddisfano i requisiti unici di dispositivi mobili, orologi, computer desktop e dispositivi domestici.

Ogni dispositivo Apple unisce *hardware*, *software* e *servizi* progettati per funzionare insieme e offrire la massima sicurezza e un'esperienza utente trasparente. Lo scopo finale principale è quello di mantenere le informazioni personali al sicuro. Ad esempio, i chip e l'hardware di sicurezza progettati da Apple sono alla base di importanti funzionalità di sicurezza. E le protezioni software lavorano assieme per mantenere sicuro il sistema operativo e le app di terze parti. Infine, i servizi forniscono un meccanismo sicuro e affidabile per effettuare gli aggiornamenti software, creano un ecosistema di app protette e consentono comunicazioni e pagamenti semplici e sicuri. Di conseguenza, i dispositivi Apple non proteggono solo il dispositivo e i relativi dati, ma l'intero ecosistema, comprese tutte le operazioni eseguite dagli utenti localmente, sulle reti e con servizi internet essenziali.

I nostri dispositivi sono progettati per essere semplici, intuitivi e funzionali ma al tempo stesso sicuri. Le funzionalità di sicurezza fondamentali, come la codifica del dispositivo basata sull'hardware, non possono essere disabilitate per errore. Altre funzionalità, come ad esempio Face ID e Touch ID, migliorano l'esperienza utente rendendo più semplice e intuitiva la protezione del dispositivo. E poiché molte di queste funzionalità sono abilitate di default, gli utenti o i reparti IT non dovranno eseguire lunghe configurazioni.

Questo documento fornisce informazioni dettagliate su come la tecnologia e le funzionalità relative alla sicurezza sono implementate all'interno delle piattaforme Apple. Aiuta inoltre le organizzazioni a conciliare tecnologia e funzionalità di sicurezza delle piattaforme Apple con le politiche e le procedure adottate, per soddisfare le proprie necessità specifiche in materia di sicurezza.

I contenuti sono organizzati per argomenti:

- **Sicurezza hardware e biometria:** i chip e l'hardware che rappresentano la base della sicurezza dei dispositivi Apple, compreso il chip Apple, Secure Enclave, un motore di crittografia dedicato, Face ID e Touch ID.
- **Sicurezza del sistema:** le funzioni software e hardware integrate che provvedono all'avvio sicuro, agli aggiornamenti e al funzionamento dei sistemi operativi Apple.
- **Codifica e protezione dei dati:** l'architettura e il design volti a proteggere i dati utente se il dispositivo viene smarrito o rubato, oppure se una persona o un processo non autorizzati provano a utilizzarlo o a modificarlo.
- **Sicurezza delle app:** il software e i servizi che forniscono un ecosistema protetto di app e consentono l'esecuzione sicura delle app senza compromettere l'integrità della piattaforma.
- **Sicurezza dei servizi:** i servizi di Apple per l'identificazione, la gestione delle password, i pagamenti, le comunicazioni e il ritrovamento dei dispositivi smarriti.
- **Sicurezza della rete:** protocolli di rete basati sugli standard del settore che forniscono autenticazione e codifica sicure durante la trasmissione dei dati.
- **Sicurezza del kit per sviluppatori:** i framework per la gestione privata e sicura di abitazioni e salute, nonché l'estensione delle funzionalità dei dispositivi e servizi Apple alle app di terze parti.
- **Gestione sicura dei dispositivi:** metodi che consentono la gestione dei dispositivi Apple, aiutano a impedire l'uso non autorizzato e abilitano l'inizializzazione remota del dispositivo in caso di smarrimento o furto.

Il nostro impegno per la sicurezza

Apple si impegna a proteggere i propri clienti con tecnologie evolute per la privacy e la sicurezza progettate per tutelare le informazioni personali, nonché adottando soluzioni a tutto tondo per contribuire a salvaguardare i dati aziendali in un ambiente enterprise. Apple premia i ricercatori per il loro lavoro nell'individuazione di vulnerabilità offrendo il programma di bug bounty sulla sicurezza di Apple. Maggiori dettagli sul programma di bug bounty e sulle categorie di bug sono disponibili all'indirizzo https://security.apple.com/bounty/.

Apple dispone di un team dedicato in grado di offrire assistenza per tutte le problematiche di sicurezza riferite ai prodotti Apple. Il team fornisce test e auditing di sicurezza per prodotti sia in fase di sviluppo che post-release. Fornisce inoltre strumenti di sicurezza e training specifico, oltre a monitorare l'esistenza di minacce e le segnalazioni di nuovi problemi relativi alla sicurezza. Apple fa parte del Forum of Incident Response and Security Teams (FIRST).

Apple continua a migliorarsi costantemente in materia di sicurezza e privacy. Utilizza chip Apple personalizzati su tutta la gamma di prodotti, da Apple Watch a iPhone e iPad, fino al chip di serie M su Mac, che rendono possibile un'elaborazione efficiente, garantendo, al contempo, la sicurezza. Ad esempio, il chip Apple sta alla base di "Avvio sicuro", Face ID, Touch ID, e della protezione dei dati. Inoltre, le funzionalità di sicurezza rese possibili dal chip Apple, come la protezione dell'integrità del kernel, i codici di autenticazione dei puntatori e le restrizioni rapide dei permessi, consentono di fronteggiare i tipi più comuni di attacchi cibernetici. Di conseguenza, anche nel caso in cui il codice di un hacker riuscisse ad essere eseguito, i possibili danni sarebbero comunque radicalmente ridotti.

Consigliamo alle organizzazioni di rivedere le proprie politiche in materia di IT e sicurezza per poter sfruttare al massimo i livelli di tecnologia di protezione offerti dalle nostre piattaforme.

Per maggiori informazioni sul modo in cui segnalare eventuali problemi ad Apple e per iscriverti alle notifiche di sicurezza, consulta Segnalare una vulnerabilità nella sicurezza o nella privacy.

Apple ritiene che la privacy sia un diritto umano fondamentale e mette a disposizione numerosi controlli e opzioni integrati che consentono agli utenti di decidere in che modo e quando le app possono utilizzare le loro informazioni e quali informazioni verranno utilizzate. Per ulteriori informazioni sull'approccio di Apple nei confronti della privacy, sui controlli per la privacy nei dispositivi Apple e sulle politiche Apple per la privacy, vai sul sito: https://www.apple.com/it/privacy**.**

Nota: se non diversamente specificato, questo documento è valido per le seguenti versioni dei sistemi operativi: iOS 17.3, iPadOS 17.3, macOS 14.3, tvOS 17.3 e watchOS 10.3.

Sicurezza hardware e biometria

Panoramica della sicurezza hardware

Perché il software sia sicuro, deve appoggiarsi a un hardware dotato di meccanismi di sicurezza. Per questo motivo, i dispositivi Apple con iOS, iPadOS, macOS, tvOS, e watchOS dispongono di funzionalità di sicurezza integrate direttamente nei componenti fisici. Tra queste ci sono delle funzionalità della CPU che potenziano le funzioni di sicurezza del sistema nonché componenti fisici aggiuntivi dedicati alla sicurezza. Un hardware incentrato sulla sicurezza si basa sul principio di supportare funzioni limitate e precisamente definite, per minimizzare la superficie di attacco. Tali componenti includono la ROM di avvio, che costituisce un root di attendibilità hardware per l'avvio protetto, motori AES dedicati per crittografie e decrittografie efficienti e sicure e il chip Secure Enclave. *Secure Enclave* è un componente di Apple system on chip (SoC) presente su tutti i più recenti iPhone, iPad, Apple Watch, Apple TV e HomePod, su tutti i Mac dotati di chip Apple e sui Mac dotati di chip di sicurezza Apple T2. Secure Enclave segue lo stesso principio di design del SoC, poiché contiene la propria ROM di avvio e il proprio motore AES. Secure Enclave costituisce inoltre le fondamenta per la creazione e l'archiviazione sicura delle chiavi necessarie alla codifica dei dati a riposo e protegge e convalida i dati biometrici per Face ID e Touch ID.

La codifica dei dati archiviati deve essere rapida ed efficiente. Al tempo stesso, non può esporre i dati (ovvero i *contenuti delle chiavi*) che utilizza per stabilire le relazioni crittografiche tra le chiavi. Il motore hardware AES risolve questo problema eseguendo rapide crittografie e decrittografie in linea *man mano che i file vengono scritti o letti*. Un canale speciale proveniente da Secure Enclave fornisce gli elementi necessari per le chiavi al motore AES senza esporre tali informazioni al processore per le applicazioni (o alla CPU) o al sistema operativo in generale. In questo modo il meccanismo di protezione dei dati Apple e FileVault possono aiutare a proteggere i file degli utenti senza esporre le chiavi di codifica di lunga durata.

Apple ha progettato l'avvio protetto per garantire la sicurezza dei livelli più bassi del software e per consentire di caricare all'avvio solo il software autorizzato del sistema operativo Apple. L'avvio protetto ha inizio nel codice immutabile chiamato *ROM di avvio*, che viene configurato durante la fabbricazione del SoC Apple ed è noto come la *radice di attendibilità hardware*. Sui Mac con un chip T2, l'attendibilità per l'avvio protetto di macOS inizia con il chip T2 stesso. (Sia il chip T2 che Secure Enclave eseguono i propri processi di avvio protetto usando le proprie ROM di avvio indipendenti, esattamente nello stesso modo in cui i chip della serie A, M1 e M2 eseguono il proprio avvio protetto).

Secure Enclave è anche responsabile dell'elaborazione dei dati del volto e delle impronte digitali acquisiti dai sensori di Face ID e Touch ID sui dispositivi Apple. Ciò fornisce un'autenticazione sicura, mantenendo sempre i dati biometrici dell'utente privati e al sicuro. Consente inoltre agli utenti di contare sulla sicurezza garantita da codici e password più lunghi e complessi, accompagnata in molti casi dalla comodità di un'autenticazione immediata per eseguire l'accesso o per effettuare acquisti.

Sicurezza del SoC Apple

I chip progettati da Apple costituiscono un'architettura comune su tutti i prodotti Apple e adesso sono presenti anche sui Mac, oltre che su iPhone, iPad, Apple TV e Apple Watch. Il team di progettazione dei processori Apple ha realizzato e perfezionato i propri SoC per oltre dieci anni. Il risultato è un'architettura scalabile progettata per tutti i dispositivi e che è divenuta un punto di riferimento nel settore per quanto riguarda le capacità di sicurezza. Queste fondamenta comuni per le funzionalità di sicurezza sono possibili solo da un'azienda che progetta i propri componenti hardware ottimizzandoli per il proprio software.

I processori Apple sono stati progettati e realizzati per offrire specificamente le seguenti funzionalità di sicurezza del sistema.

Funzionalità	A10	A11, S3	A12, A13, A14 S4 - S9	A15, A16, A17	M1, M2, M3
Protezione dell'integrità del kernel	✓	✓	✓	✓	✓
Restrizioni rapide dei permessi	✗	✓	✓	✓	✓
Protezione dell'integrità dei coprocessori di sistema	✗	✗	✓	✓	✓
Codici di autenticazione dei puntatori	✗	✗	✓	✓	✓
Page Protection Layer (PPL)	✗	✓	✓	✗	✗ Vedi la nota 1 sotto.
Secure Page Table Monitor	✗	✗	✗	✓ Vedi la nota 2 sotto.	✗

Nota 1: il Page Protection Layer (PPL) richiede che la piattaforma esegua *solo* codice firmato e attendibile. Si tratta di un modello di sicurezza che non è applicabile a macOS.

Nota 2: il Secure Page Table Monitor (SPTM) è supportato su A15, A16 e A17 e sostituisce il Page Protection Layer sulle piattaforme supportate.

I chip progettati da Apple offrono specificamente anche le seguenti funzionalità di protezione dei dati.

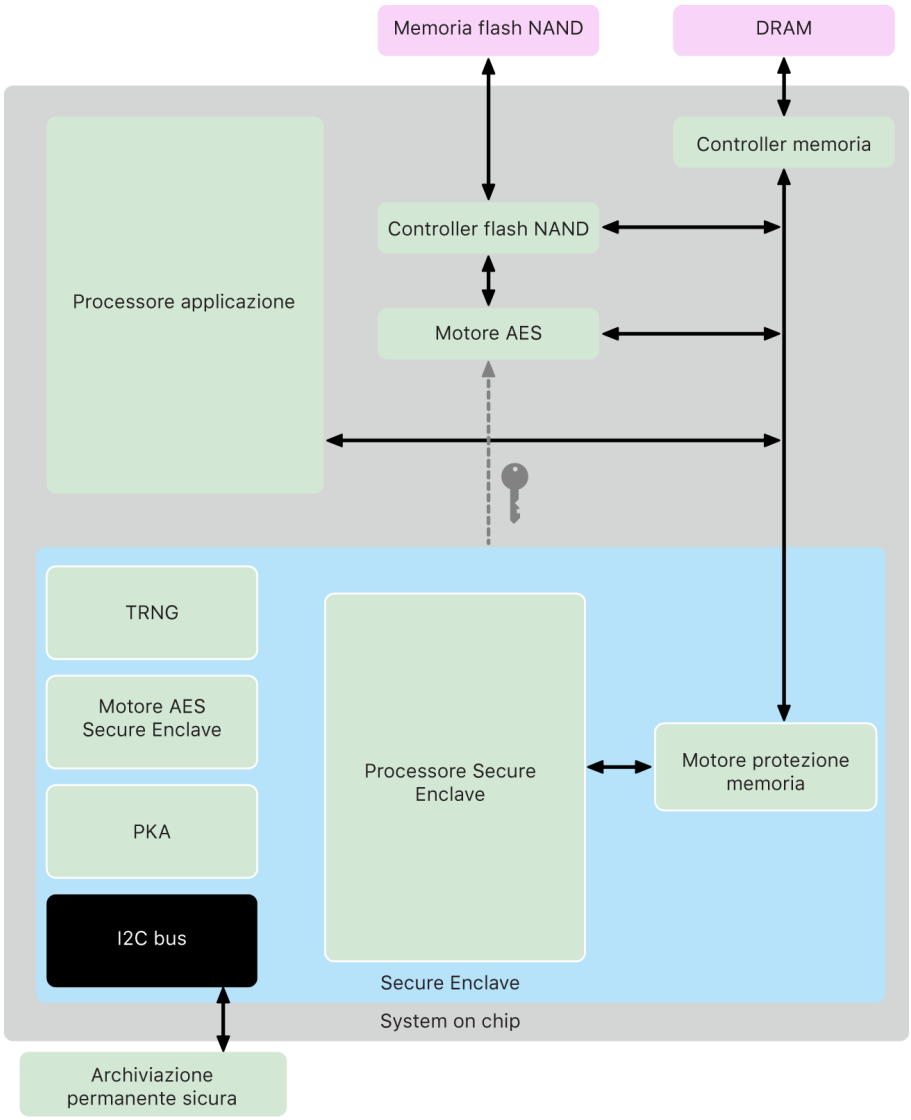
Funzionalità	A10, A11 S3	A12 - A17 S4 - S9 M1, M2, M3
Protezione SKP (Sealed Key Protection)	✓	✓
recoveryOS: tutte le classi di protezione dati	✓	✓
Avvii alternativi per modalità DFU, diagnosi Apple e aggiornamento: classi di protezione dati A, B e C	✗	✓

Secure Enclave

Secure Enclave è un sottosistema di sicurezza dedicato presente nelle versioni più recenti di iPhone, iPad, Mac, Apple TV, Apple Watch e HomePod.

Panoramica

Secure Enclave è un sottosistema sicuro dedicato integrato sui SoC di Apple. Secure Enclave è isolato dal processore principale per fornire un ulteriore livello di sicurezza ed è progettato per mantenere protetti i dati sensibili dell'utente, anche se il kernel del processore per le applicazioni venisse compromesso. Il suo design segue gli stessi principi del SoC: una ROM di avvio che stabilisce una radice di attendibilità hardware, un motore AES per operazioni crittografiche efficienti e sicure e una memoria protetta. Sebbene Secure Enclave non sia dotato di uno spazio di archiviazione, ha un meccanismo che gli consente di archiviare informazioni in modo sicuro su uno spazio collegato, separato dalla memoria flash NAND utilizzata dal processore per le applicazioni e dal sistema operativo.



Secure Enclave è una funzionalità hardware presente su gran parte dei modelli di iPhone, iPad, Mac, Apple TV, Apple Watch e HomePod, ossia:

- iPhone 5s o modelli successivi
- iPad Air o modelli successivi
- Computer Mac dotati di chip Apple
- MacBook Pro con Touch Bar (2016 e 2017) dotati di chip Apple T1
- Computer Mac dotati di processore Intel con chip di sicurezza Apple T2
- Apple TV HD o modelli successivi
- Apple Watch Series 1 o modelli successivi
- HomePod e HomePod mini

Processore di Secure Enclave

Il processore di Secure Enclave fornisce la potenza di elaborazione principale al chip. Per fornire il più alto livello di isolamento, il processore di Secure Enclave è dedicato esclusivamente a Secure Enclave. Ciò aiuta a impedire attacchi a canale laterale, che si basano su software dannoso che condivide lo stesso core di esecuzione del software oggetto dell'attacco.

Il processore di Secure Enclave esegue una versione personalizzata da Apple del microkernel L4. Esso è progettato per operare in modo efficiente a una velocità di clock bassa, che aiuta a proteggerlo da attacchi basati sul monitoraggio del clock e dei consumi. Il processore di Secure Enclave, a partire dai chip A11 e S4, include un motore protetto dalla memoria e una memoria codificata con funzionalità anti-replay, l'avvio protetto, un generatore di numeri casuali dedicato e un motore AES separato.

Motore di protezione della memoria

Secure Enclave opera da una regione dedicata della memoria DRAM del dispositivo. La memoria sicura di Secure Enclave è isolata dal processore per le applicazioni da vari livelli di protezione.

Quando il dispositivo si avvia, la ROM di avvio di Secure Enclave genera una chiave casuale di protezione della memoria effimera per il motore di protezione della memoria. Ogni volta che Secure Enclave scrive sulla propria regione di memoria dedicata, il motore di protezione codifica il blocco di memoria tramite AES in modalità Mac XEX (xor-encrypt-xor) e calcola un tag di autenticazione CMAC (Cipher-based Message Authentication Code) per la memoria. Il motore di protezione archivia il tag di autenticazione insieme alla memoria codificata. Quando Secure Enclave legge la memoria, il motore di protezione verifica il tag di autenticazione. Se viene trovata una corrispondenza, il motore di protezione decrittografa il blocco di memoria. Se non viene trovata una corrispondenza, il motore di protezione invia un segnale di errore a Secure Enclave. Dopo un errore di autenticazione della memoria, Secure Enclave smette di accettare richieste finché il sistema non viene riavviato.

A partire dai SoC Apple A11 e S4, il motore di protezione della memoria aggiunge la protezione contro i replay attack per la memoria di Secure Enclave. Per aiutare a impedire il riutilizzo di dati critici per la sicurezza, il motore di protezione della memoria archivia un numero univoco di singolo utilizzo chiamato *valore anti-replay*, che serve per il blocco di memoria, insieme al tag di autenticazione. Il valore anti-replay viene utilizzato come ulteriore elemento di sicurezza per il tag di autenticazione CMAC. I valori anti-replay per tutti i blocchi di memoria sono protetti tramite un albero di integrità che ha il proprio root in una SRAM dedicata all'interno di Secure Enclave. Per le scritture, il motore di protezione della memoria *aggiorna* i valori anti-replay e ciascun livello dell'albero di integrità fino alla SRAM. Per le letture, il motore di protezione della memoria *verifica* i valori anti-replay e ciascun livello dell'albero di integrità fino alla SRAM. Le mancate corrispondenze dei valori anti-replay vengono gestite allo stesso modo di quelle dei tag di autenticazione.

Sui SoC Apple A14, M1 o successivi, il motore di protezione della memoria supporta due chiavi di protezione della memoria effimere. La prima è usata per dati privati di Secure Enclave, mentre la seconda è usata per i dati condivisi con il processore neurale protetto.

Il motore di protezione della memoria opera in collegamento e in modo trasparente con Secure Enclave. Secure Enclave legge e scrive la memoria come se fosse una normale DRAM non codificata, mentre un osservatore al di fuori di Secure Enclave è in grado di vedere solo la versione codificata e autenticata delle memoria. Ciò fornisce una forte protezione della memoria senza svantaggi sulle prestazioni o sulla complessità del software.

ROM di avvio di Secure Enclave

Secure Enclave include una ROM di avvio dedicata. In maniera simile alla ROM di avvio del processore per le applicazioni, la ROM di avvio di Secure Enclave è costituita da codice immutabile che stabilisce la radice di attendibilità hardware per Secure Enclave.

All'avvio del sistema, iBoot assegna a Secure Enclave una regione di memoria dedicata. Prima di usare la memoria, la ROM di avvio di Secure Enclave inizializza il motore di protezione per proteggere crittograficamente tale memoria.

Quindi il processore per le applicazioni invia l'immagine del sistema operativo di Secure Enclave (sepOS) alla ROM di avvio di Secure Enclave. Dopo aver copiato l'immagine di sepOS nella memoria protetta, la ROM di avvio di Secure Enclave controlla l'hash crittografico e la firma dell'immagine per verificare che sepOS sia autorizzato a essere eseguito sul dispositivo. Se l'immagine di sepOS è correttamente firmata per l'esecuzione sul dispositivo, la ROM di avvio di Secure Enclave trasferisce il controllo a sepOS. Se la firma non è valida, la ROM di avvio di Secure Enclave è progettata per impedire qualsiasi utilizzo di quest'ultimo fino al prossimo ripristino del chip.

Sui SoC Apple A10 e modelli successivi, la ROM di avvio di Secure Enclave blocca un hash di sepOS in un registro dedicato a tale scopo. L'acceleratore delle chiavi pubbliche utilizza tale hash per le chiavi legate al sistema operativo.

Monitor di avvio di Secure Enclave

Sui SoC Apple A13 o modelli successivi, Secure Enclave include un monitor di avvio progettato per garantire un'integrità maggiore per l'hash dell'istanza di sepOS avviata.

All'avvio del sistema, la configurazione della protezione dell'integrità dei coprocessori di sistema (SCIP) del processore di Secure Enclave aiuta a impedire a quest'ultimo di eseguire qualsiasi codice che non sia la ROM di avvio di Secure Enclave. Il monitor di avvio aiuta a impedire a Secure Enclave di modificare direttamente la configurazione del SCIP. Per rendere il sepOS caricato eseguibile, la ROM di avvio di Secure Enclave invia al monitor di avvio una richiesta con l'indirizzo e le dimensioni di tale sepOS caricato. Una volta ricevuta la richiesta, il monitor di avvio inizializza il processore di Secure Enclave, applica un hash al sepOS caricato, aggiorna le impostazioni del SCIP per consentire l'esecuzione del sepOS caricato e avvia l'esecuzione all'interno del codice appena caricato. Man mano che l'avvio del sistema procede, questo stesso processo viene utilizzato ogni volta che viene reso eseguibile del nuovo codice. Ogni volta, il monitor di avvio aggiorna un hash in esecuzione del processo di avvio. Il monitor di avvio include anche importanti parametri di sicurezza nell'hash in esecuzione.

Una volta completato l'avvio, il monitor finalizza l'hash in esecuzione e lo invia all'acceleratore delle chiavi pubbliche perché venga usato nelle chiavi legate al sistema operativo. Questo processo garantisce che il collegamento delle chiavi del sistema operativo non possa essere bypassato, anche nel caso in cui ci fosse una vulnerabilità nella ROM di avvio di Secure Enclave.

Generatore di numeri veramente casuali

Il generatore di numeri veramente casuali è utilizzato per generare dati casuali sicuri. Secure Enclave lo utilizza ogni volta che genera una chiave crittografica casuale, un seed per una chiave casuale o altra entropia. Il generatore di numeri casuali è basato su vari oscillatori ad anello, successivamente elaborati tramite CTR_DRBG (un algoritmo basato sulla codifica a blocchi in modalità CTR).

Chiavi crittografiche root

Secure Enclave include una chiave crittografica root composta da un ID unico (UID). L'UID è unico per ciascun dispositivo individuale e non è correlato a nessun altro identificativo sul dispositivo.

Un UID generato in modo casuale viene impresso nel SoC durante la produzione. A partire dai SoC A9, l'UID viene creato dal generatore di numeri casuali di Secure Enclave durante la produzione e viene scritto sui fusibili tramite un processo software eseguito interamente all'interno di Secure Enclave. Tale processo impedisce che l'UID sia visibile al di fuori del dispositivo durante la produzione e quindi assicura che non sia disponibile per l'accesso o l'archiviazione da parte di Apple o dei suoi fornitori.

sepOS utilizza l'UID per proteggere alcuni segreti specifici del dispositivo. L'UID consente di collegare attraverso la codifica i dati a un dispositivo particolare. Ad esempio, la gerarchia di chiavi che protegge il file system include l'UID, quindi se l'unità di archiviazione SSD interna viene fisicamente spostata da un dispositivo all'altro, i file sono inaccessibili. Altri segreti protetti specifici di ogni dispositivo includono i dati di Face ID o di Touch ID. Sui Mac, solo l'unità di archiviazione totalmente interna collegata al motore AES riceve questo livello di codifica. Ad esempio, né i dispositivi di archiviazione esterni collegati tramite USB né le unità di archiviazione PCIe aggiunte a Mac Pro (2019) vengono codificati in questo modo.

Secure Enclave ha anche un identificatore per i gruppi di dispositivi (GID), che è comune a tutti i dispositivi che utilizzano un determinato SoC (ad esempio, tutti i dispositivi che usano il SoC Apple A15 condividono lo stesso GID).

L'UID e il GID non sono disponibili via JTAG (Joint Test Action Group) o altre interfacce di debug.

Motore AES di Secure Enclave

Il motore AES di Secure Enclave è un blocco hardware usato per eseguire operazioni di crittografia simmetrica basata sull'algoritmo AES. Il motore AES è progettato per essere immune alla fuga di informazioni tramite misurazioni temporali e l'analisi dell'energia statica (SPA). A partire dal SoC A9, il motore AES include anche misure di analisi dell'energia dinamica (DPA).

Il motore AES supporta chiavi hardware e software. Le chiavi hardware derivano dall'UID o dal GID di Secure Enclave. Tali chiavi restano all'interno del motore AES e non sono rese visibili nemmeno al software di sepOS. Sebbene il software possa richiedere operazioni di crittografia e decrittografia con le chiavi hardware, esso non può estrarre le chiavi.

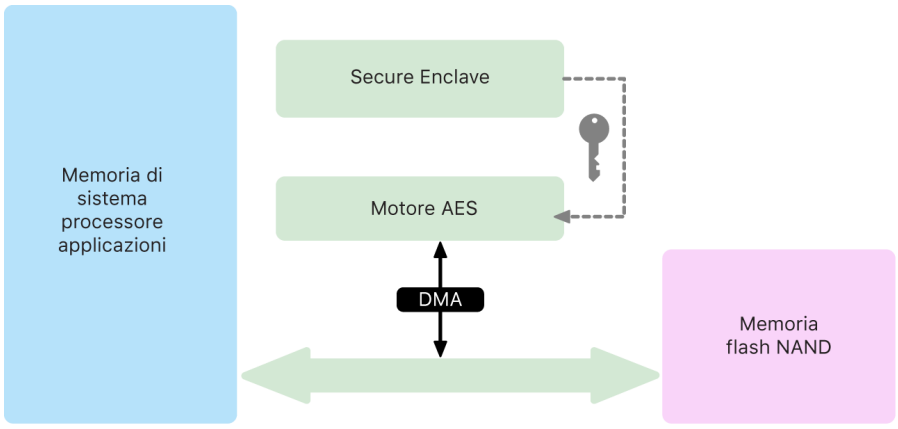
Sui SoC Apple A10 e modelli più recenti, il motore AES include bit seed bloccabili che diversificano le chiavi derivate dall'UID o GID. Ciò consente di condizionare l'accesso ai dati in base alla modalità in cui si trova il dispositivo. Ad esempio, i bit seed bloccabili vengono usati per impedire l'accesso ai dati protetti da password quando si esegue l'avvio in modalità DFU. Per ulteriori informazioni, consulta Codici e password.

Motore AES

Ogni dispositivo Apple con Secure Enclave possiede al suo interno anche un motore di codifica dedicato basato su AES256 (il "motore AES"), integrato nel percorso DMA (Direct Memory Access) tra la memoria flash NAND (non volatile) e la memoria principale del sistema, che rende altamente efficiente il processo di codifica dei file. Sui processori A9 o modelli successivi della stessa serie, il sottosistema di archiviazione flash si trova su un bus isolato, che ha accesso solo alla memoria con i dati dell'utente mediante il motore di codifica del DMA.

Durante l'avvio, sepOS genera una chiave di cifratura effimera tramite il generatore di numeri casuali. Secure Enclave trasmette questa chiave al motore AES tramite un collegamento dedicato progettato per impedirne l'accesso da parte di qualsiasi software al di fuori del chip. sepOS potrà quindi utilizzare la chiave effimera per cifrare le chiavi dei file utilizzate dal driver del file system del processore per le applicazioni. Quando il driver del file system legge o scrive un file, invia la chiave cifrata al motore AES, che decifra la chiave. Il motore AES non espone mai la chiave decifrata al software.

Nota: il motore AES è un componente separato sia da Secure Enclave che dal motore AES di Secure Enclave, ma il suo funzionamento è strettamente legato a Secure Enclave, come mostrato sotto.



Acceleratore delle chiavi pubbliche

L'acceleratore delle chiavi pubbliche (PKA) è un blocco hardware utilizzato per eseguire operazioni di crittografia asimmetrica. L'acceleratore delle chiavi pubbliche supporta algoritmi di firma e codifica RSA ed ECC (crittografia basata su curva ellittica). L'acceleratore delle chiavi pubbliche è progettato per essere immune a fughe di dati tramite misurazioni temporali e attacchi a canale laterale, come SPA e DPA.

L'acceleratore delle chiavi pubbliche supporta chiavi software e hardware. Le chiavi hardware derivano dall'UID o dal GID di Secure Enclave. Tali chiavi restano all'interno dell'acceleratore delle chiavi pubbliche e non sono rese visibili nemmeno al software di sepOS.

A partire dai SoC A13, tramite tecniche di verifica formale è stato provato che le implementazioni crittografiche dell'acceleratore delle chiavi pubbliche sono matematicamente corrette.

Sui SoC Apple A10 e modelli successivi, l'acceleratore delle chiavi pubbliche supporta le chiavi legate al sistema operativo, un meccanismo conosciuto anche come SKP (Sealed Key Protection). Tali chiavi vengono generate tramite una combinazione dell'UID del dispositivo e dell'hash del sepOS in esecuzione sul dispositivo. L'hash è fornito dalla ROM di avvio di Secure Enclave oppure dal monitor di avvio di Secure Enclave sui SoC Apple A13 o modelli successivi. Tali chiavi sono usate anche per verificare la versione di sepOS durante le richieste a determinati servizi Apple; sono inoltre usate per migliorare la sicurezza dei dati protetti da codice, aiutando a impedire l'accesso ai contenuti delle chiavi se vengono effettuate modifiche importanti al sistema senza autorizzazione da parte dell'utente.

Archiviazione non volatile protetta

Secure Enclave è dotato di un dispositivo di archiviazione non volatile protetta. L'archiviazione non volatile protetta è collegata a Secure Enclave tramite un bus I2C dedicato, quindi è accessibile solo a Secure Enclave. Tutte le chiavi di codifica dei dati utente hanno la propria radice nell'entropia memorizzata nell'archiviazione non volatile protetta di Secure Enclave.

Sui dispositivi con SoC A12, S4 e modelli successivi, Secure Enclave è abbinato a un componente Secure Storage per l'archiviazione dell'entropia. Il componente Secure Storage è progettato a sua volta con un codice ROM immutabile, un generatore di numeri casuali hardware, una chiave crittografica unica per ciascun dispositivo, motori crittografici e un sistema di rilevamento di manomissione fisica. Secure Enclave e il componente Secure Storage comunicano tramite un protocollo codificato e autenticato che fornisce un accesso esclusivo all'entropia.

I dispositivi immessi sul mercato a partire dall'autunno del 2020 sono dotati di un componente Secure Storage di seconda generazione. Il componente Secure Storage di seconda generazione è provvisto di meccanismi di blocco a contatore. Ogni meccanismo di blocco a contatore archivia un salt a 128 bit, un valore di verifica del codice a 128 bit, un contatore a 8 bit e un valore di tentativi massimi a 8 bit. L'accesso ai meccanismi di blocco a contatore avviene tramite un protocollo codificato e autenticato.

I meccanismi di blocco a contatore contengono l'entropia necessaria per sbloccare i dati utente protetti del codice. Per accedere ai dati dell'utente, il Secure Enclave abbinato deve derivare il corretto valore di entropia del codice dal codice dell'utente e dall'UID di Secure Enclave. Non è possibile venire a conoscenza del codice dell'utente tramite tentativi di sblocco inviati da una sorgente diversa dal Secure Enclave abbinato. Se viene superato il limite massimo di inserimento del codice (ad esempio, 10 tentativi su iPhone), i dati protetti dal codice vengono completamente cancellati dal componente Secure Storage.

Per creare un meccanismo di blocco a contatore, Secure Enclave invia al componente Secure Storage il valore di entropia del codice e il valore di tentativi massimi. Secure Storage genera il valore salt tramite il proprio generatore di numeri casuali. Quindi deriva un valore di verifica del codice e un valore di entropia del meccanismo di blocco dall'entropia del codice fornita, dalla chiave crittografica unica di Secure Storage e dal valore salt. Il componente inizializza il meccanismo di blocco a contatore con un conteggio pari a 0, il valore di tentativi massimi fornito, il valore di verifica del codice derivato e il valore salt. Il componente quindi restituisce il valore di entropia del meccanismo di blocco generato a Secure Enclave.

Per ricevere il valore di entropia da un meccanismo di blocco a contatore in un secondo momento, Secure Enclave invia a Secure Storage l'entropia del codice. Per prima cosa, il componente Secure Storage incrementa il conteggio del meccanismo di blocco. Se il conteggio incrementato supera il valore di tentativi massimi, il componente cancella completamente il meccanismo di blocco. Se il numero di tentativi massimi non è stato raggiunto, il componente Secure Storage tenta di derivare il valore di verifica del codice e il valore di entropia del meccanismo di blocco con lo stesso algoritmo usato per creare il meccanismo di blocco a contatore. Se il valore di verifica del codice derivato corrisponde al valore di verifica del codice archiviato, Secure Storage restituisce il valore dell'entropia del meccanismo di blocco a Secure Enclave e reimposta il contatore su 0.

Le chiavi utilizzate per accedere ai dati protetti da password hanno la propria radice nell'entropia archiviata nei meccanismi di blocco a contatore. Per ulteriori informazioni, consulta Panoramica della protezione dati.

L'archiviazione non volatile protetta viene usata per tutti i servizi anti-replay in Secure Enclave. I servizi anti-replay su Secure Enclave sono usati per la revoca dei dati in seguito ad eventi che costituiscono momenti di delimitazione per l'anti-replay, tra cui, ad esempio:

- Modifica del codice
- Abilitazione o disabilitazione di Face ID o di Touch ID
- Aggiunta o rimozione di di un volto in Face ID o di un'impronta digitale in Touch ID
- Ripristino di Face ID o di Touch ID
- Aggiunta o rimozione di una carta di Apple Pay
- Inizializzazione dei contenuti e delle impostazioni

Sulle architetture sprovviste del componente Secure Storage, per fornire servizi di archiviazione sicura a Secure Enclave viene utilizzata una memoria di sola lettura programmabile cancellabile elettricamente (EEPROM). Proprio come il componente Secure Storage, tale memoria è collegata e accessibile solo a Secure Enclave, ma non contiene funzionalità di sicurezza hardware dedicate, non garantisce accesso esclusivo all'entropia (a eccezione del fatto di essere collegata fisicamente) e non ha meccanismi di blocco a contatore.

Processore neurale protetto

Sui dispositivi con Face ID (non con Touch ID) il processore neurale protetto converte immagini 2D e mappe di profondità in una rappresentazione matematica del volto dell'utente.

Sui SoC da A11 fino ad A13, il processore neurale protetto è integrato in Secure Enclave. Il processore neurale protetto utilizza l'accesso diretto alla memoria per ottenere prestazioni maggiori. Questo accesso diretto alle regioni di memoria autorizzate è limitato da un'unità per la gestione della memoria di input/output sotto il controllo del kernel di sepOS.

A partire dai chip A14, M1 e successivi, il processore neurale protetto è implementato tramite una modalità sicura nel processore neurale del processore per le applicazioni. Un controller hardware di sicurezza dedicato esegue il passaggio dalle operazioni del processore per le applicazioni e quelle di Secure Enclave, reimpostando lo stato del processore neurale a ciascuna transizione per mantenere protetti i dati di Face ID. Un processore dedicato si occupa della codifica della memoria, dell'autenticazione e del controllo degli accessi. Al tempo stesso, utilizza una chiave crittografica separata e un intervallo di memoria separato per limitare le operazioni del processore neurale protetto alle regioni di memoria autorizzate.

Monitor di potenza e di clock

Tutti i componenti elettronici sono progettati per funzionare entro determinati limiti di tensione e frequenza. Se vengono fatti funzionare al di fuori di tali limiti, i componenti elettronici possono incontrare problemi e i controlli di sicurezza possono essere bypassati. Per aiutare a garantire che la tensione e la frequenza rimangano dentro l'intervallo sicuro, Secure Enclave è progettato con circuiti di monitoraggio. Tali circuiti di monitoraggio sono progettati per avere un intervallo di funzionamento molto più ampio rispetto al resto di Secure Enclave. Se i monitor rilevano un elemento che opera in modo non valido, i clock di Secure Enclave si interrompono automaticamente e non riprendono fino al prossimo ripristino del SoC.

Riepilogo delle funzionalità di Secure Enclave

Nota: i prodotti con processore A12, A13, S4 e S5 immessi sul mercato a partire dall'autunno del 2020 sono dotati di componente Secure Storage di seconda generazione, mentre i prodotti precedenti basati sugli stessi SoC sono dotati di Secure Storage di prima generazione.

SoC	Motore di protezione della memoria	Secure Storage	Motore AES	PKA
A8	Codifica e autenticazione	EEPROM	Sì	No
A9	Codifica e autenticazione	EEPROM	Protezione DPA	Sì
A10	Codifica e autenticazione	EEPROM	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo
A11	Codifica, autenticazione e anti-replay	EEPROM	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo
A12 (dispositivi Apple immessi sul mercato prima dell'autunno del 2020)	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.1	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo
A12 (dispositivi Apple immessi sul mercato dopo l'autunno del 2020)	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.2	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo
A13 (dispositivi Apple immessi sul mercato prima dell'autunno del 2020)	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.1	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo e monitor di avvio
A13 (dispositivi Apple immessi sul mercato dopo l'autunno del 2020)	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.2	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo e monitor di avvio
A14 - A17	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.2	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo e monitor di avvio
S3	Codifica e autenticazione	EEPROM	Protezione DPA e bit seed bloccabili	Sì
S4	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.1	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo
S5 (dispositivi Apple immessi sul mercato prima dell'autunno del 2020)	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.1	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo
S5 (dispositivi Apple immessi sul mercato dopo l'autunno del 2020)	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.2	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo
S6 - S9	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.2	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo
T2	Codifica e autenticazione	EEPROM	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo
M1, M2, M3	Codifica, autenticazione e anti-replay	Componente Secure Storage gen.2	Protezione DPA e bit seed bloccabili	Chiavi legate al sistema operativo e monitor di avvio

Face ID e Touch ID

Sicurezza di Face ID e Touch ID

I codici e le password sono elementi essenziali per la sicurezza dei dispositivi Apple. Al tempo stesso, gli utenti necessitano di un metodo pratico per accedere ai propri dispositivi, spesso più di cento volte al giorno. L'autenticazione biometrica consente di sfruttare la sicurezza di un codice sicuro (o addirittura di migliorare la sicurezza di un codice o una password, dal momento che non dovranno essere inseriti manualmente) e al tempo stesso consente di sbloccare un dispositivo comodamente e rapidamente con la pressione di un dito o con uno sguardo. Face ID e Touch ID non vanno a sostituire un codice o una password, ma nella maggior parte dei casi rendono l'accesso più rapido e veloce.

L'architettura di sicurezza dell'autenticazione biometrica di Apple si appoggia su una totale separazione di responsabilità tra i sensori biometrici e Secure Enclave e su un collegamento sicuro tra di essi. Il sensore rileva l'immagine biometrica e la trasmette in modo sicuro a Secure Enclave. Durante la registrazione, Secure Enclave elabora, esegue la crittografia e archivia i dati dei modelli ricavati da Face ID e Touch ID. Durante l'analisi per verificare la corrispondenza, Secure Enclave confronta i dati in arrivo dal sensore biometrico con i modelli archiviati per determinare se sbloccare il dispositivo o considerare la corrispondenza valida (per Apple Pay, autorizzazioni in-app e altri usi di Face ID e Touch ID). L'architettura supporta i dispositivi che includono sia il sensore che Secure Enclave (come iPhone, iPad e molti sistemi Mac), così come la possibilità di avere il sensore in una periferica separata che viene quindi abbinata in modo sicuro a Secure Enclave sui Mac con chip Apple.

Sicurezza di Face ID

Con un semplice sguardo, Face ID sblocca in tutta sicurezza i dispositivi Apple supportati. Questa funzionalità fornisce un'autenticazione intuitiva e sicura resa possibile dal sistema fotografico TrueDepth, che utilizza tecnologie avanzate per eseguire una mappatura accurata della geometria del volto dell'utente. Face ID utilizza le reti neurali per determinare l'attenzione, stabilire la corrispondenza e impedire la falsificazione. Ciò consente all'utente di sbloccare il telefono con uno sguardo, anche quando indossa una mascherina se utilizza i dispositivi che supportano la funzionalità. Face ID si adatta automaticamente ai cambiamenti di aspetto e protegge accuratamente la privacy e la sicurezza dei dati biometrici dell'utente.

Face ID è una funzionalità progettata per confermare la presenza di attenzione da parte dell'utente, fornire un solido metodo di autenticazione con basse probabilità di errato riconoscimento e ridurre la possibilità di falsificazione, sia digitale che fisica.

La fotocamera TrueDepth inquadra automaticamente il volto quando l'utente riattiva un dispositivo Apple dotato di Face ID sollevandolo o toccando lo schermo, così come quando il dispositivo tenta di autenticare l'utente per mostrare una notifica in entrata oppure quando un'app supportata richiede l'autenticazione tramite Face ID. Quando Face ID rileva un volto, conferma la presenza di attenzione e l'intenzione di eseguire lo sblocco verificando che gli occhi dell'utente siano aperti e l'attenzione sia rivolta verso il dispositivo; per questioni di accessibilità, la funzionalità di controllo dell'attenzione di Face ID è disabilitata quando VoiceOver è attivato e, se richiesto, può essere disabilitata separatamente. Quando utilizzi Face ID indossando una mascherina, il rilevamento dello sguardo è sempre richiesto.

Una volta che la fotocamera TrueDepth ha confermato la presenza di un volto attento, essa proietta e legge migliaia di punti ad infrarossi per formare una mappa di profondità del viso, insieme a un'immagine a infrarossi 2D. Tali dati vengono utilizzati per creare una sequenza di immagini 2D e di mappe di profondità, che vengono firmate digitalmente e inviate a Secure Enclave. Per contrastare la falsificazione sia fisica che digitale, la fotocamera TrueDepth rende casuale la sequenza delle immagini 2D e delle mappe di profondità e proietta un motivo casuale specifico per ogni dispositivo. Una parte del processore neurale protetto, all'interno di Secure Enclave, trasforma questi dati in una rappresentazione matematica e la confronta con i dati facciali registrati, che sono a loro volta una rappresentazione matematica del volto dell'utente, rilevato in varie pose.

Sicurezza di Touch ID

Touch ID è il sistema di rilevamento di impronte digitali che permette di accedere ai dispositivi Apple supportati in tutta sicurezza in modo semplice e veloce. Questa tecnologia legge i dati delle impronte digitali da qualsiasi angolazione e, nel tempo, impara a conoscerle sempre meglio; il sensore continua infatti ad ampliare la mappa dell'impronta perché con l'utilizzo vengono individuati nuovi nodi in sovrapposizione.

I dispositivi Apple con un sensore Touch ID possono essere sbloccati tramite impronta digitale. Touch ID non elimina la necessità di impostare un codice per il dispositivo o una password utente, che sono comunque necessari all'avvio, al riavvio o al logout (nel caso dei Mac) del dispositivo. In alcune app, Touch ID può anche essere utilizzato al posto di codici dispositivo e password utente, per esempio per sbloccare note protette da password nell'app Note, per sbloccare siti web protetti tramite portachiavi e per sbloccare le password delle app compatibili con Touch ID. Tuttavia, in alcune situazioni un codice dispositivo o una password utente sono sempre richiesti, ad esempio, per modificare un codice o una password esistenti o per rimuovere impronte digitali registrate o crearne di nuove.

Quando il sensore dell'impronta digitale rileva il tocco di un dito, attiva l'array di imaging avanzato perché scansioni l'impronta e invii la relativa scansione a Secure Enclave. Il canale utilizzato per rendere sicuro il collegamento varia a seconda del fatto che il sensore Touch ID sia integrato nel dispositivo con Secure Enclave oppure che si trovi in una periferica separata.

Mentre la scansione dell'impronta digitale viene vettorizzata per l'analisi, i dati raster sono archiviati temporaneamente nella memoria codificata all'interno di Secure Enclave e poi eliminati. L'analisi utilizza la mappatura angolare del disegno papillare dello strato sottocutaneo del dito, un processo con perdita che scarta i dettagli particolari, cioè le caratteristiche che sarebbero richieste per ricostruire l'impronta reale dell'utente. Durante la registrazione, la mappa di nodi risultante viene archiviata in un formato codificato che può essere letto solo da Secure Enclave e viene utilizzata come modello per verificare le corrispondenze in futuro, ma senza contenere informazioni sull'identità. Questi dati non escono mai dal dispositivo: non vengono inviati ad Apple e non vengono inclusi nei backup del dispositivo.

Sicurezza del canale di comunicazione per Touch ID integrato

La comunicazione tra Secure Enclave e il sensore Touch ID integrato avviene tramite bus SPI (Serial Peripheral Interface). Il processore si occupa di trasmettere i dati a Secure Enclave ma non può leggerli, perché sono codificati e autenticati con una chiave di sessione negoziata tramite una chiave condivisa fornita a ogni sensore Touch ID e al Secure Enclave corrispondente durante la fabbricazione. Per ogni sensore Touch ID, la chiave condivisa è sicura, casuale e unica. Lo scambio di chiave di sessione utilizza la cifratura della chiave AES, un processo in cui entrambe le parti forniscono una chiave casuale che stabilisce la chiave di sessione e utilizza la codifica di trasporto dati AES-CCM che garantisce sia autenticazione che riservatezza.

Magic Keyboard con Touch ID

Magic Keyboard con Touch ID (e Magic Keyboard con Touch ID e tastierino numerico) fornisce un sensore Touch ID in una tastiera esterna che può essere utilizzata con qualsiasi Mac con chip Apple. Magic Keyboard con Touch ID svolge il ruolo del sensore biometrico; non archivia i modelli biometrici, non elabora il riconoscimento delle misurazioni biometriche né applica le politiche di sicurezza (ad esempio, dover inserire la password dopo 48 ore che non è stato eseguito uno sblocco). Il sensore Touch ID su Magic Keyboard con Touch ID deve essere abbinato in maniera sicura al processore Secure Enclave sul Mac prima di poter essere utilizzato; successivamente Secure Enclave esegue la registrazione e le operazioni di riconoscimento e applica le politiche di sicurezza nello stesso modo in cui lo farebbe con un sensore Touch ID integrato. Per le tastiere Magic Keyboard con Touch ID in dotazione con un Mac, Apple esegue la procedura di abbinamento in fabbrica. L'abbinamento può essere eseguito anche dall'utente, se necessario. Una tastiera Magic Keyboard con Touch ID può essere abbinata in maniera sicura a un solo Mac per volta, ma un Mac può mantenere abbinamenti sicuri con 5 diverse tastiere Magic Keyboard con Touch ID.

Magic Keyboard con Touch ID e i sensori Touch ID integrati sono compatibili. Se un dito registrato tramite un sensore Touch ID integrato su un Mac viene presentato a una Magic Keyboard con Touch ID, il processore Secure Enclave del Mac è in grado di elaborare correttamente il riconoscimento (e vice versa).

Per supportare l'abbinamento sicuro e quindi la comunicazione tra il processore Secure Enclave del Mac e la tastiera Magic Keyboard con Touch ID, quest'ultima è dotata di un blocco di accelerazione per chiavi pubbliche, per fornire la convalida, e di chiavi basate sull'hardware, per effettuare i processi crittografici necessari.

Abbinamento sicuro

Prima che Magic Keyboard con Touch ID possa essere utilizzata per operazioni con Touch ID, deve essere abbinata in modo sicuro al Mac. Per eseguire l'abbinamento, il processore Secure Enclave sul Mac e il blocco di accelerazione per chiavi pubbliche nella tastiera Magic Keyboard con Touch ID scambiano delle chiavi pubbliche, con radice nell'autorità di certificazione attendibile Apple, e utilizzano chiavi di convalida legate all'hardware e chiavi effimere ECDH per convalidare in modo sicuro la propria identità. Sul Mac, tali dati sono protetti da Secure Enclave; su Magic Keyboard con Touch ID, tali dati sono protetti dal blocco di accelerazione per chiavi pubbliche. Una volta eseguito l'abbinamento sicuro, tutti i dati comunicati tra il Mac e Magic Keyboard tramite Touch ID vengono crittografati tramite AES-GCM, con lunghezza chiave di 256 bit e chiavi ECDH effimere che utilizzano la curva NIST P-256 basate sulle identità archiviate. Per ulteriori informazioni sull'uso della tastiera Magic Keyboard in modalità wireless, consulta Sicurezza del Bluetooth.

Rilevamento dell'intenzione per l'abbinamento sicuro

Per eseguire alcune operazioni con Touch ID per la prima volta, come la registrazione di una nuova impronta digitale, l'utente deve confermare fisicamente la propria intenzione di utilizzare Magic Keyboard con Touch ID con il Mac. L'intenzione viene confermata fisicamente premendo due volte il tasto di accensione del Mac quando indicato dall'interfaccia utente oppure ottenendo il riconoscimento di un'impronta digitale che era stata precedentemente registrata con il Mac. Per ulteriori informazioni, consulta Rilevamento sicuro dell'intenzione e collegamenti a Secure Enclave.

Le transazioni di Apple Pay possono essere autorizzate con il riconoscimento di un'impronta digitale con Touch ID oppure inserendo la password utente di macOS e premendo due volte il tasto Touch ID di Magic Keyboard con Touch ID. L'ultima opzione consente all'utente di confermare fisicamente l'intenzione anche senza il riconoscimento di un'impronta da parte di Touch ID.

Sicurezza del canale di comunicazione per Magic Keyboard con Touch ID

Per aiutare a garantire un canale di comunicazione sicuro tra il sensore Touch ID di Magic Keyboard con Touch ID e Secure Enclave sul Mac abbinato, devono essere presenti i seguenti elementi:

- L'abbinamento sicuro tra il blocco di accelerazione per chiavi pubbliche di Magic Keyboard con Touch ID e Secure Enclave, come descritto sopra.
- Un canale sicuro tra il sensore di Magic Keyboard con Touch ID e il proprio blocco di accelerazione per chiavi pubbliche.

Il canale sicuro tra il sensore di Magic Keyboard con Touch ID e il proprio blocco di accelerazione per chiavi pubbliche deve essere stabilito in fabbrica utilizzando una chiave unica condivisa tra i due componenti. (Questa è la stessa tecnica utilizzata per creare il canale sicuro tra Secure Enclave sul Mac e un sensore Touch ID integrato sul computer).

Face ID, Touch ID, codici e password

Per poter utilizzare Face ID o Touch ID, l'utente deve configurare il dispositivo in maniera tale che sia richiesta una password per sbloccarlo. Quando Face ID o Touch ID rilevano una corrispondenza corretta, il dispositivo dell'utente si sblocca senza chiedere l'inserimento del codice. In questo modo l'utilizzo di un codice o una password più lunghi e complessi diventa più pratico che mai, perché gli utenti non dovranno inserirli spesso. Face ID e Touch ID non sostituiscono il codice o la password degli utenti, ma forniscono un accesso semplice al dispositivo entro limiti e soglie temporali appositamente pensati. Si tratta di un aspetto importante, perché una password o un codice sicuri costituiscono la base della protezione crittografica dei dati dell'utente su iPhone, iPad, Mac o Apple Watch.

Quando è obbligatorio utilizzare un codice o una password sul dispositivo

Gli utenti possono utilizzare il codice o la password in qualsiasi momento al posto di Face ID o di Touch ID, ma ci sono alcuni casi in cui l'autenticazione biometrica non è consentita. Le seguenti operazioni in cui la sicurezza ha particolare importanza richiedono sempre l'inserimento di un codice o di una password.

- Aggiornamento del software.
- Inizializzazione del dispositivo.
- Visualizzazione o modifica delle impostazioni del codice.
- Installazione di profili di configurazione.
- Sblocco del pannello "Privacy e sicurezza" in Impostazioni di Sistema (macOS 13 o versioni successive).
- Sblocco del pannello "Sicurezza e Privacy" in Preferenze di Sistema (macOS 12 o versioni precedenti).
- Sblocco del pannello "Utenti e gruppi" di Impostazioni di Sistema (macOS 13 o versioni successive) sul Mac (se è attivo FileVault).
- Sblocco del pannello "Utenti e Gruppi" in Preferenze di Sistema (macOS 12 o versioni precedenti) sul Mac (se è attivo FileVault).

Il codice o la password sono richiesti anche quando il dispositivo si trova in uno dei seguenti stati:

- Il dispositivo è stato appena acceso o riavviato.
- L'utente ha eseguito il logout dal suo account sul Mac (o non ha ancora eseguito il login).
- L'utente non sblocca il dispositivo da più di 48 ore.
- L'utente non utilizza il codice o la password per sbloccare il dispositivo da 156 ore (sei giorni e mezzo) e non utilizza l'autenticazione biometrica per sbloccare il dispositivo da 4 ore.
- Il dispositivo ha ricevuto un comando di blocco da remoto.
- L'utente è uscito dalla schermata Spegni/SOS emergenze tenendo premuti contemporaneamente uno dei tasti volume e il tasto Standby/Riattiva per due secondi e premendo quindi Annulla.
- Sono stati effettuati cinque tentativi non corretti di rilevamenti biometrici (sebbene per l'usabilità, dopo un numero inferiore di tentativi non andati a buon fine il dispositivo potrebbe richiedere all'utente di inserire il codice o la password invece di utilizzare i rilevamenti biometrici).

Quando Face ID con mascherina è abilitato su iPhone, sarà disponibile per le successive 6,5 ore dopo che l'utente ha svolto una delle azioni seguenti:

- Tentativo di riconoscimento Face ID riuscito (con o senza mascherina).
- Convalida del codice del dispositivo.
- Sblocco del dispositivo con Apple Watch.

Quando una qualsiasi di queste azioni viene eseguita, il periodo si estende di altre 6,5 ore.

Quando Face ID o Touch ID sono abilitati su iPhone o iPad, il dispositivo si blocca immediatamente quando viene premuto il tasto Standby/Riattiva e ogni volta che entra in standby. Face ID e Touch ID richiedono una corrispondenza corretta (o facoltativamente il codice) a ogni riattivazione.

La possibilità che un'altra persona possa sbloccare casualmente l'iPhone o l'iPad di un utente è inferiore a una su 1.000.000 con Face ID, anche quando Face ID con mascherina è attivato. Mentre per i modelli di iPhone, iPad, Mac con Touch ID e quelli abbinati a una Magic Keyboard, è inferiore a una su 50.000. Questa probabilità diminuisce se si registrano più impronte digitali (fino a 1 su 10.000 con cinque impronte digitali) o più fisionomie (fino a 1 su 500.000 con due fisionomie). Come forma di protezione ulteriore, sia Face ID che Touch ID consentono solo cinque tentativi di riconoscimento non riusciti prima di richiedere un codice o una password per consentire l'accesso al dispositivo o account dell'utente. Con Face ID, la probabilità di un falso riconoscimento aumenta con:

- Gemelli e fratelli o sorelle che hanno lo stesso aspetto dell'utente.
- Bambini di età inferiore ai 13 anni, i cui tratti del volto potrebbero non essere ancora completamente sviluppati.

La probabilità di un falso riconoscimento aumenta ulteriormente negli ultimi due casi quando viene utilizzato Face ID con mascherina. Se ciò rappresenta motivo di preoccupazione, Apple consiglia di utilizzare un codice per l'autenticazione.

Sicurezza del riconoscimento facciale

Il riconoscimento facciale viene eseguito all'interno di Secure Enclave tramite reti neurali preparate appositamente per tale scopo. Apple ha sviluppato le reti neurali per il riconoscimento facciale utilizzando oltre un miliardo di immagini, comprese immagini ad infrarossi e immagini 3D, raccolte in studi condotti con il consenso informato dei partecipanti. Apple ha lavorato quindi con partecipanti di tutto il mondo per includere un gruppo rappresentativo di individui tenendo in considerazione genere, età, etnia e altri fattori. Gli studi sono stati appositamente ampliati per fornire un alto grado di precisione per una ricca varietà di utenti. Face ID è progettato per funzionare con cappelli, sciarpe, occhiali, lenti a contatto e molti tipi di occhiali da sole, A partire da iPhone 12 e da iOS 15.4 versioni successive, Face ID supporta lo sblocco del dispositivo anche quando viene indossata una mascherina, nonché per funzionare al chiuso, all'aperto e persino totalmente al buio. Una rete neurale aggiuntiva, preparata per individuare e impedire la falsificazione, protegge contro i tentativi di sbloccare il dispositivo con foto o maschere. I dati di Face ID, comprese le rappresentazioni matematiche del volto dell'utente, sono codificati e disponibili solo per Secure Enclave. Questi dati non escono mai dal dispositivo: non vengono inviati ad Apple e non vengono inclusi nei backup del dispositivo. I dati di Face ID salvati e codificati per l'utilizzo esclusivo da parte di Secure Enclave durante il normale funzionamento sono i seguenti:

- Le rappresentazioni matematiche del volto dell'utente calcolate durante la registrazione.
- Le rappresentazioni matematiche del volto dell'utente calcolate durante alcuni tentativi di sblocco se Face ID le reputa utili a migliorare i riconoscimenti futuri.

Le immagini del volto rilevate durante il normale funzionamento non vengono salvate e vengono eliminate immediatamente dopo il calcolo delle rappresentazioni matematiche per la registrazione o per il confronto con i dati di Face ID registrati.

Miglioramento del riconoscimento facciale di Face ID

Per migliorare le prestazioni del riconoscimento e restare al passo con i cambiamenti naturali del volto dell'utente, con il tempo Face ID incrementa le rappresentazioni matematiche archiviate. In seguito a un riconoscimento riuscito, Face ID potrebbe utilizzare le rappresentazioni matematiche appena calcolate (se la qualità è sufficiente) per un numero limitato di altri riconoscimenti, per poi eliminare tali dati. Se invece Face ID non riesce a riconoscere un volto, ma la qualità del riconoscimento è più alta di una determinata soglia e subito dopo viene inserito il codice, Face ID esegue immediatamente un altro rilevamento e incrementa i dati di Face ID registrati con la rappresentazione matematica appena calcolata. Questi nuovi dati di Face ID vengono eliminati se l'utente non risulta più corrispondente al volto registrato per il riconoscimento facciale o dopo un numero finito di riconoscimenti; i nuovi dati vengono eliminati anche quando viene selezionata l'opzione per inizializzare Face ID. Questo processo aumentativo consente a Face ID di restare al passo con cambiamenti significativi sul volto dell'utente relativi a peli facciali o all'utilizzo del trucco, minimizzando al tempo stesso i riconoscimenti errati.

Utilizzi di Face ID e Touch ID

Sblocco di un dispositivo o di un account utente

Se Face ID o Touch ID non sono attivi, quando un dispositivo o un account si bloccano, vengono eliminate le chiavi per la classe più alta della protezione dati (archiviate in Secure Enclave). I file e gli elementi del portachiavi di quella classe non sono accessibili finché l'utente non sblocca il dispositivo o l'account inserendo il codice o la password.

Se Face ID o Touch ID sono attivati, le chiavi non vengono eliminate quando il dispositivo o l'account si bloccano, ma vengono invece cifrate tramite una chiave che viene fornita al sottosistema Face ID o Touch ID all'interno di Secure Enclave. Quando un utente prova a sbloccare il dispositivo o l'account, se il dispositivo o l'account rilevano una corrispondenza corretta, forniranno la chiave per decifrare le chiavi di protezione dati e saranno dunque sbloccati. Questo processo fornisce un'ulteriore protezione perché richiede la cooperazione tra i sottosistemi della protezione dati e di Face ID o Touch ID per sbloccare il dispositivo.

Quando il dispositivo si riavvia, le chiavi richieste per Face ID o Touch ID per lo sblocco del dispositivo o dell'account vanno perse: una volta soddisfatte le condizioni che richiedono l'inserimento del codice o della password vengono infatti scartate da Secure Enclave.

Acquisti protetti con Apple Pay

L'utente può utilizzare Face ID e Touch ID anche con Apple Pay per effettuare acquisti facili e sicuri nei negozi, nelle app e sul web.

- *Utilizzo di Face ID nei negozi:* per autorizzare un pagamento in un negozio con Face ID, l'utente dovrà prima confermare l'intenzione di pagare facendo doppio clic con il tasto laterale. Questo doppio clic rileva l'intenzione dell'utente tramite un gesto fisico collegato direttamente a Secure Enclave ed è a prova di contraffazione da parte di processi potenzialmente dannosi. L'utente quindi eseguirà l'autenticazione con Face ID prima di posizionare il dispositivo vicino al lettore per il pagamento contactless. Dopo l'autenticazione tramite Face ID, è possibile selezionare un altro metodo di pagamento di Apple Pay. Ciò richiede una nuova autenticazione, ma l'utente non dovrà premere di nuovo due volte il tasto laterale.
- *Utilizzo di Face ID nelle app e sul web:* per effettuare un pagamento all'interno delle app e sul web, l'utente conferma l'intenzione di pagare facendo doppio clic con il tasto laterale, quindi eseguirà l'autenticazione con Face ID per autorizzare il pagamento. Se la transazione di Apple Pay non viene completata entro 60 secondi dal momento in cui l'utente ha premuto due volte il tasto laterale, occorrerà confermare l'intenzione di pagare premendolo di nuovo due volte.
- *Utilizzo di Touch ID:* nel caso di Touch ID, l'intenzione di pagare è confermata dal gesto di attivazione del sensore di Touch ID, insieme alla corretta corrispondenza dell'impronta digitale dell'utente.

Utilizzare la API fornite dal sistema

Le app di terze parti possono utilizzare le API fornite dal sistema per richiedere l'autenticazione dell'utente tramite Face ID, Touch ID, un codice o una password; le app compatibili con Touch ID, supportano automaticamente anche Face ID senza alcun cambiamento. Quando vengono utilizzati Face ID o Touch ID, all'app viene notificata solo l'avvenuta autenticazione: non potrà accedere a Face ID, Touch ID né ad altri dati associati all'utente registrato.

Protezione degli elementi del portachiavi

Anche gli elementi del portachiavi possono essere protetti con Face ID o Touch ID e saranno sbloccati da Secure Enclave solo con una corrispondenza corretta o utilizzando il codice del dispositivo o la password dell'account. Gli sviluppatori di app dispongono di API per verificare che l'utente abbia impostato un codice o una password prima di richiedere l'uso di Face ID, Touch ID, di un codice o di una password per sbloccare gli elementi del portachiavi. Gli sviluppatori di app possono:

- Impedire che le operazioni dell'API di autenticazione ricorrano alla password di un'app o al codice del dispositivo e verificare che un utente sia registrato, consentendo l'utilizzo di Face ID o Touch ID come secondo fattore in app sensibili alla sicurezza.
- Generare e utilizzare chiavi ECC all'interno di Secure Enclave che possono essere protette da Face ID o Touch ID. Le operazioni con queste chiavi avvengono sempre all'interno di Secure Enclave dopo che Secure Enclave ne ha autorizzato l'uso.

Acquisti e approvazione degli acquisti

Gli utenti possono configurare Face ID o Touch ID anche per l'approvazione degli acquisti su iTunes Store, App Store e Apple Books, così non dovranno inserire la password dell'ID Apple. Quando vengono effettuati degli acquisti, Secure Enclave verifica che sia stata eseguita un'autorizzazione biometrica, quindi rilascia le chiavi ECC usate per firmare la richiesta del negozio.

Rilevamento sicuro dell'intenzione e collegamenti a Secure Enclave

Il rilevamento sicuro dell'intenzione fornisce un modo per confermare l'intenzione di un utente senza alcuna interazione con il sistema operativo o con il processore per le applicazioni. Il collegamento stabilito è di tipo fisico (da un tasto fisico a Secure Enclave) ed è disponibile sui seguenti dispositivi:

- iPhone X o modelli successivi
- Apple Watch Series 1 o modelli successivi
- iPad Pro (tutti i modelli)
- iPad Air (2020)
- Computer Mac dotati di chip Apple

Tramite questo collegamento, gli utenti possono confermare la propria intenzione di completare un'operazione tramite un meccanismo che nemmeno del software con privilegi root o nel kernel è in grado di imitare.

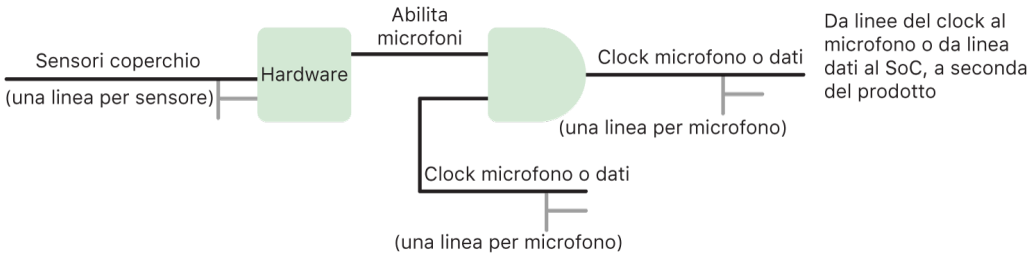
Questa funzionalità è utilizzata per confermare l'intenzione dell'utente durante le transazioni di Apple Pay e durante il completamento dell'abbinamento di Magic Keyboard con Touch ID con un Mac con chip Apple. La doppia pressione da parte dell'utente del tasto indicato (per Face ID) o la scansione di un'impronta digitale (per Touch ID) dall'interfaccia invia il segnale di conferma dell'intenzione dell'utente. Per ulteriori informazioni, consulta Acquisti protetti con Apple Pay. Un meccanismo simile, basato su Secure Enclave e sul firmware del chip T2, è supportato sui modelli di MacBook dotati di chip di sicurezza Apple T2 senza Touch Bar.

Scollegamento hardware del microfono

Tutti i Mac portatili dotati di chip Apple e i Mac portatili dotati di processore Intel con il chip di sicurezza Apple T2 prevedono uno scollegamento hardware che disabilita microfono quando viene chiuso lo schermo del computer. Su tutti i modelli da 13" di MacBook Pro e MacBook Air con chip T2, su tutti i portatili MacBook con chip T2 immessi sul mercato a partire dal 2019 e su tutti i portatili Mac dotati di chip Apple questo scollegamento è implementato solo a livello hardware. È un meccanismo progettato per impedire a qualsiasi software, anche dotato di privilegi di root o kernel in macOS e anche al software sul chip T2 o altro firmware, di collegarsi al microfono del computer quando lo schermo è chiuso (la fotocamera non è disconnessa nell'hardware perché con lo schermo chiuso il suo campo visivo è totalmente ostruito).

I modelli di iPad immessi sul mercato all'inizio del 2020 sono anch'essi dotati di uno scollegamento hardware del microfono. Quando viene collegata ad iPad una custodia compatibile con lo standard MFi (incluse quelle vendute da Apple) e viene chiusa, il microfono viene scollegato a livello hardware. Questo meccanismo è progettato per impedire che i dati audio del microfono vengano resi disponibili a qualsiasi software, anche con privilegi root o di kernel in iPadOS, o al firmware di qualsiasi dispositivo.

Le protezioni di questa sezione vengono implementate direttamente a livello hardware, secondo il seguente diagramma di circuito:



In ogni prodotto con scollegamento hardware del microfono, uno o più sensori rilevano una chiusura fisica dello schermo o della custodia tramite delle proprietà fisiche (ad esempio, effetto Hall o sensore dell'angolazione) dell'interazione. Per i sensori che necessitano di calibrazione, i parametri vengono impostati durante la produzione del dispositivo e il processo di calibrazione include un blocco hardware non reversibile che impedisce qualsiasi modifica successiva ai parametri fondamentali del sensore. Tali sensori emettono un segnale hardware diretto che passa attraverso un insieme semplice di componenti hardware non riprogrammabili. Tali componenti forniscono debounce, isteresi e/o un ritardo fino a 500 ms prima di disabilitare il microfono. A seconda del prodotto, il segnale può essere implementato disabilitando le linee che trasportano i dati tra il microfono e il SoC oppure disabilitando una delle linee di input verso il modulo del microfono che gli consente di essere attivo, come ad esempio la linea del clock o un simile controllo efficace.

Carte rapide in modalità “Basso consumo”

Se iOS non è in esecuzione perché iPhone necessita di essere caricato, potrebbe esserci energia sufficiente nella batteria per supportare le transazioni con le carte rapide trasporti. Gli iPhone compatibili supportano automaticamente questa funzionalità con:

- Una carta di pagamento o dei mezzi pubblici designata come carta rapida.
- I pass di accesso con la modalità rapida attivata.

Quando il tasto laterale viene premuto, l’icona della batteria mostra che la carica è bassa e il testo indica che le carte rapide possono essere utilizzate. Il controller NFC esegue le transazioni delle carte rapide trasporti con le stesse condizioni di quando iOS è in esecuzione, tranne per il fatto che le transazioni sono indicate solo con notifiche aptiche (non viene mostrata nessuna notifica visibile). Su iPhone SE (seconda generazione), le transazioni completate potrebbero impiegare alcuni secondi per comparire sullo schermo. Questa funzionalità non è disponibile in seguito a uno spegnimento standard da parte dell’utente.

Sicurezza del sistema

Panoramica della sicurezza del sistema

La sicurezza del sistema, costruita sulle funzionalità uniche dell'hardware Apple, è responsabile del controllo dell'accesso alle risorse del sistema nei dispositivi Apple senza comprometterne l'usabilità. La sicurezza del sistema agisce sul processo di avvio, sugli aggiornamenti software e sulla protezione delle risorse di sistema del computer come la CPU, la memoria, il disco, i programmi software e i dati archiviati.

Le versioni più recenti dei sistemi operativi Apple sono le più sicure. Una parte importante della sicurezza di Apple è l'*avvio protetto*, che rende sicuro il sistema contro infezioni da malware durante l'avvio. L'avvio protetto ha inizio nel chip e crea una catena di affidabilità tramite il software, in cui ogni passaggio è progettato per garantire il corretto funzionamento di quello successivo prima di cedergli il controllo. Questo modello di sicurezza supporta l'avvio di default dei dispositivi Apple così come le varie modalità di recupero e aggiornamento puntuale dei dispositivi Apple. Anche i sottocomponenti come Secure Enclave eseguono il proprio avvio protetto, per garantire di avviare solo codice affidabile proveniente da Apple. Il sistema di aggiornamento è progettato per impedire gli attacchi tramite downgrade, facendo in modo che i dispositivi non possano essere riportati a una versione precedente del sistema operativo (vulnerabile agli attacchi di hacker) al fine di sottrarre i dati dell'utente.

I dispositivi Apple sono inoltre dotati di protezione sia all'avvio che durante l'esecuzione dei processi, per garantirne l'integrità durante il funzionamento. I chip progettati da Apple su iPhone, iPad, Mac dotati di chip Apple, Apple Watch, Apple TV e HomePod forniscono un'architettura comune per proteggere l'integrità del sistema operativo. Inoltre, macOS fornisce un insieme espandibile e configurabile di funzionalità di protezione a supporto del diverso modello computazionale, oltre a funzionalità supportate su tutte le piattaforme hardware Mac.

Avvio protetto

Processo di avvio per i dispositivi iPhone e iPad

Ogni passo del processo di avvio contiene componenti che sono stati firmati digitalmente da Apple attraverso opportuna codifica per verificarne l'integrità e in modo tale che l'avvio proceda solo dopo aver verificato la catena di affidabilità. Tali componenti includono i bootloader, il kernel, le estensioni del kernel e il firmware del processore baseband per la connessione cellulare. Questa procedura di avvio protetto è progettata per verificare che i livelli più bassi del software non vengano alterati.

Quando un iPhone o iPad viene acceso, il processore per le applicazioni esegue immediatamente il codice dalla memoria di sola lettura conosciuta come ROM di avvio. Questo codice immutabile, conosciuto come *RoT (Root of Trust) hardware*, viene configurato durante la fabbricazione del chip ed è considerato implicitamente affidabile. Il codice della ROM di avvio contiene la chiave pubblica dell'autorità di certificazione root di Apple, utilizzata per verificare che il bootloader iBoot sia stato firmato da Apple prima di consentirne il caricamento. Questo è il primo passo della catena di affidabilità, in cui ogni passo verifica che quello successivo sia firmato da Apple. Dopo aver concluso le proprie attività, iBoot controlla ed esegue il kernel iOS o iPadOS. Per i dispositivi con processori A9 o serie A precedenti, viene caricata un'ulteriore fase bootloader di livello inferiore (LLB, Low-Level Bootloader) che viene verificata dalla ROM di avvio e che a sua volta carica e verifica iBoot.

Un mancato caricamento o una mancata verifica delle seguenti fasi vengono gestiti diversamente a seconda dell'hardware:

- *La ROM di avvio non riesce a caricare il bootloader di livello inferiore (dispositivi meno recenti):* modalità DFU (Device Firmware Upgrade)
- *LLB o iBoot:* modalità di recupero

In entrambi i casi, il dispositivo deve essere collegato al Finder (macOS 10.15 o versioni successive) o ad iTunes (macOS 10.14 o versioni precedenti) tramite USB e riportato alle impostazioni di fabbrica.

Il registro di avanzamento dell'avvio (BPR, Boot Progress Register) è utilizzato da Secure Enclave per limitare l'accesso ai dati dell'utente in diverse modalità e viene aggiornato prima di entrare nelle seguenti modalità:

- *modalità DFU:* impostata dalla ROM di avvio sui dispositivi con processori Apple A12 o SoC successivi.
- *modalità di recupero:* impostata da iBoot sui dispositivi con processori Apple A10, S2 o SoC successivi.

Sui dispositivi con accesso cellulare, un sottosistema baseband cellulare esegue un processo di avvio protetto aggiuntivo, usando software firmato e chiavi verificate dal processore baseband.

Anche Secure Enclave esegue un avvio protetto che verifica che il proprio software (sepOS) sia verificato e firmato da Apple.

Implementazione di iBoot per la protezione della memoria

In iOS 14 e iPadOS 14 o versioni successive, Apple ha modificato la toolchain per il compiler C utilizzato per eseguire la build del bootloader iBoot per migliorarne la sicurezza. La toolchain modificata implementa del codice che progettato per impedire problemi di sicurezza relativi alla memoria e ai tipi che sono diffusi nei programmi C. Ad esempio, aiuta a evitare gran parte delle vulnerabilità nelle seguenti classi:

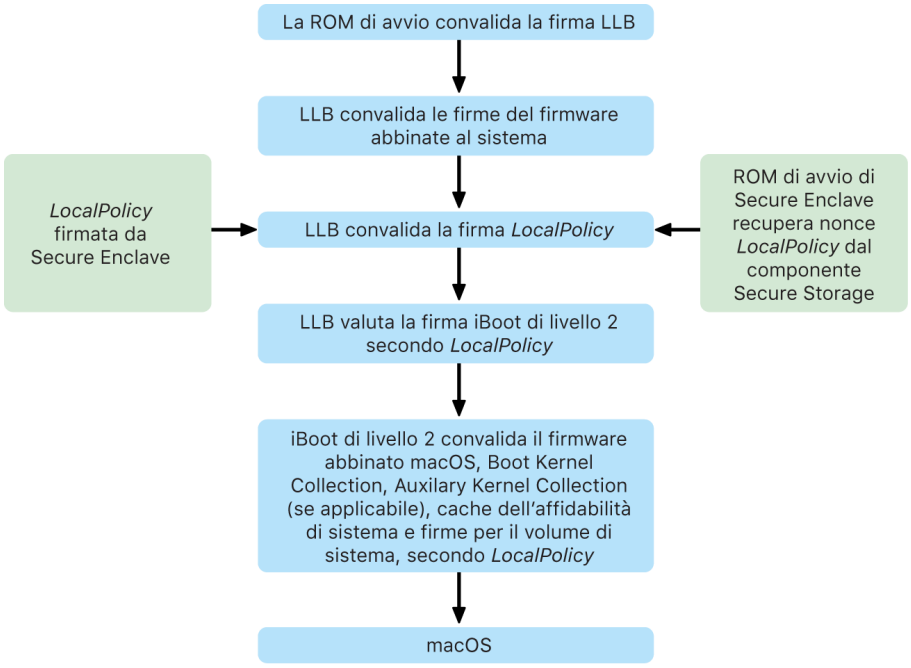
- Overflow del buffer, garantendo che tutti i puntatori contengano informazioni sui limiti che siano verificate quando accedono alla memoria.
- Sfruttamento degli heap, separando questi ultimi dai relativi metadati e rilevando accuratamente condizioni di errore come i double-free.
- Confusione dei tipi, garantendo che tutti i puntatori contengano informazioni sul tipo di runtime che siano verificate durante le operazioni di cast dei puntatori.
- Confusione dei tipi causata da errori use-after-free, isolando tutte le allocazioni di memoria dinamica per tipo statico.

Questa tecnologia è disponibile su iPhone con chip Apple A13 Bionic o modelli successivi e su iPad con chip A14 Bionic o modelli successivi.

Computer Mac dotati di chip Apple

Processo di avvio per i Mac dotati di chip Apple

Quando accendi un Mac dotato di chip Apple, viene eseguito un processo di avvio molto simile a quello di iPhone e iPad.



Nel primo passaggio della catena di attendibilità, il chip esegue del codice dalla ROM di avvio. L'avvio protetto di macOS sui Mac dotati di chip Apple verifica non solo il codice del sistema operativo stesso, ma anche le politiche di sicurezza e persino le estensioni del kernel (supportate, ma non consigliate) configurate dagli utenti autorizzati.

Quando l'LLB, ossia il bootloader di livello inferiore, viene avviato, esso verifica le firme e carica il firmware abbinato al sistema per i core intra-SoC, come l'archiviazione, il monitor, la gestione del sistema e i controller Thunderbolt. Il bootloader di livello inferiore è responsabile anche del caricamento di LocalPolicy, un file firmato da Secure Enclave. Il file LocalPolicy descrive la configurazione scelta dall'utente per le politiche per l'avvio del sistema e per la sicurezza dell'esecuzione. LocalPolicy ha lo stesso formato di struttura di dati di tutti gli altri oggetti di avvio, ma il file è firmato localmente da una chiave privata che è disponibile solo all'interno del Secure Enclave di un determinato computer, invece che essere firmato da un server centrale Apple (come gli aggiornamenti software).

Per impedire il riutilizzo di qualsiasi LocalPolicy precedente, il bootloader di livello inferiore deve cercare un valore anti-replay dal componente Secure Storage collegato a Secure Enclave. Per farlo, utilizza la ROM di avvio di Secure Enclave e si assicura che il valore anti-replay in LocalPolicy corrisponda a quello nel componente Secure Storage. Questa procedura aiuta a impedire che un LocalPolicy meno recente, che potrebbe essere stato configurato con un livello di sicurezza inferiore, venga riapplicato al sistema dopo che la sicurezza è stata aumentata. Il risultato è che l'avvio protetto sui Mac dotati di chip Apple aiuta a proteggere non solo contro l'uso di versioni precedenti del sistema operativo, ma anche contro l'applicazione di politiche di sicurezza meno severe.

Il file LocalPolicy rileva se il sistema operativo è configurato per garantire una sicurezza totale, ridotta o assente.

- *Sicurezza totale:* il sistema si comporta come iOS e iPadOS e consente solo l'avvio di software che risulta essere il più recente disponibile al momento dell'installazione.
- *Sicurezza ridotta:* al bootloader di livello inferiore viene permesso di ritenere affidabili le firme "globali" che sono incluse con il sistema operativo. Questo consente al sistema di eseguire versioni meno recenti di macOS. Dal momento che le versioni meno recenti di macOS presentano inevitabilmente vulnerabilità non risolte, questa modalità di sicurezza è definita come *ridotta*. Questo è anche il livello di sicurezza richiesto per supportare l'avvio di estensioni del kernel.
- *Sicurezza assente:* il sistema si comporta come in sicurezza ridotta per il fatto di utilizzare la verifica di firme globali per iBoot e oltre, ma inoltre consente ad iBoot di accettare che alcuni oggetti di avvio vengano firmati da Secure Enclave con la stessa chiave utilizzata per firmare LocalPolicy. Questo livello di sicurezza è pensato per gli utenti che si occupano di creazione, firma e avvio di kernel XNU personalizzati.

Se LocalPolicy indica al bootloader di livello inferiore che il sistema operativo è in esecuzione in sicurezza totale, il bootloader di livello inferiore valuta la firma personalizzata per iBoot. Se è in esecuzione in sicurezza ridotta o assente, valuta la firma globale. Qualsiasi errore di verifica della firma causa l'avvio del sistema in recoveryOS per offrire le dovute opzioni di riparazione.

Una volta che il bootloader di livello inferiore ha passato le operazioni ad iBoot, questo carica il firmware abbinato a macOS, come quello per il Secure Neural Engine, per il processore sempre attivo e altro firmware. iBoot esamina anche le informazioni riguardo a LocalPolicy fornite dal bootloader di livello inferiore. Se LocalPolicy indica che dovrebbe esserci una raccolta del kernel ausiliaria, iBoot la cerca nel file system, verifica che sia stata firmata da Secure Enclave con la stessa chiave di LocalPolicy e controlla che il relativo hash corrisponda a quello archiviato in quest'ultimo. Se la raccolta del kernel ausiliaria passa la verifica, iBoot la posiziona in memoria con la raccolta del kernel di avvio, prima di bloccare l'intera regione di memoria che copre la raccolta del kernel di avvio e la raccolta del kernel ausiliaria con la Protezione dell'integrità dei coprocessori di sistema (SCIP). Se la politica indica che dovrebbe essere presente una raccolta del kernel ausiliaria, ma questa non viene trovata, il sistema prosegue l'avvio in macOS senza di essa. iBoot è anche responsabile della verifica dell'hash root del volume di sistema firmato, per controllare che l'integrità del file system attivato dal kernel sia totalmente verificata.

Modalità di avvio per i Mac dotati di chip Apple

I Mac dotati di chip Apple dispongono delle modalità di avvio descritte di seguito.

Modalità	Combinazione di tasti	Descrizione
macOS	Dallo stato di spegnimento, premi e **rilascia** il tasto di alimentazione.	1. La ROM di avvio passa le operazioni al bootloader di livello inferiore. 2. Il bootloader di livello inferiore carica il firmware abbinato al sistema e il LocalPolicy per il tipo di macOS selezionato. 3. Il bootloader di livello inferiore blocca nel registro di avanzamento dell'avvio (BPR) un'indicazione del fatto che sta eseguendo l'avvio in macOS e passa le operazioni ad iBoot. 4. iBoot carica il firmware abbinato a macOS, la cache di affidabilità statica, la struttura ad albero del dispositivo e la raccolta del kernel di avvio. 5. Se LocalPolicy lo consente, iBoot carica la raccolta del kernel ausiliaria con le estensioni del kernel di terze parti. 6. Se LocalPolicy non lo consente, iBoot verifica l'hash della firma root per il volume di sistema firmato.
recoveryOS abbinato	Dallo stato di spegnimento, **tieni premuto** il tasto di alimentazione.	1. La ROM di avvio passa le operazioni al bootloader di livello inferiore. 2. Il bootloader di livello inferiore carica il firmware abbinato al sistema e il LocalPolicy per recoveryOS. 3. Il bootloader di livello inferiore blocca nel registro della procedura di avvio un'indicazione del fatto che sta eseguendo l'avvio nel recoveryOS abbinato e passa le operazioni a iBoot per il recoveryOS abbinato. 4. iBoot carica il firmware abbinato a macOS, la cache di affidabilità, la struttura ad albero del dispositivo e la raccolta del kernel di avvio. 5. Se l'avvio del recoveryOS abbinato non riesce, viene tentato l'avvio del recoveryOS alternativo.

Modalità	Combinazione di tasti	Descrizione
RecoveryOS alternativo	Dallo stato di spegnimento, **premi due volte e tieni premuto** il tasto di alimentazione.	1. La ROM di avvio passa le operazioni al bootloader di livello inferiore. 2. Il bootloader di livello inferiore carica il firmware abbinato al sistema e il LocalPolicy per recoveryOS. 3. Il bootloader di livello inferiore blocca nel registro della procedura di avvio un'indicazione del fatto che sta eseguendo l'avvio nel recoveryOS abbinato e passa le operazioni a iBoot per recoveryOS. 4. iBoot carica il firmware abbinato a macOS, la cache di affidabilità, la struttura ad albero del dispositivo e la raccolta del kernel di avvio.
Modalità sicura	Esegui l'avvio in recoveryOS come indicato sopra, quindi tieni premuto il tasto **Maiuscole** mentre selezioni il volume di avvio.	1. Viene eseguito l'avvio in recoveryOS come descritto sopra. 2. Premendo il tasto Maiuscole mentre si seleziona un volume, l'app BootPicker approva l'avvio di quel macOS, come avviene normalmente, e imposta anche una variabile `nvram` che indica ad iBoot di non caricare la raccolta del kernel ausiliaria all'avvio successivo. 3. Il sistema si riavvia utilizzando il volume scelto, ma i Boot non carica la raccolta del kernel ausiliaria.

Restrizioni applicate a recoveryOS abbinato

In macOS 12.0.1 o versioni successive, con ogni nuova installazione di macOS viene installata anche una versione abbinata di recoveryOS nel gruppo di volumi APFS corrispondente. Gli utenti dei Mac con processori Intel avranno familiarità con questo tipo di configurazione, ma sui Mac dotati del chip Apple, offre ulteriori garanzie di sicurezza e compatibilità. Il recoveryOS abbinato dedicato, che adesso è disponibile con ciascuna installazione di macOS, garantisce che soltanto il recoveryOS abbinato sia in grado di eseguire operazioni di downgrade della sicurezza. Questo consente di proteggere le installazioni delle versioni più recenti di macOS dalle intromissioni indesiderate che sono avvenute nelle versioni precedenti di macOS e viceversa.

Le restrizioni all'abbinamento vengono applicate come segue:

- Tutte le installazioni di macOS 11 sono abbinate a recoveryOS. Se un'installazione di macOS 11 viene selezionata per l'avvio di default, su un Mac con il chip Apple, è possibile avviare recoveryOS tenendo premuto il tasto dell'accensione al momento dell'avvio. recoveryOS è in grado di effettuare il downgrade delle impostazioni di sicurezza di tutte le installazioni di macOS 11 ma non di tutte quelle di macOS 12.0.1.
- Se un'installazione di macOS 12.0.1 o versioni successive viene selezionata per l'avvio di default, è possibile avviare il recoveryOS abbinato tenendo premuto il tasto dell'accensione al momento dell'avvio del Mac. Il recoveryOS abbinato è in grado di effettuare il downgrade dell'installazione di macOS abbinata ma non di tutte le altre installazioni di macOS.

Per poter avviare qualsiasi installazione di macOS nel recoveryOS abbinato, l'installazione deve essere selezionata come quella di default. Per eseguire questa operazione, vai in Generali > Disco di avvio in Impostazioni di Sistema (macOS 13 o versioni successive), Disco di Avvio in Preferenze di Sistema (macOS 12 o versioni precedenti) oppure avvia un recoveryOS qualsiasi tenendo premuto il tasto Opzione, mentre viene selezionato un volume.

Nota: il recoveryOS alternativo non è in grado di effettuare downgrade per nessuna installazione di macOS.

Controllo delle politiche di sicurezza per il disco di avvio per i Mac dotati di chip Apple

Panoramica

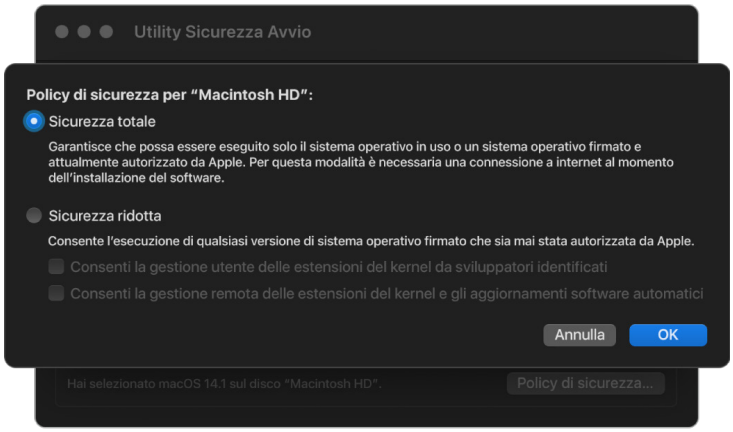
A differenza delle politiche di sicurezza per i Mac dotati di processore Intel, quelle per i Mac dotati di chip Apple sono specifiche per ciascun sistema operativo installato. Ciò significa che su uno stesso Mac è supportata l'installazione di più istanze di macOS con diverse versioni e politiche di sicurezza. Per questo motivo in Utility Sicurezza Avvio è stato aggiunto un *selettore del sistema operativo*.

Sui Mac dotati di chip Apple, Utility Sicurezza Avvio indica lo stato di sicurezza globale di macOS configurato dall'utente, come l'avvio di un'estensione del kernel o la configurazione della protezione dell'integrità del sistema. Se la modifica di un'impostazione di sicurezza dovesse andare a ridurre considerevolmente la sicurezza o dovesse rendere più facile la compromissione del sistema, l'utente dovrà entrare in recoveryOS tenendo premuto il tasto di alimentazione (in modo tale che il segnale non possa essere attivato da un software dannoso, ma solo da un umano tramite un accesso fisico) per effettuare la modifica. Per questo motivo, un Mac dotato di chip Apple non richiederà (o supporterà) una password del firmware, perché tutte le modifiche importanti sono già protette tramite l'autorizzazione da parte dell'utente. Per ulteriori informazioni sulla protezione dell'integrità del sistema, consulta Protezione dell'integrità del sistema.

La sicurezza totale e ridotta possono essere impostate utilizzando Utility Sicurezza Avvio da recoveryOS. Invece è possibile accedere alla sicurezza assente solo tramite strumenti a riga di comando, da utenti che accettano il rischio di rendere il proprio Mac molto meno sicuro.

Politica “Sicurezza totale”

L’opzione “Sicurezza totale” è quella impostata di default e si comporta come iOS e iPadOS. Nel momento in cui il software viene scaricato e preparato per l’installazione, invece di utilizzare la firma globale fornita con il software, macOS contatta lo stesso server di firma Apple utilizzato per iOS e iPadOS e richiede una nuova firma “personalizzata”. Una firma viene definita “personalizzata” quando include l’ECID (Exclusive Chip Identification) come parte della richiesta di firma, ossia un ID unico in questo caso specifico per la CPU Apple. La firma restituita dal server di firma è quindi unica e utilizzabile solo da quella CPU Apple in concreto. Quando è in vigore la politica “Sicurezza totale”, la ROM di avvio e il bootloader di livello inferiore aiutano a garantire che una determinata firma non sia solo di Apple, ma anche creata appositamente per quel Mac, vincolando quella versione di macOS a quel Mac in concreto.

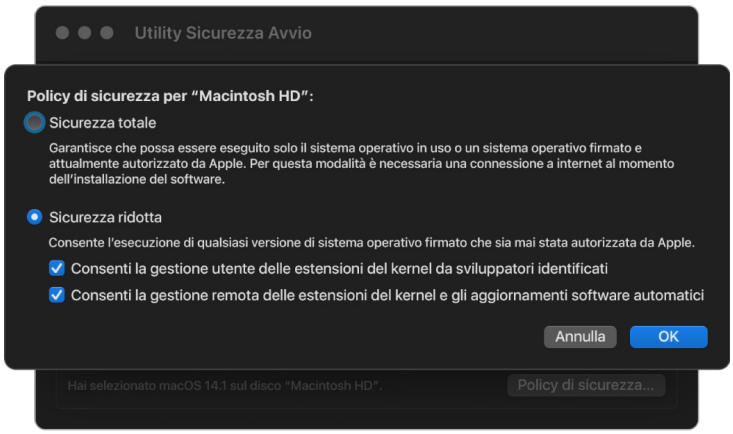


L’uso di un server di firma in linea fornisce inoltre una protezione migliore contro gli attacchi rollback rispetto alla firma globale tipica. In un sistema di firma globale, il periodo di sicurezza poteva essere riutilizzato molte volte, ma un sistema che non ha mai conosciuto il firmware più recente non lo saprà. Per esempio, un computer che attualmente crede di essere nel periodo di sicurezza 1 accetta software dal periodo di sicurezza 2 persino se il periodo di sicurezza attuale è 5. Con un sistema di firma in linea come quello usato con il chip Apple, il server di firma può rifiutare la creazione di firme per il software che non si trova nel periodo di sicurezza più recente.

Inoltre, se un hacker scopre una falla dopo la modifica di un periodo di sicurezza, non potrà semplicemente prendere il software vulnerabile di un periodo precedente dal sistema A e trasferirlo nel sistema B al fine di attaccarlo. Il fatto che il software vulnerabile di un periodo precedente sia stato personalizzato per il sistema A aiuta a impedirne il trasferimento e quindi l’uso per gli attacchi sul sistema B. Tutti questi meccanismi lavorano insieme per fornire fortissime garanzie che gli hacker non possano inserire deliberatamente del software vulnerabile su un Mac per eludere le protezioni fornite dal software più recente. Tuttavia, se un utente è in possesso di nome utente e password di amministratore di un Mac può comunque scegliere di impostare la politica di sicurezza che più si adatta alle sue esigenze.

Politica “Sicurezza ridotta”

L’opzione “Sicurezza ridotta” è simile all’impostazione “Sicurezza media” dei Mac dotati di processore Intel con chip T2, in cui un fornitore (in questo caso Apple) genera una firma digitale per il codice per dichiarare che questo proviene dal fornitore stesso. Questo meccanismo aiuta a impedire agli hacker di inserire del codice non firmato. Apple definisce tale firma come “globale”, perché può essere utilizzata su qualsiasi Mac e per qualunque durata di tempo per i Mac su cui è impostata la politica “Sicurezza ridotta”. Di per sé, l’opzione “Sicurezza ridotta” non fornisce protezione contro gli attacchi rollback. Tuttavia, le modifiche non autorizzate al sistema operativo possono far sì che i dati dell’utente vengano resi inaccessibili. Per ulteriori informazioni, consulta Estensioni del kernel sui Mac dotati di chip Apple.

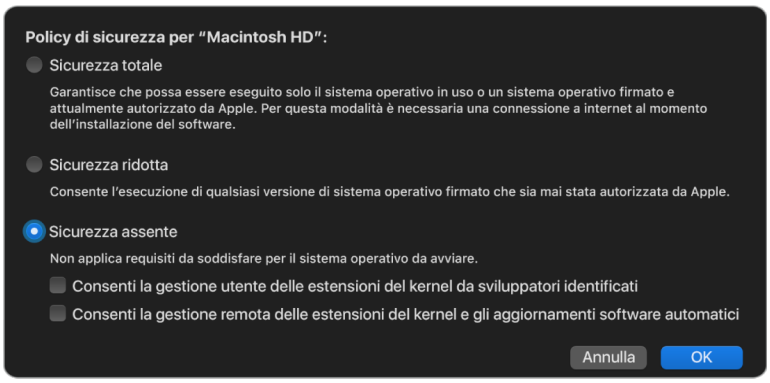


Oltre a consentire agli utenti l’esecuzione di versioni meno recenti di macOS, la sicurezza ridotta è richiesta anche per altre azioni che possono mettere a rischio la sicurezza del sistema dell’utente, come l’introduzione di estensioni del kernel di terze parti. Le estensioni del kernel hanno gli stessi privilegi del kernel, quindi eventuali vulnerabilità nelle estensioni di terze parti possono causare una compromissione dell’intero sistema operativo. Questo è il motivo per cui gli sviluppatori sono fortemente incoraggiati ad adottare le estensioni di sistema, prima che il supporto per le estensioni del kernel venga rimosso da macOS per i Mac futuri dotati di chip Apple. Anche quando le estensioni del kernel sono abilitate, non possono essere caricate nel kernel su richiesta. Esse vengono invece incluse in una raccolta del kernel ausiliaria, il cui hash viene archiviato in LocalPolicy, rendendo quindi necessario un riavvio. Per ulteriori informazioni sulla generazione della raccolta del kernel ausiliaria, consulta Estensione sicura del kernel in macOS.

Politica “Sicurezza assente”

L’opzione “Sicurezza assente” è riservata agli utenti che accettano il rischio di impostare il proprio Mac in uno stato molto meno sicuro. Questa modalità è uguale all’opzione “Nessuna sicurezza” sui Mac dotati di processore Intel con chip T2. Con l’opzione “Sicurezza assente”, la verifica della firma viene comunque effettuata sull’intera catena di avvio protetto, ma impostando tale politica si indica ad iBoot di accettare oggetti di avvio firmati localmente da Secure Enclave, come una raccolta del kernel di avvio generata dall’utente, creata da un kernel XNU personalizzato. In questo modo, la politica “Sicurezza assente” fornisce anche la possibilità a livello strutturale di eseguire un kernel di un sistema operativo totalmente non autorizzato. Quando una raccolta del kernel di avvio personalizzata o un sistema operativo non attendibile vengono caricati sul sistema, alcune chiavi di decrittografia diventano non disponibili. Questo meccanismo è progettato per impedire a un sistema operativo non attendibile di accedere ai dati di sistemi operativi attendibili.

Importante: Apple non fornisce né supporta i kernel XNU personalizzati.



È presente un’ulteriore differenza tra “Sicurezza assente” e l’opzione “Nessuna sicurezza” dei Mac dotati di processore Intel con chip T2: si tratta di un prerequisito per alcune riduzioni della sicurezza che in passato sono state controllabili in modo indipendente. In particolare, per disabilitare la protezione dell’integrità del sistema sui Mac dotati di chip Apple, l’utente deve riconoscere che sta impostando il sistema su “Sicurezza assente”. Ciò è richiesto perché la disabilitazione della protezione dell’integrità del sistema ha sempre comportato l’impostazione del sistema in uno stato che rende molto più facile la compromissione del kernel. In particolare, se si disabilita la protezione dell’integrità del sistema sui Mac dotati di chip Apple, viene disabilitata la richiesta di firma per le estensioni del kernel durante la generazione della raccolta del kernel ausiliaria, consentendo quindi a qualsiasi estensione arbitraria di essere caricata nella memoria del kernel. Un altro miglioramento riguardante la protezione dell’integrità del sistema sui Mac dotati di chip Apple è che l’archiviazione della politica è stata spostata fuori dalla memoria NVRAM e all’interno di LocalPolicy. Quindi adesso la disabilitazione della protezione dell’integrità del sistema richiede l’autenticazione da parte di un utente che abbia accesso alla chiave per la firma di LocalPolicy, operazione effettuata da recoveryOS (accessibile tenendo premuto il tasto di alimentazione). Ciò rende significativamente più difficile per un hacker che esegue un attacco solo tramite software o persino per un hacker fisicamente presente, di disabilitare la protezione dell’integrità del sistema.

Non è consentito ridurre la sicurezza a “Sicurezza assente” dall’app Utility Sicurezza Avvio. Gli utenti possono ridurre il livello di sicurezza solo eseguendo strumenti a riga di comando da Terminale in recoveryOS, come `csrutil` (per disabilitare la protezione dell’integrità del sistema). Una volta eseguita la riduzione della sicurezza, ciò è visibile in Utility Sicurezza Avvio, quindi l’utente può impostare la sicurezza su un livello più alto.

Nota: i Mac dotati di chip Apple non richiedono né supportano una politica di avvio da supporto specifica perché tecnicamente tutti gli avvii vengono eseguiti localmente. Se un utente sceglie di eseguire l'avvio da un supporto esterno, tale versione del sistema operativo deve essere prima personalizzata tramite un riavvio autenticato da recoveryOS. Tale riavvio crea un file LocalPolicy sull'unità interna che viene usato per eseguire un avvio attendibile dal sistema operativo archiviato sul supporto esterno. Questo significa che la configurazione di un avvio dal supporto esterno è sempre abilitata esplicitamente per ciascun sistema operativo e richiede già l'autorizzazione dell'utente, quindi non è necessaria nessuna configurazione di sicurezza aggiuntiva.

Creazione e gestione della chiave per la firma di LocalPolicy

Creazione

Quando macOS viene installato per la prima volta in fabbrica o quando viene effettuata un'inizializzazione e installazione tramite tethering, il Mac esegue del codice da un disco RAM di ripristino temporaneo per inizializzare lo stato di default. Durante questo processo, l'ambiente di ripristino crea una nuova coppia di chiavi (una chiave pubblica e una chiave privata) che vengono conservate in Secure Enclave. La chiave privata viene chiamata *Owner Identity Key (OIK)*. Se esiste già una OIK, questa viene cancellata durante il processo. L'ambiente di ripristino inizializza anche la chiave utilizzata per il blocco attivazione, chiamata *User Identity Key (UIK)*. Una parte del processo che è esclusiva per i Mac on chip Apple è la richiesta della certificazione della UIK per il blocco attivazione, incluso un insieme di restrizioni obbligatorie che vengono implementate durante la convalida su LocalPolicy. Se il dispositivo non è in grado di ottenere una UIK certificata per il blocco attivazione (ad esempio, perché il dispositivo è attualmente associato a un account di "Trova il mio Mac" ed è segnalato come smarrito), il processo non può continuare con la creazione di un LocalPolicy. Se per il dispositivo è stato emesso un *User identity Certificate (ucrt)*, tale certificato ucrt contiene restrizioni imposte dal server e restrizioni richieste dall'utente in estensione X.509 v3.

Quando un `ucrt` per il blocco attivazione viene ricevuto correttamente, viene archiviato in un database sul server e viene restituito al dispositivo. Una volta che il dispositivo ha ricevuto un certificato ucrt, viene inviata alla *BBA (Basic Attestation Authority)* una richiesta di verifica per la chiave pubblica che corrisponde alla OIK. La BBA verifica la richiesta di certificazione della OIK tramite la chiave pubblica del certificato ucrt archiviato nel database accessibile alla BBA. Se la BBA riesce a verificare la certificazione, la chiave pubblica viene certificata, restituendo il certificato *OIC (Owner Identity Certificate)*, firmato dalla BBA e contenente le restrizioni archiviate nel certificato ucrt. Il certificato OIC viene inviato a Secure Enclave. Da questo momento, ogni volta che Secure Enclave firma un nuovo LocalPolicy, allega il certificato OIC al file Image4. Il bootloader di livello inferiore è dotato di un'attendibilità integrata nel certificato root della BBA; ciò fa in modo che la BBA consideri attendibile il certificato OIC, che a sua volta considererà attendibile la firma globale di LocalPolicy.

Restrizioni di RemotePolicy

Tutti i file Image4 (non solo LocalPolicy) contengono restrizioni per la valutazione del manifesto Image4. Tali restrizioni sono codificate tramite identificativi oggetto speciali nel certificato leaf. La libreria per la verifica del file Image4 cerca l'identificativo oggetto speciale per la restrizione in un certificato durante la valutazione della firma, quindi valuta meccanicamente le restrizioni specificate al suo interno. Le restrizioni hanno la forma:

- X deve esistere
- X non deve esistere
- X deve avere un valore specifico

Quindi, ad esempio, per le firme "personalizzate", le restrizioni del certificato conterranno "L'ECID deve esistere" e per le firme "globali", conterranno "L'ECID non deve esistere". Queste restrizioni sono progettate per garantire che tutti i file Image4 firmati da una certa chiave siano conformi a determinati requisiti, per evitare la generazione di manifesti Image4 firmati in modo errato.

Nel contesto di ciascun LocalPolicy, queste restrizioni relative ai certificati vengono chiamate *RemotePolicy*. Può esistere un RemotePolicy diverso per diversi LocalPolicy degli ambienti di avvio. Il RemotePolicy viene usato per limitare il LocalPolicy di recoveryOS in modo tale che, quando quest'ultimo viene avviato, possa comportarsi esclusivamente come se l'avvio avvenisse in modalità "Sicurezza totale". Ciò aumenta l'affidabilità dell'integrità di recoveryOS, come ambiente di avvio in cui le politiche possono essere modificate. RemotePolicy verifica che LocalPolicy contenga l'ECID del Mac in cui quest'ultimo è stato generato e il valore `rpnh` (Remote Policy Nonce Hash) specifico archiviato nel componente Secure Storage su tale Mac. Il valore `rpnh`, e quindi RemotePolicy, cambia solo quando vengono effettuate azioni relative a "Trova il mio Mac" e al blocco attivazione, come la registrazione, la revoca della registrazione, il blocco da remoto e la cancellazione remota. Le restrizioni di RemotePolicy sono determinate e specificate al momento della certificazione della chiave UIK e vengono firmate nel certificato ucrt emesso. Alcune restrizioni di RemotePolicy, come quelle relative a ECID, ChipID e BoardID, sono determinate dal server. Questo meccanismo è progettato per impedire a un dispositivo di firmare i file LocalPolicy di un altro dispositivo. Altre restrizioni di RemotePolicy possono essere specificate dal dispositivo, per aiutare a impedire l'uso di un livello di sicurezza inferiore per LocalPolicy senza fornire l'autenticazione locale richiesta per accedere alla OIK attuale e l'autenticazione remota dell'account a cui il dispositivo è collegato per il blocco attivazione.

Contenuti del file LocalPolicy per i Mac dotati di chip Apple

LocalPolicy è un file Image4 firmato da Secure Enclave. Image4 è un formato di struttura di dati ASN.1 (Abstract Syntax Notation One) con codifica DER che è anche usato per descrivere le informazioni degli oggetti della catena di avvio protetto sulle piattaforme Apple. In un modello di avvio protetto basato su Image4, le politiche di sicurezza sono richieste durante l'installazione del software, tramite una richiesta di firma su un server di firma centrale di Apple. Se la politica risulta accettabile, il server restituisce un file Image4 firmato, contenente una serie di sequenze di codici di 4 caratteri. Tali file Image4 firmati e i codici di 4 caratteri vengono valutati durante l'avvio da software come la ROM di avvio o il bootloader di livello inferiore.

Passaggio di proprietà tra sistemi operativi

L'accesso alla chiave OIK è conosciuto come "proprietà". La proprietà è richiesta per consentire agli utenti di firmare nuovamente il LocalPolicy dopo aver effettuato modifiche alle politiche o al software. La OIK è protetta tramite la stessa gerarchia di chiavi descritta in Protezione SKP (Sealed Key Protection): la OIK è protetta dalla stessa chiave di codifica delle chiavi della chiave di codifica per il volume. Ciò significa che è normalmente protetta sia delle password dell'utente che dalle misurazioni del sistema operativo e dalle politiche di protezione. Sul Mac è presente una singola OIK per tutti i sistema operativi. Quindi, quando si installa un secondo sistema operativo, è richiesto un consenso esplicito da parte degli utenti del primo sistema operativo per passare la proprietà agli utenti del secondo. Tuttavia, gli utenti del secondo sistema operativo ancora non esistono quando il programma di installazione viene eseguito dal primo sistema operativo. Gli utenti del sistema operativo normalmente non vengono generati finché questo non viene avviato e Impostazione Assistita non è in esecuzione. Quindi sono necessarie due nuove azioni quando si installa un secondo sistema operativo su un Mac dotato di chip Apple.

- Creare un LocalPolicy per il secondo sistema operativo.
- Preparare un "utente di installazione" per il passaggio della proprietà.

Quando si esegue un'installazione assistita e si usa come destinazione un volume secondario vuoto, all'utente viene chiesto se vuole copiare un utente dal volume attuale per fare da primo utente nel secondo volume. Se l'utente accetta, l'utente di installazione che viene creato è, in realtà, una chiave di codifica delle chiavi derivata dalla password dell'utente e dalle chiavi hardware, che viene successivamente usata per codificare la OIK mentre viene passata al secondo sistema operativo. Successivamente, nell'installazione assistita del secondo sistema operativo, viene richiesta la password di tale utente, per consentire l'accesso alla OIK in Secure Enclave per il nuovo sistema operativo. Se l'utente non accetta di copiare un utente, l'utente di installazione viene creato nello stesso modo, ma viene usata una password vuota invece della password di un utente. Questa seconda procedura è pensata per determinate situazioni legate all'amministrazione del sistema. Tuttavia, per gli utenti che desiderano avere installazioni su più volumi e vogliono eseguire il passaggio della proprietà nel modo più sicuro, è consigliabile accettare sempre di copiare un utente dal primo sistema operativo sul secondo sistema operativo.

LocalPolicy sui Mac dotati di chip Apple

Nei Mac dotati di chip Apple, il controllo delle politiche di sicurezza locali è stato delegato a un'app in esecuzione su Secure Enclave. Tale software può usare le credenziali dell'utente e la modalità di avvio della CPU principale per determinare chi può modificare la politica di sicurezza e da quale ambiente di avvio. Ciò aiuta a impedire a software dannoso di utilizzare i controlli della politica di sicurezza contro l'utente, riducendoli per poter ottenere maggiori privilegi.

Proprietà del manifesto LocalPolicy

Il file LocalPolicy contiene alcuni codici di 4 caratteri strutturali che sono presenti in quasi tutti i file Image4, come BORD (che indica una scheda o un ID modello), CHIP (che indica un particolare chip Apple) o ECID (l'identificatore unico del processore). I seguenti codici di 4 caratteri invece si concentrano solo sulle politiche di sicurezza che possono essere configurate dall'utente.

Nota: Apple utilizza la sigla *1TR (Paired One True recoveryOS)* per indicare l'avvio in recoveryOS abbinato, che si ottiene tenendo premuto una volta il tasto di alimentazione fisico. Questo è diverso da un avvio in recoveryOS ordinario, che avviene tramite la NVRAM oppure premendo due volte e poi tenendo premuto il tasto di alimentazione fisico; in alternativa, può avvenire quando si verificano degli errori durante l'avvio. Una determinata pressione fisica del tasto aumenta la certezza che l'ambiente di avvio non sia raggiungibile da un hacker che esegue un attacco solo tramite software e che ha ottenuto l'accesso a macOS.

Hash del nonce di LocalPolicy (lpnh)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* Il nonce `lpnh` viene usato per impedire il riutilizzo di LocalPolicy. Si tratta di un hash SHA384 del nonce di LocalPolicy che viene archiviato nel componente Secure Storage ed è accessibile tramite la ROM di avvio di Secure Enclave o tramite Secure Enclave. L'effettivo valore anti-replay non è mai visibile al processore per le applicazioni, ma può essere visto solo dal sistema operativo Secure Enclave. Un hacker che vuole convincere il bootloader di livello inferiore che un LocalPolicy precedente di cui si è impossessato era valido dovrebbe posizionare un valore nel componente Secure Storage che produca un hash verso lo stesso valore `lpnh` trovato nel LocalPolicy che vuole riutilizzare. Normalmente si ha un singolo nonce di LocalPolicy valido, tranne durante gli aggiornamenti software, quando ce ne sono due validi simultaneamente, per consentire la possibilità di riavviare il software meno recente in caso di un errore di aggiornamento. Quando qualsiasi LocalPolicy per qualsiasi sistema operativo viene modificato, tutte le politiche vengono nuovamente firmate con il nuovo valore *lpnh* corrispondente al nuovo nonce della politica locale trovato nel componente Secure Storage. Questa modifica avviene quando un utente modifica le impostazioni di sicurezza o crea nuovi sistemi operativi, ciascuno con un nuovo LocalPolicy.

Hash del nonce della politica remota (rpnh)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* Il nonce `rpnh` si comporta allo stesso modo di `lpnh`, ma si aggiorna solo quando viene aggiornata la politica remota, come ad esempio quando si cambia lo stato della registrazione di Dov'è. Questa modifica avviene quando l'utente cambia lo stato di Dov'è sul Mac.

Hash del nonce di recoveryOS (ronh)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* Il nonce `ronh` si comporta allo stesso modo di <CodeBody>lpnh</CodeBody>, ma si trova esclusivamente nel LocalPolicy per il recoveryOS di sistema. Si aggiorna solo quando viene aggiornato il recoveryOS di sistema, ad esempio durante l'aggiornamento del software. Un valore anti-replay diverso da `lpnh` e `rpnh` viene usato affinché, quando un dispositivo viene disabilitato da Dov'è, i sistemi operativi possano essere disabilitati (rimuovendo i relativi LPN e RPN dal componente Secure Storage) ma il recoveryOS di sistema possa comunque essere avviato. In questo modo, i sistemi operativi possono essere riabilitati quando il proprietario del sistema dimostra di poterlo controllare inserendo la propria password di iCloud utilizzata per l'account di Dov'è. Questa modifica avviene quando un utente aggiorna il recoveryOS di sistema o crea nuovi sistemi operativi.

Hash del manifesto Image4 di fase successiva (nsih)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* Il campo *nsih* rappresenta un hash SHA384 della struttura di dati del manifesto che descrive la copia di macOS avviata. Il manifesto Image4 di macOS contiene misurazioni relative a tutti gli oggetti di avvio come iBoot, la cache di affidabilità statica, la struttura ad albero del dispositivo, la raccolta del kernel di avvio e l'hash root del volume di sistema firmato. Quando al bootloader di livello inferiore viene chiesto di avviare una determinata copia di macOS, lo scopo è quello di garantire che l'hash del manifesto Image4 di macOS allegato ad iBoot corrisponda a ciò che viene rilevato nel campo `nsih` di LocalPolicy. In questo modo, `nsih` rileva per quale sistema operativo l'utente ha intenzionalmente creato un file LocalPolicy. Gli utenti modificano il valore `nsih` in modo implicito quando eseguono un aggiornamento software.

Hash del manifesto Image4 di Cryptex1 (spih)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* Il campo `spih` rappresenta un hash SHA384 della struttura dei dati del manifesto Image4 di Cryptex1. Il manifesto Image4 di Cryptex1 contiene misurazioni relative ai propri cryptex, i sigilli dei relativi file system e la cache di attendibilità associata. All'avvio di macOS, il kernel XNU e il Page Protection Layer verificano che l'hash del manifesto Image4 di Cryptex1 corrisponda a quello pubblicato da iBoot nel campo `spih` di LocalPolicy. Gli utenti modificano il valore `spih` in modo implicito quando installano un intervento di sicurezza rapido o eseguono un aggiornamento software. L'hash del manifesto Image4 di Cryptex1 può essere aggiornato in maniera indipendente rispetto al manifesto Image4 di fase successiva.

Generazione Cryptex1 (stng)

- *Tipo:* intero non firmato di 64 bit
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* il campo `stng` è un valore contatore che rappresenta l'ultimo aggiornamento dell'hash del manifesto Image4 di Cryptex1 in LocalPolicy. Fornisce un valore anti-replay al posto di `lpnh` durante la valutazione di Page Protection Layer della policy locale per l'applicazione del cryptex in entrata. Gli utenti aumentano il valore `stng` in modo implicito quando installano un intervento di sicurezza rapido o eseguono un aggiornamento software.

Hash della politica per la raccolta del kernel ausiliaria (auxp)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* macOS
- *Descrizione:* Il campo `auxp` è un hash SHA384 della politica per l'elenco di estensioni del kernel autorizzate dall'utente. Esso viene usato durante la generazione della raccolta del kernel ausiliaria per aiutare a garantire che in essa siano incluse solo le estensioni del kernel autorizzate dall'utente. `smb2` è un prerequisito per impostare questo campo. Gli utenti modificano il valore `auxp` in maniera implicita quando modificano l'elenco di estensioni del kernel autorizzate dall'utente approvando un'estensione del kernel da "Privacy e Sicurezza" in Impostazioni di Sistema (macOS 13 o versioni successive) o dal pannello "Sicurezza e Privacy" in Preferenze di Sistema (macOS 12 o versioni precedenti).

Hash del manifesto Image4 per la raccolta del kernel ausiliaria (auxi)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* macOS
- *Descrizione:* Una volta che il sistema ha verificato che l'hash dell'elenco di estensioni del kernel autorizzate dall'utente corrisponde al campo `auxp` di LocalPolicy, richiede che la raccolta del kernel ausiliaria venga firmata dall'app del processore Secure Enclave che è responsabile per la firma di LocalPolicy. Successivamente un hash SHA384 della firma del manifesto Image4 della raccolta del kernel ausiliaria viene posizionato in LocalPolicy, per evitare la potenziale applicazione errata di raccolte del kernel ausiliarie precedenti a un sistema operativo durante l'avvio. Se iBoot trova il campo `auxi` in LocalPolicy, tenta di caricare la raccolta del kernel ausiliaria dallo spazio di archiviazione e ne convalida la firma. Verifica anche che l'hash del manifesto Image4 allegato alla raccolta del kernel ausiliaria corrisponda al valore trovato nel campo `auxi`. Se per qualsiasi motivo il caricamento della raccolta del kernel ausiliaria non va a buon fine, il sistema continua l'avvio senza questo oggetto di avvio, quindi senza caricare estensioni del kernel di terze parti. Il campo `auxp` è un prerequisito per l'impostazione del campo auxi in LocalPolicy. Gli utenti modificano il valore `auxi` in maniera implicita quando modificano l'elenco di estensioni del kernel autorizzate dall'utente approvando un'estensione del kernel da "Privacy e Sicurezza" in Impostazioni di Sistema (macOS 13 o versioni successive) o dal pannello "Sicurezza e Privacy" in Preferenze di Sistema (macOS 12 o versioni precedenti).

Hash della ricevuta per la raccolta del kernel ausiliaria (auxr)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* macOS
- *Descrizione:* Il campo `auxr` è un hash SHA384 della ricevuta della raccolta del kernel ausiliaria, che indica l'esatto insieme di estensioni del kernel incluse all'interno della raccolta del kernel ausiliaria. La ricevuta della raccolta del kernel ausiliaria può essere un sottoinsieme dell'elenco di estensioni del kernel autorizzate dall'utente, perché le estensioni del kernel possono essere escluse dalla raccolta del kernel ausiliaria anche se sono autorizzate, se è noto che vengono utilizzate per effettuare attacchi. Inoltre, alcune estensioni del kernel che possono essere utilizzate per superare il confine tra utente e kernel potrebbero ridurre alcune funzionalità come la possibilità di usare Apple Pay o di riprodurre contenuti 4K e HDR. Gli utenti che desiderano avere tali possibilità sono disposti ad accettare un'inclusione all'interno della raccolta del kernel ausiliaria più restrittiva. Il campo `auxp` è un prerequisito per l'impostazione del campo `auxr` in LocalPolicy. Gli utenti modificano il valore `auxr` in maniera implicita quando creano una nuova raccolta del kernel ausiliaria da "Privacy e Sicurezza" in Impostazioni di Sistema (macOS 13 o versioni successive) o dal pannello "Sicurezza e Privacy" in Preferenze di Sistema (macOS 12 o versioni precedenti).

Hash del manifesto Image4 di CustomOS (coih)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* 1TR
- *Descrizione:* Il valore `coih` è un hash SHA384 del manifesto Image4 di CustomOS. Il payload di tale manifesto è utilizzato da iBoot (al posto del kernel XNU) per trasferire il controllo. L'utente modifica il valore `coih` in modo implicito quando utilizza lo strumento a linea di comando `kmutil configure-boot` nella modalità 1TR.

UUID del gruppo di volumi APFS (vuid)

- *Tipo:* OctetString (16)
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* Il valore `vuid` indica il gruppo di volumi che il kernel deve utilizzare come root. Questo campo ha uno scopo principalmente informativo e non è utilizzato per misure di sicurezza. Il valore `vuid` viene impostato in maniera implicita dall'utente durante la creazione dell'installazione di un nuovo sistema operativo.

UUID di gruppo della chiave di codifica delle chiavi (kuid)

- *Tipo:* OctetString (16)
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* Il valore `kuid` indica il volume che è stato avviato. La chiave di codifica delle chiavi era tipicamente usata per la protezione dei dati. Per ciascun LocalPolicy, viene utilizzata per proteggere la relativa chiave per la firma. Il valore `kuid` viene impostato in maniera implicita dall'utente durante la creazione dell'installazione di un nuovo sistema operativo.

Misurazione della politica di avvio attendibile abbinata a recoveryOS (prot)

- *Tipo:* OctetString (48)
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* La misurazione della politica di avvio attendibile abbinata a recoveryOS è un calcolo hash SHA384 iterativo speciale effettuato sul manifesto Image4 di un LocalPolicy questo caso i valori anti-replay vengono esclusi per poter fornire una misurazione coerente nel tempo (dato che i valori anti-replay come `lpnh` vengono aggiornati frequentemente). Il campo `prot`, che si trova solo in ciascun LocalPolicy di macOS, indica quale LocalPolicy di recoveryOS corrisponde al LocalPolicy di macOS.

Verifica della firma di Secure Enclave al LocalPolicy di recoveryOS (hrlp)

- *Tipo:* Booleano
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* Il valore `hrlp` indica se il valore `prot` descritto in precedenza è la misurazione di un LocalPolicy di recoveryOS firmato da Secure Enclave oppure no. Se non lo è, il LocalPolicy di recoveryOS viene firmato dal server di Apple online, che firma elementi come i file Image4 di macOS.

Versione locale del sistema operativo (Local Operating System Version, love)

- *Tipo:* Booleano
- *Ambienti mutabili:* 1TR, recoveryOS, macOS
- *Descrizione:* `love` indica la versione del sistema operativo per cui il file LocalPolicy è stato creato. La versione è ottenuta dal manifesto dello stato successivo durante la creazione del file LocalPolicy e viene utilizzata per applicare le restrizioni all'abbinamento di recoveryOS.

Avvio multiplo protetto (smb0)

- *Tipo:* Booleano
- *Ambienti mutabili:* 1TR, recoveryOS
- *Descrizione:* Se `smb0` è presente e vero, il bootloader di livello inferiore consente la firma del manifesto Image4 di fase successiva, invece che richiedere una firma personalizzata. Gli utenti possono modificare questo campo tramite Utility Sicurezza Avvio o tramite `bputil` per impostare il sistema su "Sicurezza ridotta".

Avvio multiplo protetto (smb1)

- *Tipo:* Booleano
- *Ambienti mutabili:* 1TR
- *Descrizione:* Se `smb1` è presente e vero, iBoot consente che oggetti come una raccolta del kernel personalizzata vengano firmati da Secure Enclave con la stessa chiave di LocalPolicy. La presenza di `smb0` è un prerequisito per la presenza di `smb1`. Gli utenti possono modificare questo campo tramite strumenti a riga di comando come `csrutil` o `bputil` per impostare il sistema su "Sicurezza assente".

Avvio multiplo protetto (smb2)

- *Tipo:* Booleano
- *Ambienti mutabili:* 1TR
- *Descrizione:* Se `smb2` è presente e vero, iBoot consente che la raccolta del kernel ausiliaria venga firmata da Secure Enclave con la stessa chiave di LocalPolicy. La presenza di `smb0` è un prerequisito per la presenza di `smb2`. Gli utenti possono modificare questo campo tramite Utility Sicurezza Avvio o tramite `bputil` per impostare il sistema su "Sicurezza ridotta" e consentire estensioni del kernel di terze parti.

Avvio multiplo protetto (smb3)

- *Tipo:* Booleano
- *Ambienti mutabili:* 1TR
- *Descrizione:* Se `smb3` è presente e vero, un utente sul dispositivo ha accettato il controllo del sistema tramite una soluzione di gestione dei dispositivi mobili (MDM). La presenza di questo campo fa in modo che l'app del processore Secure Enclave che controlla LocalPolicy accetti l'autenticazione MDM invece di richiedere un'autenticazione dall'utente locale. Gli utenti possono modificare questo campo tramite Utility Sicurezza Avvio o `bputil` per abilitare il controllo gestito su estensioni del kernel di terze parti e aggiornamenti software. (In macOS 11.2 o versioni successive, una soluzione MDM può anche avviare un aggiornamento all'ultima versione di macOS se la modalità di sicurezza attuale è "Sicurezza totale").

Avvio multiplo protetto (smb4)

- *Tipo:* Booleano
- *Ambienti mutabili:* macOS
- *Descrizione:* Se `smb4` è presente e vero, il dispositivo ha accettato il controllo del sistema operativo da parte di una soluzione MDM tramite Apple School Manager, Apple Business Manager o Apple Business Essentials. La presenza di questo campo fa in modo che l'app del processore Secure Enclave che controlla LocalPolicy accetti l'autenticazione MDM invece di richiedere un'autenticazione dall'utente locale. Questo campo viene modificato dalla soluzione MDM quando rileva che il numero di serie di un dispositivo compare in uno dei tre servizi.

Protezione dell'integrità del sistema (sip0)

- *Tipo:* Intero non firmato di 64 bit
- *Ambienti mutabili:* 1TR
- *Descrizione:* Il valore `sip0` contiene i bit esistenti della politica per la protezione dell'integrità del sistema, precedentemente archiviati nella NVRAM. I nuovi bit della politica per la protezione dell'integrità del sistema vengono aggiunti qui (invece di utilizzare i campi di LocalPolicy come quello sotto) se vengono usati solo in macOS e non vengono usati dal bootloader di livello inferiore. Gli utenti possono modificare questo campo tramite `csrutil` da 1TR per disabilitare la protezione dell'integrità del sistema e impostare il sistema su "Sicurezza assente".

Protezione dell'integrità del sistema (sip1)

- *Tipo:* Booleano
- *Ambienti mutabili:* 1TR
- *Descrizione:* se `sip1` è presente e vero, iBoot consente la verifica dell'hash root del volume di sistema firmato in caso di operazioni non riuscite. Gli utenti possono modificare questo campo tramite `csrutil` o `bputil` da 1TR.

Protezione dell'integrità del sistema (sip2)

- *Tipo:* booleano
- *Ambienti mutabili:* 1TR
- *Descrizione:* se sip2 è presente e vero, iBoot non bloccherà il registro hardware *Configurable Text Read-only Region (CTRR)* che contrassegna la memoria del kernel come non scrivibile. Gli utenti possono modificare questo campo tramite `csrutil` o `bputil` da 1TR.

Protezione dell'integrità del sistema (sip3)

- *Tipo:* Booleano
- *Ambienti mutabili:* 1TR
- *Descrizione:* se `sip3` è presente e vero, iBoot non applicherà l'elenco integrato di elementi consentiti per la variabile della NVRAM boot-args, che altrimenti filtrerebbe le opzioni trasmesse al kernel. Gli utenti possono modificare questo campo tramite `csrutil` o `bputil` da 1TR.

Certificati e RemotePolicy

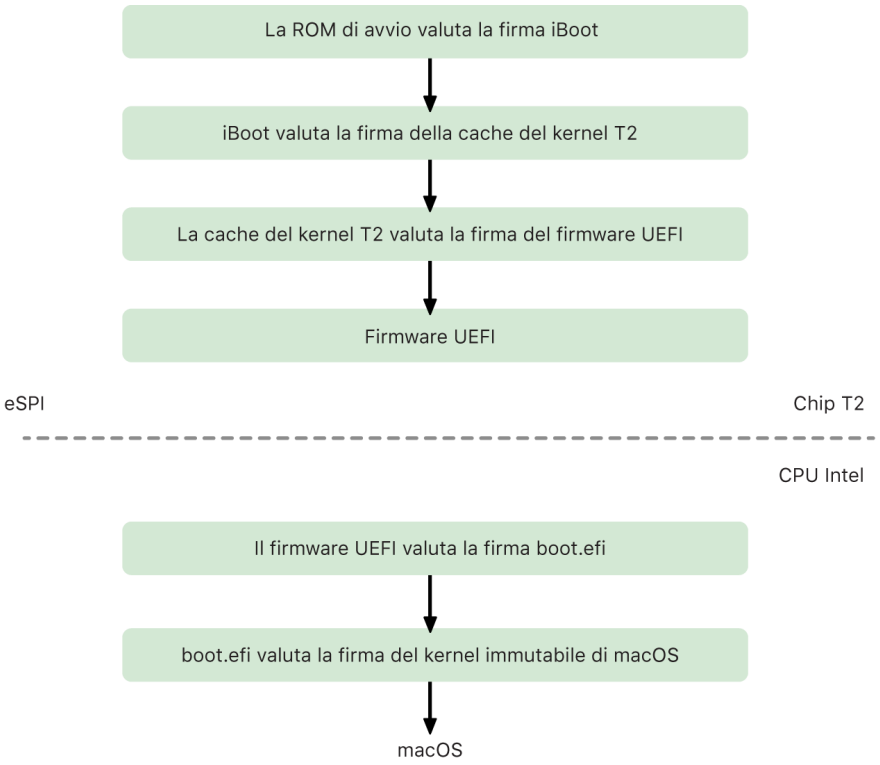
Come descritto in Creazione e gestione della chiave per la firma di LocalPolicy, il file Image4 di LocalPolicy contiene anche il certificato OIC (Owner Identity Certificate) e il RemotePolicy integrato.

Computer Mac dotati di processore Intel

Processo di avvio per i Mac dotati di processore Intel

Mac dotati di processore Intel con chip di sicurezza Apple T2

Quando un Mac dotato di processore Intel con chip di sicurezza Apple T2 viene acceso, il chip esegue un avvio protetto dalla propria ROM di avvio in maniera analoga a ciò che avviene su iPhone, su iPad e sui Mac dotati di chip Apple. In questo modo viene verificato il bootloader iBoot ed è il primo passaggio della catena di attendibilità. iBoot verifica il kernel e il codice di estensione del kernel con il chip T2, il quale successivamente verifica il firmware UEFI Intel. Il firmware UEFI e la relativa firma inizialmente sono disponibili solo per il chip T2.



Dopo la verifica, l'immagine del firmware UEFI viene mappata in una parte della memoria del chip T2, che è resa disponibile alla CPU Intel tramite l'eSPI (enhanced Serial Peripheral Interface). Quando la CPU Intel si avvia per la prima volta, recupera il firmware UEFI tramite il protocollo eSPI dalla copia del firmware, mappata sulla memoria e di cui è stata previamente verificata l'integrità, situata nel chip T2.

Il processo di valutazione della catena di attendibilità continua sulla CPU Intel, con il firmware UEFI che valuta la firma per boot.efi, il bootloader di macOS. Le firme di avvio protetto di macOS di Intel sono archiviate nello stesso formato Image4 usato per l'avvio protetto del chip T2, iOS e iPadOS; inoltre, il codice che analizza i file Image4 è lo stesso codice sottoposto a hardening attualmente implementato per l'avvio protetto su iOS e iPadOS. Il boot.efi verifica la firma di un nuovo file chiamato immutablekernel. Quando viene abilitato un avvio protetto, il file immutablekernel rappresenta l'insieme completo di estensioni del kernel di Apple richieste per avviare macOS. La politica relativa all'avvio protetto termina nel momento del passaggio all'immutablekernel e, da lì in poi, entrano in vigore le politiche di sicurezza di macOS (come la protezione dell'integrità del sistema e le estensioni del kernel firmate).

Eventuali errori o problemi riscontrati durante il processo faranno entrare il Mac in modalità di recupero, in modalità di recupero del chip di sicurezza Apple T2 o in modalità DFU per il chip di sicurezza Apple T2.

Microsoft Windows sui Mac dotati di processore Intel con chip T2

unicamente i contenuti firmati da Apple. Tuttavia, per migliorare la sicurezza delle installazioni Boot Camp, Apple supporta anche l'avvio protetto per Windows. Il firmware UEFI (Unified Extensible Firmware Interface) include una copia del certificato Microsoft Windows Production CA 2011 utilizzato per autenticare i bootloader Microsoft.

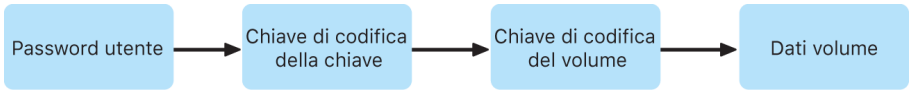
Nota: attualmente non viene fornita attendibilità per Microsoft Corporation UEFI CA 2011, che consentirebbe la verifica del codice firmato dai partner di Microsoft. Questa autorità di certificazione UEFI viene usata solitamente per verificare l'autenticità dei bootloader per altri sistemi operativi, come le varianti di Linux.

Il supporto per l'avvio protetto di Windows non è abilitato di default, ma tramite Assistente Boot Camp. Quando un utente esegue Assistente Boot Camp, macOS viene riconfigurato per ritenere affidabile il codice firmato di prima mano da Microsoft durante l'avvio. Una volta completato Assistente Boot Camp, se macOS non supera la verifica dell'affidabilità di Apple durante l'avvio protetto, il firmware UEFI cerca di verificare l'affidabilità dell'oggetto secondo la formattazione dell'avvio protetto UEFI. Se la verifica dell'affidabilità avviene correttamente, il Mac continua e avvia Windows. In caso di esito negativo invece, entra in recoveryOS e informa l'utente dell'errore della verifica di affidabilità.

Computer Mac dotati di processore Intel sprovvisti di chip T2

I Mac dotati di processore Intel sprovvisti di chip T2 non supportano l'avvio protetto. Quindi il firmware UEFI carica il bootloader di macOS (boot.efi) dal file system senza verificarlo, e il bootloader carica il kernel (prelinkedkernel) dal file system senza verificarlo. Per proteggere l'integrità della catena di avvio, gli utenti dovrebbero abilitare tutti i meccanismi di sicurezza seguenti:

- *Protezione dell'integrità del sistema (SIP):* abilitata di default, quest'opzione protegge il bootloader e il kernel da processi di scrittura dannosi provenienti da un macOS in esecuzione.
- *FileVault:* può essere abilitato dall'utente oppure da un amministratore MDM (Mobile Device Management). Protegge dagli attacchi di un hacker fisicamente presente che usa la modalità disco di destinazione per sovrascrivere il bootloader.
- *Password del firmware:* può essere abilitata dall'utente oppure da un amministratore MDM (Mobile Device Management). Aiuta a proteggere dall'attivazione di modalità di avvio alternative da parte di un hacker fisicamente presente, quali ad esempio recoveryOS, "Modalità utente singolo" o "Modalità disco di destinazione", da cui può essere sovrascritto il bootloader. Questa password aiuta inoltre a impedire l'avvio da supporti multimediali alternativi, da cui un hacker potrebbe eseguire del codice per sovrascrivere il bootloader.



Modalità di avvio dei Mac dotati di processore Intel con chip di sicurezza Apple T2

I Mac dotati di processore Intel con chip di sicurezza Apple T2 dispongono di una varietà di modalità di avvio accessibili durante la fase di avvio premendo delle combinazioni di tasti riconosciute dal software di avvio o dal firmware UEFI. Alcune modalità di avvio, come "Modalità utente singolo", funzionano solo se la politica di sicurezza viene impostata su "Nessuna sicurezza" in Utility Sicurezza Avvio.

Modalità	Combinazione di tasti	Descrizione
Avvio di macOS	Nessuna	Il firmware UEFI esegue il programma di avvio di macOS (un'app UEFI) che esegue il kernel di macOS. Nell'avvio standard di un Mac su cui è abilitato FileVault, il software di avvio di macOS presenta l'interfaccia della finestra di login in cui inserire la password per la decrittografia degli elementi archiviati sul computer.
Assistente di avvio	Opzione (⌥)	Il firmware UEFI avvia l'app UEFI integrata che presenta all'utente l'interfaccia per la selezione del dispositivo da avviare.
Modalità disco di destinazione (TDM)	T	Il firmware UEFI avvia l'app UEFI integrata che mostra il dispositivo interno di archiviazione come un dispositivo di archiviazione a blocchi tramite FireWire, Thunderbolt, USB o qualsiasi combinazione di questi tre tipi di collegamento (in base al modello del Mac).
Modalità utente singolo	Comando (⌘)-S	Il kernel macOS trasmette l'indicatore –s al vettore dell'argomento di launchd, quindi launchd crea una shell utente singolo sul tty dell'app Console. *Nota:* se l'utente esiste nella shell, macOS continua l'avvio nella finestra di login.
recoveryOS	Comando (⌘)-R	Il firmware UEFI carica un macOS di base da un file immagine disco firmato (.dmg) sul dispositivo di archiviazione interno.
recoveryOS tramite internet	Opzione (⌥)-Comando (⌘)-R	L'immagine disco firmata viene scaricata da internet tramite HTTP.
Diagnosi	D	Il firmware UEFI carica un ambiente di diagnosi UEFI di base da un file immagine disco firmato sul dispositivo di archiviazione interno.
Diagnosi internet	Opzione (⌥)-D	L'immagine disco firmata viene scaricata da internet tramite HTTP.
Avvio di Windows	Nessuna	Se Windows è stato installato tramite Boot Camp, il firmware UEFI esegue il programma di avvio di Windows, che esegue il kernel di Windows.

Utility Sicurezza Avvio per i Mac dotati di chip di sicurezza Apple T2

Panoramica

Sui Mac dotati di processore Intel con chip di sicurezza Apple T2, Utility Sicurezza Avvio gestisce varie impostazioni delle politiche di sicurezza. L'utility è accessibile eseguendo l'avvio in recoveryOS e selezionando Utility Sicurezza Avvio dal menu Utility. Il suo scopo è quello di proteggere le impostazioni di sicurezza supportate da facili manipolazioni da parte di un hacker.

Per le modifiche a politiche fondamentali è necessaria l'autenticazione, anche in modalità di recupero. Quando l'utente apre per la prima volta Utility Sicurezza Avvio gli viene chiesto di inserire la password di amministratore dell'installazione principale di macOS associata all'istanza di recoveryOS da cui è stato attualmente eseguito l'avvio. Se non esiste alcun amministratore, occorre prima crearne uno perché sia possibile modificare la politica. Il chip T2 richiede che il Mac sia attualmente avviato in recoveryOS e che sia avvenuta un'autenticazione con una credenziale supportata da Secure Enclave prima che sia possibile effettuare tale modifica alla politica. Le modifiche alla politica di sicurezza hanno due requisiti impliciti. recoveryOS deve:

- Essere avviato da un dispositivo di archiviazione collegato direttamente al chip T2, perché le partizioni sugli altri dispositivi non dispongono di credenziali supportate da Secure Enclave vincolate al dispositivo di archiviazione interno.
- Trovarsi su un volume APFS, perché supporta unicamente l'archiviazione delle credenziali di autenticazione in Recovery inviate a Secure Enclave sul volume APFS di pre-avvio di un'unità. I volumi HFS Plus non possono essere utilizzati per l'avvio protetto.

Questa politica viene mostrata solo in Utility Sicurezza Avvio sui Mac dotati di processore Intel con chip T2. Sebbene nella maggior parte dei casi non dovrebbero essere necessarie modifiche alla politica di avvio protetto, in definitiva sono gli utenti ad avere il controllo delle impostazioni dei propri dispositivi e potrebbero decidere di disabilitare o ridurre la funzionalità di avvio protetto del Mac in base alle proprie esigenze.

Le modifiche alle politiche di avvio protetto effettuate dall'interno di questa app saranno applicate solo alla verifica della catena di affidabilità sul processore Intel. L'opzione relativa all'avvio protetto del chip T2 è sempre in vigore.

La politica di avvio protetto può essere impostata su una di queste tre opzioni: "Sicurezza totale", "Sicurezza media" e "Nessuna sicurezza". Nell'ultimo caso viene disabilitata completamente la verifica dell'avvio protetto sul processore Intel e l'utente può eseguire l'avvio di ciò che preferisce.

Politica di avvio "Sicurezza totale"

"Sicurezza totale" è la politica di avvio di default e si comporta in modo analogo ad iOS e iPadOS o a "Sicurezza totale" sui Mac dotati di chip Apple. Nel momento in cui il software viene scaricato e preparato per l'installazione, viene personalizzato con una firma che include l'ECID (Exclusive Chip Identification) come parte della richiesta di firma, ossia un ID unico in questo caso specifico per il chip T2. La firma restituita dal server di firma è quindi unica e utilizzabile solo da quel chip T2 in concreto. Il firmware UEFI è progettato per garantire che, quando viene applicata la politica "Sicurezza totale", una firma determinata non sia solo di Apple, ma venga anche creata appositamente per quel Mac, vincolando quella versione di macOS a quel Mac specifico. Ciò aiuta a impedire attacchi rollback, come descritto per l'opzione "Sicurezza totale" sui Mac dotati di chip Apple.

Politica di avvio "Sicurezza media"

La politica di avvio "Sicurezza media" è pressoché simile all'avvio protetto UEFI, in cui un fornitore (in questo caso, Apple) genera una firma digitale per il codice dichiarando così che proviene dal fornitore. In questo modo gli hacker non potranno inserire codice non firmato. Apple definisce tale firma come "globale", perché può essere utilizzata su qualsiasi Mac e per qualunque durata di tempo per i Mac su cui è impostata la politica "Sicurezza media". iOS, iPadOS e il chip T2 non supportano le firme globali. Questa impostazione non tenta di impedire gli attacchi rollback.

Politica di avvio da supporto

La politica di avvio da supporto è disponibile solo sui Mac dotati di processore Intel con chip T2 ed è indipendente dalla politica di avvio protetto. Dunque, anche se un utente disabilita l'avvio protetto, il comportamento di default non consentirà l'avvio del Mac da dispositivi di archiviazione non direttamente collegati al chip T2. (La politica di avvio da supporto non è richiesta sui Mac dotati di chip Apple. Per ulteriori informazioni, consulta Controllo delle politiche di sicurezza per il disco di avvio.)

Protezione tramite password del firmware sui Mac dotati di processore Intel

macOS sui Mac dotati di processore Intel supporta l'uso della password del firmware per aiutare a impedire modifiche non desiderate alle impostazioni del firmware su un Mac specifico. La password del firmware è progettata per impedire modalità alternative di avvio, come ad esempio l'avvio in recoveryOS o "Modalità utente singolo", da un volume non autorizzato oppure l'avvio in "Modalità disco di destinazione".

Nota: la password del firmware non è richiesta sui Mac dotati di chip Apple, perché la funzionalità essenziale del firmware che essa limitava è stata spostata in recoveryOS e (quando FileVault è abilitato) recoveryOS richiede l'autenticazione da parte dell'utente per raggiungere tale funzionalità fondamentale.

La modalità più basilare della password del firmware può essere raggiunta da Utility Password Firmware di recoveryOS sui Mac dotati di processore Intel *senza* chip T2 e da Utility Sicurezza Avvio sui Mac dotati di processore Intel *con* chip T2. Le opzioni più avanzate (come la possibilità di richiedere la password a ogni avvio) sono disponibili tramite lo strumento a linea di comando `firmwarepasswd` in macOS.

L'impostazione di una password del firmware è particolarmente importante per ridurre il rischio di attacchi ai Mac dotati di processore Intel sprovvisti di chip T2 effettuati da un hacker presente fisicamente. La password del firmware aiuta a impedire a un hacker di avviare recoveryOS, da cui potrebbe disabilitare la protezione dell'integrità di sistema. Limitando i supporti di avvio alternativi, inoltre, impedisce a un hacker di eseguire del codice privilegiato da un altro sistema operativo al fine di attaccare i firmware delle periferiche.

Per aiutare gli utenti che hanno dimenticato la password, esiste un meccanismo di reimpostazione della password del firmware. Gli utenti dovranno premere una combinazione di tasti all'avvio e visualizzeranno una stringa specifica del modello da fornire ad AppleCare. AppleCare firma digitalmente una risorsa e tale firma viene verificata dall'URI (Uniform Resource Identifier). Se la firma viene convalidata e il contenuto è di quel Mac in concreto, il firmware UEFI rimuove la password del firmware.

Per gli utenti che non vogliono consentire ad altri di rimuovere la password del firmware tramite software, è stata aggiunta l'opzione `–disable–reset–capability` allo strumento a linea di comando `firmwarepasswd` in macOS 10.15. Prima di impostare questa opzione, gli utenti sono tenuti a dichiarare di aver compreso che, qualora dimentichino la password e debbano rimuoverla, il costo della sostituzione della scheda madre da effettuare a tale fine sarà a carico dell'utente. Le organizzazioni che vogliono proteggere i propri Mac da attacchi sia esterni che da parte di impiegati devono impostare una password del firmware sui propri sistemi. È possibile procedere all'impostazione su un dispositivo nei seguenti modi:

- Manualmente durante il provisioning, mediante lo strumento a linea di comando `firmwarepasswd`.
- Con strumenti di gestione di terze parti che usano lo strumento a linea di comando `firmwarepasswd`.
- Usando la gestione dei dispositivi mobili (MDM).

Ambienti di diagnosi e recoveryOS per i Mac dotati di processore Intel

recoveryOS

recoveryOS è completamente separato dal sistema macOS principale e tutti i suoi contenuti sono archiviati in un file immagine disco chiamato BaseSystem.dmg. Esiste anche un file BaseSystem.chunklist associato, che viene utilizzato per verificare l'integrità del file BaseSystem.dmg. Il file chunklist consiste in una serie di hash per blocchi di 10 MB del file BaseSystem.dmg. Il firmware UEFI valuta la firma del file chunklist, quindi valuta l'hash, un blocco alla volta, del file BaseSystem.dmg. Questo meccanismo aiuta a garantire la corrispondenza con il contenuto firmato presente nel file chunklist. In caso di mancata corrispondenza di uno qualsiasi di questi hash, l'avvio dal recoveryOS locale viene annullato e il firmware UEFI cerca quindi di avviare da recoveryOS tramite internet.

Se la verifica viene completata correttamente, il firmware UEFI attiva il file BaseSystem.dmg come disco RAM e avvia il boot.efi lì contenuto. Il firmware UEFI non dovrà effettuare una verifica specifica del boot.efi né il boot.efi dovrà verificare il kernel, perché la verifica dell'integrità dei contenuti completi del sistema operativo (di cui questi elementi rappresentano solo un sottoinsieme) è già avvenuta.

Strumenti di diagnosi Apple

Il processo di avvio dell'ambiente di diagnosi locale è perlopiù uguale a quello di avvio di recoveryOS. Vengono utilizzati dei file AppleDiagnostics.dmg e AppleDiagnostics.chunklist separati, che però vengono verificati nello stesso modo dei file BaseSystem. Invece di avviare il boot.efi, il firmware UEFI avvia un file che si trova all'interno dell'immagine disco (file .dmg) chiamato diags.efi, che si occupa di richiamare una varietà di altri driver UEFI con cui interfacciarsi e verificare la presenza di eventuali errori nell'hardware.

Ambiente di diagnosi e recoveryOS tramite internet

Se si è verificato un errore durante l'avvio degli ambienti di diagnosi o recupero locali, il firmware UEFI cerca di scaricare le immagini da internet. (L'utente può anche richiedere specificamente che le immagini siano scaricate da internet usando una speciale sequenza di tasti da tenere premuti durante l'avvio). La convalida dell'integrità delle immagini disco e dei file chunklist scaricati da OS Recovery Server viene effettuata nello stesso modo utilizzato per le immagini recuperate da un dispositivo di archiviazione.

Nonostante la connessione a OS Recovery Server avvenga tramite HTTP, i contenuti completi scaricati vengono comunque sottoposti alla verifica dell'integrità descritta sopra e sono quindi protetti da attacchi di hacker che dovessero assumere il controllo della rete. Nel caso in cui un singolo blocco non superi la verifica dell'integrità, la richiesta a OS Recovery Server viene effettuata altre 11 volte prima che il processo venga interrotto e venga visualizzato un errore.

Quando il recupero via internet e le modalità di diagnosi sono state aggiunte ai Mac nel 2011, è stato deciso di preferire il trasferimento tramite un protocollo più semplice come HTTP e gestire l'autenticazione dei contenuti tramite il meccanismo del chunklist, piuttosto che implementare una funzionalità più complicata come HTTPS nel firmware UEFI, aumentando le possibilità di attacco al firmware.

Sicurezza del volume di sistema firmato

In macOS 10.15, Apple ha introdotto il volume di sistema di sola lettura, ovvero un volume dedicato e isolato per i contenuti di sistema. macOS 11 o versioni successive aggiunge delle protezioni crittografiche forti per i contenuti di sistema con un *volume di sistema firmato*. Il volume di sistema firmato è dotato di un meccanismo nel kernel che verifica l'integrità dei contenuti del sistema e rifiuta qualsiasi dato (codice e non codice) che non disponga di una firma crittografica valida fornita da Apple. A partire da iOS 15 e iPadOS 15, anche il volume di sistema su iPhone e iPad acquisisce la protezione crittografica di un volume di sistema firmato.

Il volume di sistema firmato non solo aiuta a impedire la manomissione del software Apple che fa parte del sistema operativo, rende anche l'aggiornamento del software di macOS più affidabile e molto più sicuro. E dato che il volume di sistema firmato utilizza istantanee APFS (Apple File System), se un aggiornamento non può essere effettuato, è possibile ripristinare la versione meno recente del sistema senza eseguire una reinstallazione.

Fin dalla sua introduzione, APFS ha garantito l'integrità dei metadati del file system tramite checksum non crittografici sul dispositivo di archiviazione interno. Il volume di sistema firmato rafforza il meccanismo di integrità aggiungendo hash crittografici, estendendolo quindi a ogni byte dei dati dei file. Ai dati del dispositivo di archiviazione interno (compresi i metadati del file system) viene applicato un hash crittografico nel percorso di lettura e l'hash viene quindi confrontato con un valore atteso nei metadati del file system. In caso di mancata corrispondenza, il sistema presume che i dati siano stati manomessi e non li restituirà al software che li richiede.

Ciascun hash SHA256 del volume di sistema firmato viene archiviato nell'albero principale dei metadati del file system, a cui, a sua volta, viene applicato un hash. E dato che ogni nodo dell'albero verifica in maniera ricorsiva l'integrità degli hash dei nodi inferiori, in maniera simile a un albero di hash binario (Merkle), il valore hash del nodo radice, chiamato *sigillo*, raccoglie ogni byte di dati nel volume di sistema firmato, il che significa che la firma crittografica copre l'intero volume di sistema.

Durante l'installazione e l'aggiornamento di macOS, il sigillo viene ricalcolato dal file system sul dispositivo e tale misurazione viene confrontata con quella firmata da Apple. Sui Mac dotati di chip Apple, il bootloader verifica il sigillo prima di trasferire il controllo al kernel. Sui Mac dotati di processore Intel con chip di sicurezza Apple T2, il bootloader inoltra la misurazione e la firma al kernel, che quindi verifica il sigillo direttamente, prima di attivare il file system root. In entrambi i casi, se la verifica non va a buon fine, il processo di avvio si interrompe e all'utente verrà richiesto di reinstallare macOS. Questa procedura viene ripetuta a ogni avvio, a meno che l'utente non abbia scelto di usare una modalità di sicurezza inferiore e abbia separatamente scelto di disabilitare il volume di sistema firmato.

Durante gli aggiornamenti software di iOS e iPadOS, il volume di sistema viene preparato e ricalcolato in modo simile. I bootloader di iOS e iPadOS verificano che il sigillo sia intatto e che corrisponda al valore firmato da Apple prima di consentire al dispositivo di avviare il kernel. Se durante l'avvio non viene rilevata una corrispondenza, all'utente viene richiesto di aggiornare il software di sistema sul dispositivo. Gli utenti non sono autorizzati a disabilitare la protezione di un volume di sistema firmato su iOS e iPadOS.

Volume di sistema firmato e firma del codice

La firma del codice è ancora presente e implementata dal kernel. Il volume di sistema firmato fornisce protezione per ogni singolo byte letto dal dispositivo di archiviazione interno. La firma del codice, invece, fornisce protezione quando gli oggetti Mach sono mappati nella memoria come eseguibili. Sia il volume di sistema firmato che la firma del codice proteggono il codice eseguibile in tutti i percorsi di lettura ed esecuzione.

Volume di sistema firmato e FileVault

In macOS 11 o versioni successive, una protezione equivalente dei contenuti di sistema a riposo è fornita dal volume di sistema firmato, quindi non è più necessario che il volume di sistema sia codificato. Qualsiasi modifica effettuata al file system a riposo viene rilevata dal file system stesso quando viene letta. Se l'utente ha attivato FileVault, i suoi contenuti sul volume di dati sono comunque codificati con un segreto fornito dall'utente.

Se l'utente sceglie di disabilitare il volume di sistema firmato, quando il sistema si trova a riposo esso diviene vulnerabile e una possibile manomissione potrebbe consentire a un hacker di estrarre dati utente codificati al prossimo avvio del sistema. Dunque il sistema non permette all'utente di disabilitare il volume di sistema firmato se FileVault è attivato. La protezione a riposo deve essere abilitata o disabilitata per entrambi i volumi in modo coerente.

In macOS 10.15 o versioni precedenti, FileVault protegge il software del sistema operativo a riposo codificando i contenuti dell'utente e del sistema con una chiave protetta da un segreto fornito dall'utente. Ciò impedisce a un hacker che ha accesso fisico al dispositivo di accedere al file system contenente il software di sistema o di modificarlo.

Volume di sistema firmato e Mac con chip di sicurezza Apple T2

Sui Mac con chip di sicurezza Apple T2, solo macOS stesso è protetto dal volume di sistema firmato. Il software in esecuzione sul chip T2 e che verifica macOS non è protetto dall'avvio protetto.

Aggiornamenti software sicuri

La sicurezza è un processo. Non è sufficiente avviare in maniera affidabile la versione del sistema operativo installata in fabbrica; è necessario anche un meccanismo che consenta di ottenere in modo rapido e sicuro gli ultimi aggiornamenti di sicurezza. Apple rilascia periodicamente aggiornamenti software volti a risolvere sul nascere eventuali problematiche di sicurezza. Gli utenti di iPhone e iPadOS ricevono notifiche per l'aggiornamento sul dispositivo. Gli utenti Mac possono trovare gli aggiornamenti disponibili in Impostazioni di Sistema (macOS 13 o versioni successive) o in Preferenze di Sistema (macOS 12 o versioni precedenti). Gli aggiornamenti vengono inviati in modalità wireless, per consentire l'adozione rapida delle ultime soluzioni a problematiche di sicurezza.

Sicurezza del processo di aggiornamento

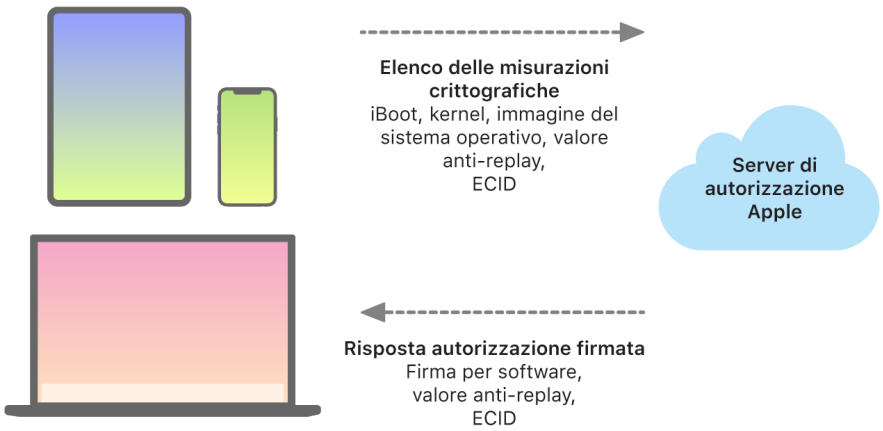
Il processo di aggiornamento utilizza la stessa radice di attendibilità hardware utilizzata dall'avvio protetto, progettata per installare solo codice firmato da Apple. Il processo di aggiornamento utilizza anche l'autorizzazione del software di sistema per verificare che su iPhone e iPad o sui Mac con l'impostazione "Sicurezza totale" configurata come politica di avvio protetto in Utility Sicurezza Avvio possano essere installate solo le copie delle versioni del sistema operativo firmate attivamente da Apple. Queste misure di sicurezza consentono ad Apple di interrompere la firma di versioni meno recenti del sistema operativo soggette a vulnerabilità note e di aiutare a impedire gli attacchi che sfruttano l'installazione di versioni precedenti.

Per una sicurezza degli aggiornamenti maggiore, quando il dispositivo da aggiornare è collegato fisicamente a un Mac, viene scaricata e installata una copia completa di iOS o iPadOS. Tuttavia, per gli aggiornamenti software in modalità wireless *vengono scaricati solo i componenti richiesti per completare l'aggiornamento* invece di scaricare l'intero sistema operativo, migliorando così l'efficienza della rete. Inoltre, gli aggiornamenti software possono essere archiviati nella cache sui Mac con macOS 10.13 o versioni successive e su cui è abilitata la cache dei contenuti; in questo modo gli iPhone e gli iPad non hanno bisogno di scaricare nuovamente gli aggiornamenti necessari da internet. (Tuttavia dovranno contattare i server Apple per completare il processo di aggiornamento).

Processo di aggiornamento personalizzato

Durante gli aggiornamenti, determinate informazioni vengono rese disponibili al server Apple di autorizzazione per l'installazione, che include un elenco di misurazioni crittografiche per ogni singola parte del pacchetto di installazione che deve essere installato (ad esempio iBoot, il kernel e l'immagine del sistema operativo), un valore anti-replay casuale e l'ID unico del chip del dispositivo (ECID).

Il server di autorizzazione verifica l'elenco di misurazioni che è stato presentato e lo paragona alle versioni in cui è stata permessa l'installazione; se trova una corrispondenza, aggiunge l'ECID alla misurazione e firma il risultato. Il server trasmette al dispositivo un set completo di dati firmati come parte del processo di aggiornamento. L'aggiunta dell'ECID "personalizza" l'autorizzazione per il dispositivo che la richiede. Autorizzando e firmando solo le misurazioni conosciute, il server aiuta a garantire che l'aggiornamento avvenga esattamente secondo i parametri dettati da Apple.



La verifica della catena di affidabilità durante l'avvio controlla che la firma provenga da Apple e che la misurazione dell'elemento caricato dal dispositivo di archiviazione, insieme all'ECID del dispositivo, corrispondano a ciò che risulta coperto dalla firma. Questi passaggi sono progettati per garantire che, sui dispositivi che supportano la personalizzazione, l'autorizzazione sia per un dispositivo specifico e che un sistema operativo o una versione del firmware meno recenti presenti su un dispositivo non possano essere copiati su un altro. Il valore anti-replay aiuta a impedire che un hacker possa salvare la risposta del server e che possa utilizzarla per danneggiare un dispositivo oppure per alterare il software di sistema.

Il processo di personalizzazione è ciò che rende sempre necessaria una connessione di rete con Apple per aggiornare qualsiasi dispositivo dotato di chip Apple e i Mac dotati di processore Intel con chip di sicurezza Apple T2.

Sui dispositivi dotati di Secure Enclave, quest'ultimo utilizza anche il processo di autorizzazione del software di sistema per verificare l'integrità del medesimo software ed è progettato per impedire l'installazione di versioni non aggiornate.

Integrità del sistema operativo

Il software dei sistemi operativi Apple è progettato fin dalle basi in maniera tale da garantire la sicurezza. Esso include una catena di attendibilità hardware (sfruttata per consentire l'avvio protetto) e un processo di aggiornamento del software al tempo stesso rapido e sicuro. I sistemi operativi Apple fanno anche uso di chip appositamente creati per fornire funzionalità hardware che aiutano a impedire attacchi durante l'esecuzione del sistema. Queste funzionalità proteggono l'integrità del codice attendibile mentre si trova in esecuzione. In breve, il software dei sistemi operativi Apple aiuta a contrastare gli attacchi a prescindere dal fatto che provengano da app dannose, dal web o da qualsiasi altro canale. Le protezioni elencate di seguito sono disponibili sui dispositivi con i SoC Apple supportati, come iOS, iPadOS, tvOS, watchOS e adesso anche macOS sui Mac dotati di chip Apple.

Funzionalità	A10	A11, S3	A12, A13, A14 S4 - S9	A15, A16, A17	M1, M2, M3
Protezione dell'integrità del kernel	✓	✓	✓	✓	✓
Restrizioni rapide dei permessi	✗	✓	✓	✓	✓
Protezione dell'integrità dei coprocessori di sistema	✗	✗	✓	✓	✓
Codici di autenticazione dei puntatori	✗	✗	✓	✓	✓
Page Protection Layer (PPL)	✗	✓	✓	✓	✗ Vedi la nota 1 sotto.
Secure Page Table Monitor	✗	✗	✗	✓ Vedi la nota 2 sotto.	✗

Nota 1: il Page Protection Layer (PPL) richiede che la piattaforma esegua *solo* codice firmato e attendibile. Si tratta di un modello di sicurezza che non è applicabile a macOS.

Nota 2: il Secure Page Table Monitor (SPTM) è supportato su A15, A16 e A17 e sostituisce il Page Protection Layer sulle piattaforme supportate.

Protezione dell’integrità del kernel

Una volta terminata l’inizializzazione del kernel del sistema operativo, viene abilitata la protezione dell’integrità del kernel (KIP, Kernel Integrity Protection) per aiutare a impedire modifiche al codice del kernel e dei driver. Il controller della memoria fornisce un’area di memoria fisica protetta usata da iBoot per caricare il kernel e le estensioni del kernel. Una volta completato l’avvio, il controller della memoria nega la scrittura sulla regione di memoria fisica protetta. L’unità di gestione della memoria del processore per le applicazioni è configurata in modo tale da aiutare a impedire la mappatura di codice con privilegi dalla memoria fisica al di fuori dalla regione di memoria protetta e in modo tale da aiutare a impedire mappature scrivibili della memoria fisica all’interno della regione di memoria del kernel.

Per impedire la riconfigurazione, l’hardware utilizzato per abilitare la protezione dell’integrità del kernel viene bloccato dopo il completamento della procedura di avvio.

Restrizioni rapide dei permessi

A partire dai SoC Apple A11 Bionic e S3, è stato introdotto un nuovo primitivo hardware, le restrizioni rapide dei permessi, che includono un registro CPU che limita velocemente i permessi per thread. Grazie a queste restrizioni rapide dei permessi (conosciute anche come registri APRR), i sistemi operativi supportati possono rimuovere i permessi di esecuzione dalla memoria senza il sovraccarico di una chiamata di sistema e di uno svuotamento o un’analisi della tabella della pagina. Questi registri forniscono un ulteriore livello di protezione dagli attacchi dal web, in particolare per il codice compilato durante il runtime (compilazione “just in time”), perché la memoria non può essere eseguita nello stesso momento in cui è in corso la lettura e la scrittura.

Protezione dell’integrità dei coprocessori di sistema

Il firmware dei coprocessori gestisce molte attività fondamentali del sistema, per esempio Secure Enclave, il processore del sensore di immagini e il coprocessore di movimento. La sua sicurezza è quindi una parte fondamentale della sicurezza del sistema globale. Per impedire la modifica al firmware dei coprocessori, Apple utilizza un meccanismo chiamato *protezione dell’integrità dei coprocessori di sistema (SCIP)*.

Il SCIP funziona in modo simile alla protezione dell’integrità del kernel (KIP): durante l’avvio, iBoot carica il firmware di ciascun coprocessore in una regione di memoria protetta, riservata e separata dalla regione per la protezione dell’integrità del kernel. iBoot configura ciascuna unità di memoria dei coprocessori per aiutare a impedire quanto segue:

- Mappature eseguibili al di fuori della parte di regione di memoria protetta.
- Mappature scrivibili all’interno della parte di regione di memoria protetta.

Inoltre al momento dell’avvio, viene usato il sistema operativo Secure Enclave per configurare il SCIP per Secure Enclave. Una volta completato il processo di avvio, l’hardware utilizzato per abilitare il SCIP viene bloccato. Questo meccanismo è progettato per impedire la riconfigurazione.

Codici di autenticazione dei puntatori

I codici di autenticazione dei puntatori (PAC) sono utilizzati per proteggere contro gli attacchi mirati ai bug di corruzione della memoria. Il software di sistema e le app integrate utilizzano i codici di autenticazione dei puntatori per aiutare a impedire la modifica dei puntatori alle funzioni e degli indirizzi di restituzione (puntatori al codice). Un PAC usa cinque valori segreti a 128 bit per firmare i dati e le istruzioni del kernel, e ogni processo nello spazio utente ha le proprie chiavi B. Agli elementi vengono aggiunti salt e firme come indicato di seguito.

Elemento	Chiave	Salt
Indirizzo di ritorno della funzione	IB	Indirizzo archiviazione
Puntatori funzione	IA	0
Funzione di richiamo del blocco	IA	Indirizzo archiviazione
Cache metodo Objective-C	IB	Indirizzo archiviazione + Classe + Selettore
Voci V-Table C++	IA	Indirizzo archiviazione + Hash (nome metodo mangled)
Etichetta Goto calcolata	IA	Hash (nome funzione)
Stato thread del kernel	GA	•
Registri stato thread dell'utente	IA	Indirizzo archiviazione
Puntatori V-Table C++	DA	0

Il valore della firma è archiviato nei bit di inserimento inutilizzati all'inizio del puntatore a 64 bit. La firma viene verificata prima dell'uso e l'inserimento viene ripristinato per aiutare a garantire il funzionamento dell'indirizzo del puntatore. Se la verifica non va a buon fine, l'operazione viene interrotta. Questa verifica aumenta la difficoltà di molti attacchi come ad esempio un attacco basato sul return oriented programming, che tenta di ingannare il dispositivo in modo tale che esegua del codice in maniera dannosa manipolando gli indirizzi di ritorno delle funzioni archiviati sullo stack.

Page Protection Layer (PPL)

Il Page Protection Layer (PPL) in iOS, iPadOS e watchOS è progettato per proteggere il codice dello spazio utente dalle modifiche una volta che è stato completato il processo di verifica della firma. Basandosi sulla protezione dell'integrità del kernel e sulle restrizioni veloci alle autorizzazioni, il PPL gestisce gli override dei permessi della tabella della pagina per garantire che le pagine protette contenenti codice utente e le tabelle delle pagine possano essere modificate unicamente dal PPL. Il sistema fornisce una riduzione massiva della superficie di attacco supportando l'applicazione dell'integrità del codice su tutto il sistema, anche di fronte a un kernel compromesso. Il PPL non è offerto in macOS perché è applicabile solo ai sistemi in cui tutto il codice deve essere firmato.

Secure Page Table Monitor e Trusted Execution Monitor

Secure Page Table Monitor (SPTM) e Trusted Execution Monitor (TXM) sono concepiti per funzionare insieme poiché contribuiscono a proteggere da modifica le page table per i processi sia utente che per il kernel, anche quando gli hacker dispongono di capacità di scrittura a livello di kernel e sono in grado di aggirare le protezioni del flusso di controllo. STPM usufruisce di un livello di privilegi superiore rispetto al kernel e utilizza il TXM con privilegi inferiori per applicare le politiche che governano l'esecuzione del codice. Questo sistema è concepito in modo da evitare che la manomissione del TXM comporti automaticamente l'aggiramento dell'SPM, grazie alla separazione dei privilegi e alla gestione dell'affidabilità tra di loro. Nei SOC di A15, A16, e A17, SPTM (insieme a TXM) sostituisce PPL, poiché offre una superficie di attacco più piccola, che non si basa sull'attendibilità del kernel, anche durante le prime fasi dell'avvio. Inoltre, SPTM si basa su nuovi primitivi del chip che rappresentano un'evoluzione delle restrizioni rapide dei permessi utilizzate da PPL.

Attivazione sicura delle connessioni dati

Su iPhone, su iPad e sui Mac, se recentemente non sono stati stabiliti collegamenti dati, gli utenti devono utilizzare Face ID, Touch ID o il codice per attivare un collegamento dati tramite un cavo Thunderbolt, Lightning, USB o Smart Connector oppure su macOS 13.3 o versioni successive, tramite l'interfaccia a schede SD Extended Capacity (SDXC). Questo limita la possibilità di attacco per mezzo di dispositivi collegati fisicamente come caricatori dannosi, permettendo al tempo stesso di utilizzare altri accessori entro limiti di tempo ragionevoli. Se è trascorsa più di un'ora da quando iPhone o iPad è stato bloccato o da quando si è concluso il collegamento dati di un accessorio, il dispositivo non consentirà nuovi collegamenti dati finché non verrà sbloccato. Durante questo periodo di un'ora, verranno consentiti solo i collegamenti dati da accessori che sono stati precedentemente connessi al dispositivo mentre questo era sbloccato. Tali accessori verranno ricordati per 30 giorni dall'ultima volta che sono stati collegati. I tentativi da parte di un accessorio sconosciuto di aprire un collegamento dati durante questo periodo causerà la disattivazione di tutti i collegamenti dati tramite accessori finché il dispositivo non verrà di nuovo sbloccato. Questo periodo di un'ora:

- Aiuta a garantire che gli utenti che si collegano frequentemente a un Mac o a un PC, ad accessori o a CarPlay tramite cavo non debbano inserire il codice ogni volta che collegano i propri dispositivi.
- È necessario, perché l'ecosistema degli accessori non fornisce un metodo crittografico affidabile per l'identificazione dell'accessorio stesso prima di aver stabilito un collegamento dati.

Inoltre, se sono trascorsi più di 3 giorni dall'ultima volta che è stato stabilito un collegamento dati con un accessorio, il dispositivo impedirà nuovi collegamenti subito dopo il blocco. Ciò serve ad aumentare la protezione per gli utenti che non utilizzano tali accessori frequentemente. Tali collegamenti dati sono disabilitati ogni volta che il dispositivo si trova in uno stato che richiede un codice per riabilitare l'autenticazione tramite rilevamenti biometrici.

L'utente può scegliere di abilitare nuovamente i collegamenti dati sempre attivi in Impostazioni e può configurare alcuni dispositivi di tecnologia assistiva perché lo facciano automaticamente.

Verifica degli accessori per iPhone e iPad

Il programma di licenze MFi (Made for iPhone, Made for iPad) fornisce ai produttori di accessori verificati l'accesso al protocollo iAP (iPod Accessories Protocol) oltre che ai componenti di supporto hardware necessari.

Quando un accessorio MFi comunica con un iPhone o un iPad, l'accessorio deve dimostrare ad Apple che è stato verificato. La connessione tra accessorio e dispositivo deve essere stabilita tramite cavo Thunderbolt o Lightning o connessione Bluetooth oppure, per alcuni dispositivi, tramite USB-C. Come prova dell'autorizzazione, l'accessorio invia un certificato fornito da Apple stessa, che viene poi verificato dal dispositivo. Il dispositivo invia successivamente una richiesta a cui l'accessorio deve rispondere con una risposta firmata. Questo processo è interamente gestito da un circuito integrato personalizzato che Apple fornisce ai produttori di accessori approvati e che è trasparente all'accessorio stesso.

Gli accessori MFi verificati possono richiedere l'accesso a metodi di trasporto e funzionalità diversi, come ad esempio l'accesso a streaming audio digitali tramite cavo Thunderbolt oppure le informazioni di localizzazione fornite tramite Bluetooth. Un circuito integrato di autenticazione è progettato per garantire che il pieno accesso al dispositivo venga concesso solo agli accessori approvati. Se un accessorio non supporta l'autenticazione, il suo accesso verrà limitato all'audio analogico e a un numero limitato di controlli di riproduzione audio seriali (UART).

Anche AirPlay utilizza l'autenticazione con circuito integrato per verificare che i ricevitori siano stati approvati da Apple. Gli streaming audio di AirPlay e video di CarPlay utilizzano il protocollo MFi-SAP (Secure Association Protocol), che codifica la comunicazione tra l'accessorio e il dispositivo utilizzando AES128 in modalità CTR. Le chiavi effimere sono scambiate usando lo scambio di chiavi ECDH (Curve25519) e firmate utilizzando la chiave RSA a 1024 bit del circuito integrato di autenticazione come parte del protocollo STS (Station-to-Station).

BlastDoor per Messaggi e IDS

iOS, iPadOS, macOS e watchOS sono dotati di una funzionalità di sicurezza chiamata *BlastDoor*, che è stata introdotta a partire da iOS 14 e release correlate. L'obiettivo di BlastDoor è proteggere il sistema, isolando gli hacker e chiedendo loro un maggiore impegno nel tentare di sfruttare Messaggi e gli Apple Identity Services (IDS). BlastDoor isola, analizza, transcodifica e convalida i dati non affidabili che arrivano tramite Messaggi, IDS e altri vettori per prevenire gli attacchi informatici.

BlastDoor adotta le limitazioni in sandboxing e la convalida della sicurezza della memoria dell'output ponendo un ostacolo difficile da superare per gli hacker, prima che possano raggiungere altre parti del sistema operativo. È una funzionalità concepita per aumentare in modo considerevole la protezione dagli attacchi informatici, in particolare da quelli zero-clic, ossia che non richiedono alcuna interazione da parte dell'utente.

Infine, Messaggi è in grado di distinguere tra traffico proveniente da mittenti conosciuti e quello proveniente da mittenti sconosciuti e offre funzionalità diverse per ciascun raggruppamento, poiché segmenta i dati "noti" e quelli "sconosciuti" in istanze separate di BlastDoor.

Sicurezza della “Modalità di isolamento” per i dispositivi Apple

“Modalità di isolamento” è una funzionalità di sicurezza opzionale ed estrema, concepita per un numero molto ristretto di utenti che, in ragione della loro identità o della loro professione, potrebbero venire presi di mira dalle minacce informatiche più sofisticate, come lo spyware mercenario. La maggioranza degli utenti non subirà mai attacchi di questo tipo.

Quando “Modalità di isolamento” è attiva, il dispositivo non funziona più normalmente. Al fine di ridurre la superficie di attacco che potrebbe venire sfruttata, l’utilizzo di determinate app, siti web e funzionalità è molto limitato per motivi di sicurezza e alcune esperienze potrebbero non essere affatto disponibili.

“Modalità di isolamento” è disponibile in iOS 16, iPadOS 16, macOS 13 e watchOS 10 o versioni successive. “Modalità di isolamento” è disponibile in iOS 17, iPadOS 17, macOS 14 e negli aggiornamenti di watchOS 10.1 o versioni successive. Per utilizzare a pieno le funzionalità aggiuntive di “Modalità di isolamento”, è consigliabile aggiornare i dispositivi all’ultima versione del sistema operativo. Per ulteriori informazioni, consulta l’articolo del supporto Apple Informazioni sulla modalità di isolamento.

“Modalità di isolamento” implementa delle misure per aumentare la sicurezza che riducono funzionalità, prestazioni o entrambe. Tali misure influiscono su:

- Servizi in background
- Connettività
- Gestione dei dispositivi
- FaceTime
- Game Center
- Mail
- Messaggi
- Foto
- Safari
- Impostazioni di Sistema
- WebKit

Funzionalità aggiuntive di sicurezza del sistema di macOS

Funzionalità aggiuntive di sicurezza del sistema di macOS

macOS opera su un'architettura hardware più varia (ad esempio, processori Intel, processori Intel in combinazione con il chip di sicurezza Apple T2 e SoC Apple) e supporta una gamma di utilizzi più generali. Mentre alcuni utenti utilizzano solo le app di base preinstallate o quelle disponibili su App Store, altri utenti arrivano a intervenire sul kernel e hanno quindi bisogno di disabilitare essenzialmente tutte le protezioni della piattaforma per poter eseguire e testare il proprio codice con il più alto livello di attendibilità. Gran parte degli utenti rientrano in una categoria intermedia e molti di essi hanno periferiche e software che richiedono vari livelli di accesso. Apple ha ideato la piattaforma macOS con un approccio integrato rispetto a software, hardware e servizi, offrendo un prodotto sicuro già a partire dalla progettazione e semplice da configurare, distribuire e gestire, pur mantenendo la configurabilità che gli utenti si aspettano. macOS include anche le tecnologie di sicurezza chiave necessarie a un professionista dell'IT per contribuire alla protezione dei dati della propria azienda e all'integrazione in ambienti di networking aziendali sicuri.

Le seguenti funzionalità supportano e aiutano a rendere sicure le varie necessità degli utenti di macOS. Esse includono:

- Sicurezza del volume di sistema firmato
- Protezione dell'integrità del sistema
- Cache di attendibilità
- Protezione per le periferiche
- Supporto e sicurezza per Rosetta 2 (traduzione automatica) per i Mac dotati di chip Apple
- Supporto e protezioni DMA
- Supporto e sicurezza per le estensioni del kernel
- Supporto e sicurezza per la ROM opzionale
- Sicurezza del firmware UEFI per i Mac dotati di processore Intel

Protezione dell’integrità del sistema

macOS utilizza i permessi del kernel per limitare la capacità di scrittura su file di sistema critici, tramite una funzionalità chiamata *protezione dell’integrità del sistema (SIP)*. Questa è una funzionalità distinta e aggiuntiva rispetto alla protezione dell’integrità del kernel, basata sull’hardware e disponibile sui Mac dotati di chip Apple, che protegge la modifica del kernel in memoria. Per fornire tale protezione vengono implementati i controlli di accesso obbligatori e una gamma di protezioni a livello di kernel, tra cui il sandboxing e i data vault.

Controlli di accesso obbligatori

macOS utilizza i controlli di accesso obbligatori, ossia delle politiche che impostano le restrizioni di sicurezza, create dallo sviluppatore, che non possono essere ignorate. Questo approccio è diverso da quello dei controlli di accesso discrezionali, che consentono agli utenti di ignorare le politiche di sicurezza in base alle preferenze individuali.

I controlli di accesso obbligatori non sono visibili agli utenti, ma rappresentano la tecnologia soggiacente che contribuisce all’abilitazione di diverse importanti funzionalità, tra cui sandbox, controlli parentali, preferenze gestite, estensioni e protezione dell’integrità del sistema.

Protezione dell’integrità del sistema

La *protezione dell’integrità del sistema* limita a sola lettura i componenti situati in determinate posizioni critiche del file system, per aiutare a impedire che tali componenti possano essere modificati da codice dannoso. La protezione dell’integrità del sistema è un’impostazione specifica per ogni computer che è attiva di default quando un utente esegue l’aggiornamento a OS X 10.11 o versioni successive. Sui Mac dotati di processore Intel, la disabilitazione di tale opzione rimuove la protezione per tutte le partizioni esistenti sul dispositivo di archiviazione fisica. macOS applica questa politica di sicurezza a tutti i processi in esecuzione sul sistema, a prescindere dal fatto che abbiano privilegi amministrativi o siano eseguiti in sandbox.

Cache di attendibilità

Uno degli oggetti inclusi nella catena di avvio protetto è la cache di attendibilità statica, un record attendibile di tutti i binari Mach-O salvati nel volume di sistema firmato. Ciascun Mach-O è rappresentato da un hash di directory di codice. Per rendere efficiente la ricerca, tali hash vengono ordinati prima di essere inseriti nella cache di attendibilità. La directory di codice è il risultato dell'operazione di firma eseguita da `codesign(1)`. Per implementare la cache di attendibilità, la protezione dell'integrità del sistema deve rimanere abilitata. Per poter disabilitare l'implementazione della cache di attendibilità sui Mac dotati di chip Apple, l'avvio protetto deve essere impostato su "Sicurezza assente".

Quando viene eseguito un binario (sia che generi un nuovo processo o che mappi del codice eseguibile in un processo esistente), viene estratta la relativa directory di codice a cui viene applicato un hash. Se l'hash risultante viene trovato nella cache di attendibilità, alle mappature eseguibili create per il binario verranno concessi i privilegi da piattaforma, ovvero possono avere qualsiasi permesso ed essere eseguite senza ulteriori verifiche di autenticità della firma. Ciò è in contrasto con quello che si verifica sui Mac dotati di processore Intel, dove i privilegi da piattaforma vengono concessi al contenuto del sistema operativo dal certificato Apple che firma i binari. (Questo certificato non pone restrizioni sui permessi che il binario potrebbe avere).

I binari non appartenenti alla piattaforma (ad esempio, codice autenticato di terze parti) devono avere catene di certificati valide per poter essere eseguiti e i permessi che potrebbero avere sono limitati dal profilo di firma emesso dall'Apple Developer Program allo sviluppatore.

Tutti i binari inclusi all'interno di macOS sono firmati con un *identificativo di piattaforma*. Sui Mac dotati di chip Apple, tale identificativo è utilizzato per indicare che, nonostante il binario sia firmato da Apple, il relativo hash della directory di codice deve essere presente nella cache di attendibilità perché possa essere eseguito. Sui Mac dotati di processore Intel, l'identificativo di piattaforma è utilizzato per eseguire una revoca mirata dei binari da versioni meno recenti di macOS; tale revoca mirata aiuta a impedirne l'esecuzione sulle versioni più recenti.

La cache di attendibilità vincola completamente un insieme di binari a una determinata versione di macOS. Ciò aiuta a impedire che binari legittimamente firmati da Apple provenienti da sistemi operativi meno recenti vengano introdotti da un hacker in versioni più nuove per trarne vantaggio.

Codice di piattaforma fornito al di fuori del sistema operativo

Apple fornisce alcuni binari (come ad esempio Xcode e l'insieme degli strumenti di sviluppo) che non sono firmati con un identificativo di piattaforma. Tuttavia, essi possono essere eseguiti con privilegi di piattaforma sui Mac dotati di chip Apple e sui Mac con chip T2. Dal momento che tale software di piattaforma viene fornito in maniera indipendente da macOS, non è soggetto alle metodologie di revoca imposte dalla cache di attendibilità statica.

Cache di attendibilità caricabili

Apple fornisce alcuni pacchetti software con delle *cache di attendibilità caricabili*. Tali cache hanno la stessa struttura di dati della cache di attendibilità statica. Ma sebbene vi sia una sola cache di attendibilità statica e i suoi contenuti siano sempre bloccati in intervalli di sola lettura dopo il completamento dell'inizializzazione iniziale del kernel, le cache di attendibilità caricabili vengono aggiunte al sistema in fase di esecuzione.

Queste cache di attendibilità vengono autenticate tramite lo stesso meccanismo che autentica il firmware di avvio (personalizzazione tramite il servizio di firma attendibile di Apple) oppure vengono autenticate come oggetti firmati globali (le cui firme non li legano a un particolare dispositivo).

Un esempio di cache di attendibilità personalizzata è quella fornita con l'immagine disco utilizzata per eseguire la diagnosi sui Mac dotati di chip Apple. Questa cache è personalizzata, insieme all'immagine disco, e caricata nel kernel del Mac mentre questo viene avviato in modalità di diagnosi. La cache di attendibilità consente al software all'interno dell'immagine disco di essere eseguito con privilegi da piattaforma.

Un esempio di cache di attendibilità firmata globalmente è fornita con gli aggiornamenti software di macOS. Questa cache di attendibilità consente a una parte del codice dell'aggiornamento software (la *parte principale*) di essere eseguita con privilegi da piattaforma. La parte principale effettua tutte quelle operazioni necessarie all'aggiornamento software che il sistema host non è in grado di eseguire in modo coerente tra una versione e l'altra.

Sicurezza dei processori delle periferiche nei computer Mac

Tutti i moderni sistemi informatici hanno vari processori per le periferiche integrate, dedicati ad attività come networking, grafica, gestione dell'energia e altro ancora. Tali processori delle periferiche sono spesso destinati a un solo scopo e sono molto meno potenti della CPU principale. Le periferiche integrate che non implementano un livello di sicurezza sufficiente diventano un facile obiettivo per gli hacker, che tramite esse possono infettare in maniera persistente il sistema operativo. Dopo aver infettato il firmware di un processore, l'hacker potrebbe puntare al software presente sulla CPU principale oppure acquisire direttamente dei dati sensibili (ad esempio, un dispositivo Ethernet potrebbe visualizzare i contenuti dei pacchetti non codificati).

Apple si impegna a ridurre, dove possibile, il numero di processori di periferiche necessari o a evitare progettazioni che richiedano dei firmware. Tuttavia, quando sono necessari dei processori secondari con il proprio firmware, vengono adottate tutte le misure possibili per fare in modo che un eventuale hacker non possa attaccare tali processori. Ciò si può ottenere verificando il processore in uno dei seguenti due modi:

- Eseguendo il processore in una modalità che preveda il download del firmware verificato dalla CPU principale all'avvio.
- Facendo in modo che il processore della periferica implementi la propria catena di avvio protetto per verificare il proprio firmware ogni volta che il Mac si avvia.

Apple collabora con i fornitori per verificare le loro implementazioni e per migliorare la progettazione in modo da includere proprietà desiderate, quali:

- Garanzia di forza di crittografia minima
- Revoca solida di firmware noto come dannoso
- Disabilitazione delle interfacce di debug

- Firma del firmware con le chiavi di codifica archiviate nei moduli di sicurezza hardware (HSM) controllati da Apple

Di recente Apple ha lavorato con alcuni fornitori esterni per adottare infrastruttura di firma, codice di verifica e strutture di dati "Image4" uguali a quelli utilizzati dai chip Apple.

Quando non sono disponibili né il funzionamento senza archiviazione né l'archiviazione con avvio protetto, il design richiede necessariamente che gli aggiornamenti firmware siano firmati tramite crittografia e verificati prima che sia possibile aggiornare l'archiviazione persistente.

Rosetta 2 sui Mac dotati di chip Apple

I Mac dotati di chip Apple sono in grado di eseguire il codice compilato per il set di istruzioni x86_64 utilizzando un meccanismo di traduzione chiamato *Rosetta 2*. I tipi di traduzione offerti sono due: JIT (Just In Time) e AOT (Ahead OF Time).

Traduzione JIT (Just In Time)

Nel flusso di traduzione JIT, un oggetto Mach x86_64 viene identificato in precedenza nel percorso di esecuzione dell'immagine. Quando tali immagini vengono incontrate, il kernel trasferisce il controllo a una speciale porzione di Rosetta responsabile della traduzione piuttosto che all'editor dei link dinamici `dyld(1)`. La porzione responsabile della traduzione traduce le pagine x86_64 durante l'esecuzione dell'immagine. La traduzione avviene interamente all'interno del processo. Il kernel verifica comunque gli hash del codice di ciascuna pagina x86_64 tramite la firma allegata al binario. Nel caso di una mancata corrispondenza tra gli hash, il kernel implementa le politiche di rimedio appropriate per tale processo.

Traduzione AOT (Ahead OF Time)

Nella procedura di traduzione AOT, i binari x86_64 vengono letti dallo spazio di archiviazione in momenti che il sistema ritiene ottimali per la reattività di tale codice. Gli artefatti tradotti vengono scritti sullo spazio di archiviazione come un tipo speciale di file di oggetto Mach. Tale file è simile a un'immagine eseguibile, ma è contrassegnato in modo da indicare che si tratta della traduzione di un'altra immagine.

In questo modello, l'artefatto AOT prende tutte le informazioni della sua identità dall'immagine eseguibile x86_64 originale. Per implementare questo legame, un'entità dello spazio utente privilegiata firma l'artefatto tradotto tramite una chiave specifica per il dispositivo che è gestita da Secure Enclave. Questa chiave viene rilasciata solo all'entità dello spazio utente privilegiata, che è identificata come tale tramite un permesso limitato. La directory di codice creata per l'artefatto tradotto include l'hash della directory di codice dell'immagine eseguibile x86_64 originale. La firma dell'artefatto tradotto stesso è conosciuta come *firma supplementare*.

Il flusso di traduzione AOT inizia in modo simile a quello JIT, con il kernel che trasferisce il controllo a Rosetta piuttosto che all'editor dei link dinamici `dyld(1)`. Ma in questo caso, successivamente Rosetta invia una richiesta di comunicazione tra processi al servizio di sistema di Rosetta, il quale controlla se è disponibile una traduzione AOT per l'attuale immagine eseguibile. Se viene trovata, il servizio di Rosetta fornisce un collegamento a tale traduzione e questa viene mappata nel processo ed eseguita. Durante l'esecuzione, il kernel implementa gli hash della directory di codice dell'artefatto tradotto, che sono autenticati dalla firma che ha la propria radice nella chiave specifica per il dispositivo. Gli hash della directory di codice dell'immagine x86_64 originale non sono coinvolti in questo processo.

Gli artefatti tradotti sono archiviati in un data vault non accessibile in runtime da nessuna entità, tranne che dal servizio di Rosetta. Il servizio di Rosetta gestisce l'accesso alla propria cache distribuendo descrittori di file di sola lettura ad artefatti tradotti individuali; ciò limita l'accesso alla cache degli artefatti AOT. La comunicazione tra processi del servizio e gli elementi dipendenti sono intenzionalmente ristretti per limitare le possibilità di attacco.

Se l'hash della directory di codice dell'immagine x86_64 originale non corrisponde a quello codificato nella firma dell'artefatto tradotto AOT, il risultato viene considerato equivalente a una firma del codice non valida e vengono implementate le misure appropriate.

Se un processo remoto richiede al kernel dei permessi o altre proprietà di identità del codice di un eseguibile tradotto in modalità AOT, vengono restituite le proprietà dell'identità dell'immagine x86_64 originale.

Contenuti della cache di attendibilità statica

macOS 11 o versioni successive viene fornito con binari Mach "multiarchitettura", che contengono porzioni di codice macchina sia x86_64 che arm64. Sui Mac dotati di chip Apple, l'utente potrebbe scegliere di eseguire il codice x86_64 di un binario di sistema tramite il flusso di Rosetta, ad esempio per caricare un plugin che non ha una variante arm64 nativa. Per supportare questa opzione, la cache di attendibilità statica fornita con macOS, in linea generale, contiene tre hash di directory di codice per file di oggetto Mach.

- Un hash della directory di codice della porzione arm64
- Un hash della directory di codice della porzione x86_64
- Un hash della directory di codice della traduzione AOT della porzione x86_64

La procedura di traduzione di Rosetta è deterministica, nel senso che riproduce un output identico per ciascun input dato, a prescindere dal momento in cui la traduzione è stata effettuata o su quale dispositivo.

Durante il processo di build di macOS, ogni file di oggetto Mach viene tradotto tramite il flusso di Rosetta associato alla versione di macOS in fase di build e l'hash della directory del codice risultante viene registrato nella cache di attendibilità. Per ragioni di efficienza, i prodotti tradotti non vengono forniti con il sistema operativo e vengono realizzati su richiesta dell'utente.

Quando un'immagine x86_64 è in esecuzione su un Mac dotato di chip Apple, se l'hash della directory di tale codice si trova nella cache di attendibilità statica, è previsto che *anche* l'hash della directory del codice dell'artefatto AOT risultante si trovi nella cache di attendibilità statica. Tali prodotti non sono firmati dalla chiave specifica per il dispositivo, perché l'autorità per la firma ha la propria radice nella catena di avvio protetto di Apple.

Codice x86_64 non firmato

I Mac dotati di chip Apple non consentono l'esecuzione di codice nativo arm64 se non vi è allegata una firma valida. Questa può essere anche una semplice firma "ad hoc" (vedi `codesign(1)`) che non contiene nessuna informazione di identità dalla metà segreta della coppia di chiavi asimmetrica (è semplicemente una misurazione autenticata del binario).

Per questioni di compatibilità dei binari, il codice x86_64 tradotto può essere eseguito tramite Rosetta senza alcuna informazione riguardante la firma. La procedura di firma di Secure Enclave specifica per il dispositivo non fornisce alcuna identità a tale codice, che viene eseguito esattamente con le stesse limitazioni del codice nativo non firmato in esecuzione sui Mac dotati di processore Intel.

Protezioni dell’accesso diretto alla memoria per i computer Mac

Per ottenere una capacità di trasmissione maggiore su interfacce come PCIe, FireWire, Thunderbolt e USB, i computer devono supportare l’accesso diretto alla memoria (DMA) delle periferiche, ossia queste ultime devono essere in grado di leggere e scrivere sulla RAM senza il coinvolgimento continuo della CPU. Dal 2012, sui computer Mac sono state implementate numerose tecnologie per la protezione DMA, che ad oggi rappresentano l’insieme di protezioni DMA migliore e più completo disponibile su qualsiasi personal computer.

Protezioni dell’accesso diretto alla memoria per i Mac dotati di chip Apple

I SoC Apple contengono un’unità per la gestione della memoria di input/output per ciascun agente DMA nel sistema, incluse le porte PCIe e Thunderbolt. Dal momento che ogni unità per la gestione della memoria di input/output ha il proprio insieme di tabelle per la traduzione degli indirizzi per le richieste DMA, le periferiche connesse tramite PCIe o Thunderbolt possono accedere solo alla memoria che è stata esplicitamente associata al loro utilizzo. Le periferiche non possono accedere alla memoria che appartiene ad altre parti del sistema, come il kernel o il firmware, o alla memoria assegnata ad altre periferiche. Se un’unità per la gestione della memoria di input/output rileva il tentativo di una periferica di accedere a una parte di memoria che non le è stata associata, viene attivato un kernel panic.

Protezioni dell’accesso diretto alla memoria sui Mac dotati di processore Intel

I Mac dotati di processore Intel con Tecnologia di virtualizzazione per I/O diretti (VT-d) di Intel inizializzano l’unità per la gestione della memoria di input/output, abilitando la rimappatura DMA e la rimappatura degli interrupt, nelle primissime fasi del processo di avvio, così da mitigare varie classi di vulnerabilità di sicurezza. L’hardware dell’unità per la gestione della memoria di input/output di Apple avvia le proprie operazioni con una politica che nega di default le richieste, quindi nell’istante in cui il sistema viene acceso, inizia automaticamente a bloccare le richieste DMA dalle periferiche. Una volta inizializzata dal software, l’unità per la gestione della memoria di input/output inizia a consentire le richieste DMA dalle periferiche alle regioni di memoria che sono state loro esplicitamente associate.

Nota: la rimappatura degli interrupt per le porte PCIe non è necessaria sui Mac dotati di chip Apple perché ciascuna unità per la gestione della memoria di input/output gestisce gli MSI per le proprie periferiche.

A partire da macOS 11, tutti i Mac dotati di chip di sicurezza Apple T2 eseguono driver UEFI che facilitano l’accesso diretto alla memoria in un ambiente con livello 3 di protezione quando tali driver eseguono l’abbinamento con dispositivi esterni. Questa proprietà aiuta a mitigare le vulnerabilità di sicurezza che potrebbero verificarsi quando un dispositivo dannoso interagisce con un driver UEFI in modo inatteso durante l’avvio. In particolare, riduce l’impatto delle vulnerabilità nella gestione da parte dei driver dei buffer di accesso diretto alla memoria.

Estensione sicura del kernel in macOS

A partire da macOS 11, se le estensioni del kernel di terze parti sono abilitate, non possono essere caricate nel kernel su richiesta. Vengono invece unite in una *raccolta del kernel ausiliaria*, che viene caricata durante il processo di avvio. Per i Mac dotati di chip Apple, la misurazione della raccolta del kernel ausiliaria viene firmata in LocalPolicy (per i modelli di hardware precedenti la raccolta del kernel ausiliaria risiedeva nel volume dedicato ai dati). La ricostruzione della raccolta del kernel ausiliaria richiede l'approvazione dell'utente e il riavvio di macOS per caricare le modifiche nel kernel; richiede inoltre che l'avvio protetto sia configurato su "Sicurezza ridotta".

Importante: le estensioni del kernel non sono più consigliate per macOS. Le estensioni del kernel mettono a repentaglio l'integrità e l'affidabilità del sistema operativo; Apple consiglia agli utenti di optare per soluzioni che non richiedano l'estensione del kernel.

Estensioni del kernel sui Mac dotati di chip Apple

Nei Mac dotati di chip Apple, le estensioni del kernel devono essere abilitate esplicitamente tenendo premuto il tasto di accensione durante l'avvio per entrare in modalità One True Recovery (1TR), scegliendo l'opzione "Sicurezza ridotta" e selezionando il riquadro per abilitarle. Questa azione richiede anche l'inserimento di una password da amministratore per autorizzare la riduzione del livello di sicurezza. La combinazione di modalità 1TR e richiesta della password rendono difficile a un hacker che effettui un attacco solo al software a partire da macOS applicare estensioni del kernel al sistema operativo per poi sfruttarle per ottenere privilegi kernel.

Una volta che un utente ha autorizzato il caricamento delle estensioni del kernel, per autorizzare l'installazione delle stesse viene utilizzata la procedura di caricamento delle estensioni del kernel approvate dall'utente descritta sopra. L'autorizzazione utilizzata per la procedura descritta viene usata anche per registrare un hash SHA384 dell'elenco delle estensioni del kernel autorizzate dall'utente in LocalPolicy. Successivamente, il deamon di gestione del kernel (`kmd`) si occupa di convalidare solo le estensioni del kernel presenti nell'elenco delle estensioni del kernel autorizzate dall'utente per essere incluse nella raccolta del kernel ausiliaria.

- Se la protezione dell'integrità del sistema è abilitata, prima dell'inclusione nella raccolta del kernel ausiliaria, viene verificata la firma di ogni estensione del kernel.
- Se la protezione dell'integrità del sistema è disabilitata, la firma delle estensioni del kernel non è richiesta.

Questo approccio consente operazioni in modalità "Sicurezza assente" in cui sviluppatori o clienti che non fanno parte dell'Apple Developer Program testano le estensioni del kernel prima che vengano firmate.

Dopo che la raccolta del kernel ausiliaria è stata creata, la relativa misurazione viene inviata a Secure Enclave perché venga firmata e inclusa in una struttura di dati Image4 che possa essere valutata da iBoot durante l'avvio. Durante la creazione della raccolta del kernel ausiliaria, viene generata anche una ricevuta per le estensioni del kernel. Essa contiene l'elenco delle estensioni del kernel effettivamente incluse nella raccolta del kernel ausiliaria, perché potrebbe essere un sottoinsieme dell'elenco delle estensioni del kernel autorizzate dall'utente se sono state trovate estensioni del kernel non autorizzate. Un hash SHA384 della struttura di dati Image4 della raccolta del kernel ausiliaria e la ricevuta delle estensioni del kernel vengono inclusi in LocalPolicy. L'hash Image4 della raccolta del kernel ausiliaria viene utilizzato per un'ulteriore verifica da parte di iBoot all'avvio, per aiutare a garantire che non sia possibile avviare un file Image4 della raccolta del kernel ausiliaria meno recente firmato da Secure Enclave con un LocalPolicy più recente. La ricevuta delle estensioni del kernel è usata da sottosistemi come Apple Pay per determinare se ci sono estensioni del kernel attualmente caricate che possano interferire con l'attendibilità di macOS. Se sono presenti, le funzionalità di Apple Pay potrebbero venire disabilitate.

Estensioni di sistema

macOS 10.15 consente agli sviluppatori di ampliare le funzionalità di macOS installando e gestendo le estensioni di sistema eseguite sullo spazio utente piuttosto che al livello del kernel. Se eseguite sullo spazio utente, le estensioni di sistema aumentano la stabilità e la sicurezza di macOS. Sebbene le estensioni del kernel abbiano accesso per definizione all'intero sistema operativo, quelle eseguite sullo spazio utente ricevono unicamente i privilegi necessari all'esecuzione della loro funzione specifica.

Gli sviluppatori possono utilizzare i framework, come DriverKit, EndpointSecurity e NetworkExtension, per scrivere su driver UI e USB, strumenti di sicurezza endpoint (come la prevenzione della perdita di dati o altri agenti endpoint) nonché strumenti di rete e VPN, il tutto senza dover scrivere delle estensioni del kernel. Gli agenti di sicurezza di terze parti dovrebbero essere utilizzati solo se sfruttano queste API o se hanno una solida roadmap di transizione verso di esse e di allontanamento dalle estensioni del kernel.

Caricamento delle estensioni del kernel approvate dall'utente

Per migliorare la sicurezza, per il caricamento delle estensioni del kernel installate con o dopo aver installato macOS 10.13 è necessario il consenso dell'utente. Questo processo è noto come *caricamento delle estensioni del kernel approvate dall'utente*. Per l'approvazione di un'estensione del kernel è necessaria l'autorizzazione di un amministratore. Le estensioni del kernel non richiedono autorizzazione se:

- Sono installate su un Mac con macOS 10.12 o versioni precedenti.
- Sostituiscono delle estensioni approvate in precedenza.
- Possono essere caricate senza il consenso dell'utente usando lo strumento a linea di comando `spctl` disponibile quando il Mac è avviato da recoveryOS.
- Possono essere caricate tramite una configurazione MDM (Mobile Device Management).

  A partire da macOS 10.13.2, gli utenti possono usare la MDM per indicare un elenco di estensioni del kernel che può essere caricato senza il consenso dell'utente. Questa opzione richiede un Mac con macOS 10.13.2 registrato in una soluzione MDM effettuata dall'utente oppure tramite Apple School Manager o Apple Business Manager.

Sicurezza della ROM opzionale in macOS

Nota: le ROM opzionali non sono attualmente supportate sui Mac dotati di chip Apple.

Sicurezza della ROM opzionale sui Mac con chip di sicurezza Apple T2

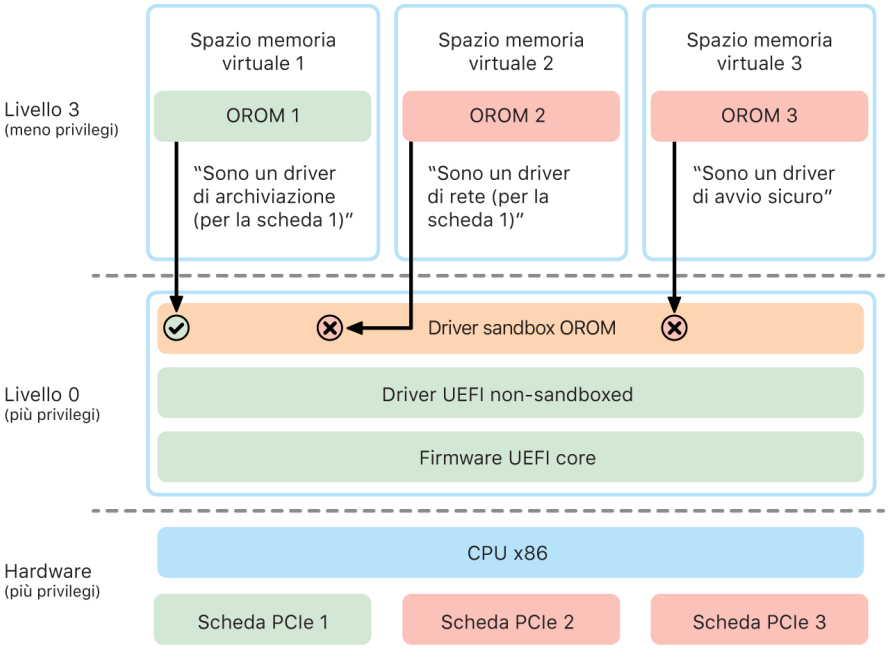
Sia i dispositivi Thunderbolt che PCIe possono avere una ROM opzionale (OROM) collegata fisicamente al dispositivo (in genere non si tratta di una vera e propria ROM, ma di un chip riscrivibile che contiene il firmware). Sui sistemi basati su UEFI, tale firmware normalmente è un driver UEFI, che viene letto dal firmware UEFI ed eseguito. Il codice eseguito deve inizializzare e configurare l'hardware da cui viene recuperato, in modo da renderlo utilizzabile dal resto del firmware. Si tratta di una funzionalità necessaria perché l'hardware specializzato di terze parti possa essere caricato e funzionare durante le prime fasi di avvio, per esempio per l'avvio da array RAID esterni.

Tuttavia, dal momento che le ROM opzionali sono generalmente riscrivibili, se un hacker sovrascrive la ROM opzionale di una periferica valida, il suo codice verrà eseguito nelle prime fasi del processo di avvio, consentendogli di alterare l'ambiente di esecuzione e di violare l'integrità del software caricato successivamente. Allo stesso modo, se l'hacker introduce il proprio codice dannoso nel sistema, sarà in grado anche di eseguire del codice dannoso.

In macOS 10.12.3, il comportamento dei computer Mac immessi sul mercato dopo il 2011 è stato modificato per non eseguire le ROM opzionali di default al momento dell'avvio del Mac, salvo nei casi in cui viene premuta una determinata combinazione di tasti. In questo modo i computer venivano protetti dall'immissione involontaria di OROM dannose nella sequenza di avvio di macOS. È stato modificato anche il comportamento di default di Utility Password Firmware in modo che, quando l'utente impostava una password per il firmware, le OROM non potessero essere eseguite anche se la combinazione di tasti era premuta. Questa misura di sicurezza proteggeva nei casi in cui un hacker, fisicamente presente, tentasse di introdurre un'OROM dannosa. Gli utenti che devono comunque eseguire le OROM quando hanno una password del firmware impostata possono configurare un'opzione non attiva di default tramite lo strumento a linea di comando `firmwarepasswd` in macOS.

Sicurezza della sandbox dell'OROM

In macOS 10.15, il firmware UEFI è stato aggiornato per includere un meccanismo di sandbox e per diminuire i privilegi delle ROM opzionali. Il firmware UEFI normalmente esegue tutto il codice, ROM opzionali incluse, al livello di privilegio massimo della CPU, chiamato "livello 0", e ha un'unica memoria virtuale condivisa per tutto il codice e tutti i dati. Il livello 0 è il livello di privilegio in cui viene eseguito il kernel di macOS, mentre il livello di privilegio più basso, ossia il livello 3, è quello in cui vengono eseguite le app. La sandbox dell'OROM riduce i privilegi delle OROM utilizzando una separazione della memoria virtuale allo stesso modo del kernel e facendo quindi in modo che le OROM siano eseguite al livello 3.



La sandbox limita notevolmente sia le interfacce che possono essere chiamate dalle OROM (in modo simile al sistema di filtraggio delle chiamate adottato dai kernel) sia il tipo di dispositivo a nome di cui un'OROM può registrarsi (in modo simile all'approvazione delle app). Il vantaggio di questo approccio è che le OROM dannose non possono più scrivere direttamente in nessuna posizione all'interno del livello 0. Esse sono invece limitate a un'interfaccia sandbox molto ristretta e ben definita. Tale interfaccia limitata riduce notevolmente la superficie esposta agli attacchi e obbliga i malintenzionati prima a evadere la sandbox e poi ad aumentare il privilegio.

Sicurezza del firmware UEFI per i Mac dotati di processore Intel

I Mac dotati di processore Intel con chip di sicurezza Apple T2 offrono la sicurezza tramite il firmware UEFI (Intel).

Panoramica

Dal 2006, i Mac con una CPU Intel usano un firmware Intel basato sull'EFI (Extensible Firmware Interface) Development Kit (EDK) versione 1 o versione 2. Il codice EDK2 è conforme alla specifica UEFI (Unified Extensible Firmware Interface). Questa sezione fa riferimento al firmware Intel come *firmware UEFI*. Il firmware UEFI è stato il primo codice eseguito sul chip Intel.

Per i Mac dotati di processore Intel e sprovvisti del chip di sicurezza Apple T2, la radice di attendibilità per il firmware UEFI è il chip in cui è archiviato il firmware. Gli aggiornamenti del firmware UEFI vengono firmati digitalmente da Apple e verificati dal firmware prima che venga aggiornato il dispositivo di archiviazione. Per aiutare a impedire gli attacchi rollback, gli aggiornamenti devono avere sempre una versione più nuova di quella esistente. Tuttavia un hacker con accesso fisico al Mac potrebbe potenzialmente utilizzare l'hardware per ottenere accesso al chip di archiviazione del firmware e aggiornarlo con contenuti dannosi. Allo stesso modo, se le vulnerabilità vengono rilevate nel processo di avvio iniziale del firmware UEFI (prima che sia impedita la modifica del chip di archiviazione), anche ciò potrebbe comportare un'infezione persistente del firmware UEFI. Si tratta di un limite dell'architettura dell'hardware comune alla maggior parte dei PC Intel e presente in tutti i Mac dotati di processore Intel e sprovvisti del chip T2.

Per aiutare a impedire attacchi fisici che tentano di sovvertire il firmware UEFI, l'architettura dei Mac è stata ridisegnata in modo da avere la radice dell'attendibilità del firmware UEFI nel chip T2. Su questi Mac, la radice di attendibilità per il firmware UEFI è precisamente il firmware T2, come descritto nella sezione Processo di avvio per i Mac dotati di processore Intel.

Sotto-componente Intel Management Engine (ME)

Un sotto-componente archiviato nel firmware UEFI è il firmware *Intel Management Engine (ME)*. Il firmware ME (un processore e un sottosistema separato all'interno dei chip Intel) viene usato principalmente per la protezione del copyright dei contenuti audio e video sui Mac dotati di scheda grafica solo Intel. Per ridurre la superficie di attacco di tale sottocomponente, i Mac dotati di processore Intel eseguono un firmware ME personalizzato, da cui sono stati rimossi la maggior parte dei contenuti. Dal momento che il firmware ME Mac risultante è più piccolo della dimensione minima di default che Intel mette a disposizione, molti componenti che in passato sono stati oggetto di attacchi pubblici da parte di ricercatori sulla sicurezza non sono più presenti.

Modalità di gestione del sistema (SMM)

I processori Intel hanno una modalità di esecuzione speciale, diversa dal funzionamento normale. È chiamata *modalità di gestione del sistema (SMM)* ed è stata introdotta originariamente per gestire le operazioni a tempo come la gestione dell'energia. Tuttavia, per realizzare tali azioni, storicamente i computer Mac usavano un micro-controller a parte chiamato *SMC (System Management Controller)*. Tale controller adesso non è più un micro-controller separato, ma è stato integrato nel chip T2.

Sicurezza del sistema in watchOS

Apple Watch utilizza molte delle stesse funzionalità di sicurezza della piattaforma basate sull'hardware presenti in iOS. Ad esempio, Apple Watch:

- Implementa l'avvio protetto e gli aggiornamenti software sicuri.
- Protegge l'integrità del sistema operativo.
- Aiuta a proteggere i dati sia sul dispositivo che durante la comunicazione con un iPhone abbinato o con internet.

Le tecnologie adottate includono quelle elencate in "Sicurezza del sistema" (come ad esempio la protezione dell'integrità del kernel, la protezione SKP e la protezione dell'integrità dei coprocessori di sistema), nonché la protezione dei dati, il portachiavi e tecnologie di rete.

Aggiornamento di watchOS

È possibile configurare watchOS affinché esegua l'aggiornamento durante la notte. Per ulteriori informazioni sul modo in cui il codice di Apple Watch viene archiviato e utilizzato durante l'aggiornamento, consulta la sezione dedicata alle keybag.

Rilevamento del polso

Se il rilevamento del polso è abilitato, il dispositivo si blocca automaticamente poco dopo essere stato rimosso dal polso dell'utente. Se il rilevamento del polso è disabilitato, Centro di Controllo fornisce un'opzione per bloccare Apple Watch. Quando Apple Watch è bloccato, Apple Pay può essere utilizzato solo inserendo il codice sull'orologio stesso. Il rilevamento del polso si disattiva dall'app Watch su iPhone e può essere applicato tramite una soluzione MDM.

Blocco attivazione

Quando Dov'è è attivato su iPhone, l'Apple Watch abbinato può utilizzare il blocco attivazione. Il blocco attivazione rende più difficile l'utilizzo o la vendita di un Apple Watch smarrito o rubato. Il blocco attivazione richiede l'ID Apple e la password dell'utente per annullare l'abbinamento, inizializzare o riattivare Apple Watch.

Abbinamento protetto con iPhone

Apple Watch può essere abbinato solo con un iPhone alla volta. Quando l'abbinamento ad Apple Watch viene annullato, iPhone comunica delle istruzioni per inizializzare tutti i contenuti e tutti i dati dall'orologio.

L'abbinamento di Apple Watch e iPhone è protetto utilizzando un processo OOB (out-of-band) per scambiare le chiavi pubbliche, seguito dal segreto condiviso del collegamento Bluetooth® Low Energy (BLE). Apple Watch mostra un motivo animato, che viene acquisito dalla fotocamera di iPhone. Tale motivo contiene un segreto codificato che consente l'abbinamento OOB per BLE 4.1. Se necessario, come metodo di abbinamento alternativo può essere usato un codice BLE standard.

Una volta stabilita la sessione BLE, codificata tramite il protocollo di sicurezza più alto disponibile nelle specifiche di base Bluetooth, iPhone e Apple Watch scaricano le chiavi tramite:

- Una procedura basata sul servizio Apple Identity Service (IDS), come descritto in Panoramica sulla sicurezza di iMessage.
- Uno scambio di chiavi tramite il protocollo IKEv2/IPsec. Lo scambio di chiavi iniziale è autenticato tramite la chiave di sessione Bluetooth (per l'abbinamento) o tramite le chiavi IDS (per l'aggiornamento del sistema operativo). Ciascun dispositivo genera una coppia di chiavi casuale (una chiave pubblica e una chiave privata) Ed25519 da 256 bit e, durante il processo di scambio iniziale, le chiavi pubbliche vengono scambiate. Quando un Apple Watch con watchOS 10 o versione successiva viene abbinato per la prima volta, la radice delle chiavi private si trova nel Secure Enclave.

  Su un iPhone con iOS 17 o versione successiva, la radice delle chiavi private non si trova nel Secure Enclave, perché se un utente esegue il ripristino del backup di iCloud sullo stesso iPhone l'abbinamento all'Apple Watch esistente viene conservato senza richiedere la migrazione.

Nota: il meccanismo usato per lo scambio e la codifica delle chiavi può variare e dipende dalla versione del sistema operativo su iPhone e su Apple Watch. Gli iPhone con iOS 13 o versioni successive abbinati a Apple Watch con watchOS 6 o versioni successive utilizzano solo il protocollo IKEv2/IPsec per lo scambio e la codifica delle chiavi.

Una volta scambiate le chiavi:

- La chiave della sessione Bluetooth viene scartata e tutte le comunicazioni tra iPhone e Apple Watch sono codificate tramite uno dei metodi descritti sopra (con i collegamenti codificati Bluetooth, Wi-Fi e cellulare che forniscono un livello di codifica secondario).
- (Solo IKEv2/IPsec) Le chiavi vengono archiviate nel portachiavi di sistema e utilizzate per l'autenticazione di future sessioni IKEv2/IPsec tra i dispositivi. Le ulteriori comunicazioni tra i dispositivi vengono crittografate e la loro integrità viene protetta tramite AES-256-GCM su iPhone con iOS 15 o versioni successive abbinate ad Apple Watch Series 4 o modelli successivi con watchOS 8 o versioni successive. (Su dispositivi meno recenti con versioni di sistema operativo meno recenti viene utilizzato ChaCha20-Poly1305 con chiavi a 256 bit).

L'indirizzo Bluetooth Low Energy del dispositivo cambia a intervalli di 15 minuti per ridurre il rischio che il dispositivo venga tracciato localmente a causa della trasmissione di un identificativo persistente.

Per supportare le app che devono trasmettere dati, la codifica viene fornita tramite i metodi descritti in Sicurezza di FaceTime, mediante il servizio IDS dell'iPhone abbinato o mediante una connessione a internet diretta.

Apple Watch implementa una codifica hardware dell'archiviazione e una protezione dei file e degli elementi del portachiavi basata sulle classi, nonché keybag con controllo degli accessi per gli elementi del portachiavi. Anche le chiavi usate per le comunicazioni tra Apple Watch e iPhone sono tutelate dal sistema di protezione basato su classi. Per ulteriori informazioni, consulta Keybag per la protezione dei dati.

Sblocco automatico e Apple Watch

Per una maggiore praticità, durante l'utilizzo di più dispositivi Apple, alcuni dispositivi possono sbloccarne altri in determinate situazioni. Lo sblocco automatico supporta tre scenari di utilizzo:

- Apple Watch può essere sbloccato da iPhone.
- Il Mac può essere sbloccato da Apple Watch.
- iPhone può essere sbloccato da Apple Watch se l'utente viene rilevato con il naso e la bocca coperti.

Tutti e tre i casi si basano sugli stessi principi di base: un protocollo Station-to-Station (STS) reciprocamente autenticato, con chiavi a lungo termine scambiate nel momento in cui la funzionalità viene abilitata e chiavi di sessione effimere uniche negoziate per ciascuna richiesta. A prescindere dal canale di comunicazione sottostante, il tunnel STS viene negoziato direttamente tra i chip Secure Enclave in entrambi i dispositivi e tutto il materiale crittografico viene mantenuto all'interno del dominio sicuro (a eccezione dei Mac senza Secure Enclave, in cui il tunnel STS termina nel kernel).

Sblocco

Una sequenza di sblocco completa può essere suddivisa in due fasi. Per iniziare, il dispositivo da sbloccare (chiamato "destinazione") genera un apposito segreto crittografico e lo invia al dispositivo che esegue lo sblocco (chiamato "iniziatore"). Successivamente, l'iniziatore esegue lo sblocco utilizzando il segreto generato precedentemente.

Per consentire lo sblocco automatico, i dispositivi si connettono tramite una connessione Bluetooth Low Energy (BLE). Quindi un segreto per lo sblocco di 32 byte generato in modo casuale dal dispositivo di destinazione viene inviato all'iniziatore tramite il tunnel STS. Durante prossimo sblocco tramite sensore biometrico o tramite codice, il dispositivo di destinazione cifra la propria chiave derivata dal codice con il segreto per lo sblocco ed elimina tale segreto dalla propria memoria.

Per eseguire lo sblocco, i dispositivi avviano una nuova connessione BLE, quindi utilizzano la connessione Wi-Fi peer-to-peer per stimare in maniera sicura la loro distanza reciproca. Se i dispositivi si trovano entro la distanza specificata e le politiche di sicurezza richieste sono soddisfatte, l'iniziatore invia il segreto per lo sblocco alla destinazione tramite il tunnel STS. La destinazione quindi genera un nuovo segreto per lo sblocco di 32 byte e lo restituisce all'iniziatore. Se il segreto attuale inviato dall'iniziatore decrittografa correttamente il record per lo sblocco, il dispositivo di destinazione viene sbloccato e la chiave derivata dal codice viene nuovamente cifrata con un nuovo segreto. Infine, il nuovo segreto per lo sblocco e la chiave derivata dal codice vengono eliminati dalla memoria del dispositivo di destinazione.

Politiche di sicurezza per lo sblocco automatico di Apple Watch

Per una maggiore praticità, Apple Watch può essere sbloccato da iPhone direttamente dopo l'avvio iniziale, senza che l'utente debba inserire il codice sull'Apple Watch stesso. Perché ciò sia possibile, il segreto casuale per lo sblocco (generato durante la primissima sequenza di sblocco, quando viene abilitata la funzionalità) viene usato per creare un record di escrow a lungo termine, che viene archiviato nella keybag di Apple Watch. Il segreto del record di escrow viene archiviato nel portachiavi di iPhone e viene usato per avviare una nuova sessione dopo ogni riavvio di Apple Watch.

Politiche di sicurezza per lo sblocco automatico di iPhone

Per lo sblocco automatico di iPhone tramite Apple Watch vengono implementate delle politiche di sicurezza aggiuntive. Apple Watch non può essere utilizzato al posto di Face ID su iPhone per altre operazioni, come l'acquisto con Apple Pay o le autorizzazioni nelle app. Quando Apple Watch sblocca correttamente un iPhone abbinato, l'orologio mostra una notifica e produce un feedback aptico associato. Se l'utente tocca il pulsante "Blocca iPhone" nella notifica, l'orologio invia ad iPhone un comando di blocco tramite BLE. Quando iPhone riceve tale comando, si blocca e disabilita sia Face ID che lo sblocco tramite Apple Watch. Il successivo sblocco di iPhone dovrà essere effettuato tramite il codice di iPhone.

Per poter sbloccare un iPhone abbinato da Apple Watch (quando l'opzione è abilitata), è necessario che siano soddisfatti i seguenti criteri:

- iPhone deve essere stato sbloccato tramite un altro metodo almeno una volta dopo che l'Apple Watch associato è stato indossato al polso ed è stato sbloccato.
- I sensori devono poter rilevare che il naso e la bocca sono coperti.
- La distanza misurata deve essere 2-3 metri o meno.
- Apple Watch non deve essere in modalità notturna.
- Apple Watch o iPhone devono essere stati sbloccati recentemente oppure Apple Watch deve aver rilevato del movimento fisico che indica che l'utente che lo indossa è attivo (ad esempio, non sta dormendo).
- iPhone deve essere stato sbloccato almeno una volta nelle ultime 6,5 ore.
- iPhone deve essere in uno stato che consenta a Face ID di eseguire lo sblocco del dispositivo. (Per ulteriori informazioni, consulta Face ID, Touch ID, codici e password).

Approvazione in macOS con Apple Watch

Quando è abilitato lo sblocco automatico con Apple Watch, è possibile utilizzare Apple Watch insieme a Touch ID o al suo posto per approvare le richieste di autorizzazione e autenticazione di:

- App di Apple e macOS che richiedono l'autorizzazione
- App di terze parti che richiedono l'autenticazione
- Password salvate di Safari
- Note protette

Utilizzo sicuro di Wi-Fi, dati cellulare, iCloud e Gmail

Quando Apple Watch non si trova all'interno della copertura Bluetooth, può essere utilizzata la connessione Wi-Fi o cellulare. Apple Watch si collega automaticamente alle reti Wi-Fi alle quali l'iPhone abbinato si è già connesso e le cui credenziali sono state sincronizzate su Apple Watch mentre entrambi i dispositivi si trovavano nel raggio di copertura. Questo comportamento di connessione automatica può essere configurato rete per rete nella sezione Wi-Fi dell'app Impostazioni di Apple Watch. È possibile accedere manualmente alle reti Wi-Fi a cui non è mai stata effettuata una connessione da nessuno dei due dispositivi tramite la sezione Wi-Fi dell'app Impostazioni di Apple Watch.

Quando Apple Watch e iPhone sono fuori distanza di copertura, Apple Watch si connette direttamente ai server di iCloud e di Gmail per scaricare la posta, piuttosto che sincronizzare i dati di Mail con l'iPhone abbinato tramite internet. Per gli account Gmail, l'utente deve eseguire l'autenticazione a Google nella sezione Mail dell'app Watch su iPhone. Il token OAuth ricevuto da Google viene inviato ad Apple Watch in formato codificato tramite IDS di Apple, in modo che possa essere utilizzato per scaricare la posta. Questo token OAuth non viene mai utilizzato per la connessione al server Gmail dall'iPhone abbinato.

Generazione di numeri casuali

I generatori di numeri pseudocasuali crittograficamente sicuri (CPRNG) sono una componente estremamente importante del software sicuro. Per questo motivo Apple ha dotato i kernel iOS, iPadOS, macOS, tvOS e watchOS di un software CPRNG attendibile, che si incarica di unire l'entropia del sistema e di fornire numeri casuali sicuri ai consumatori sia nel kernel che nello spazio utente.

Sorgenti di entropia

Il CPRNG del kernel è alimentato da più sorgenti di entropia durante l'avvio e la vita del dispositivo, tra cui (in base alla disponibilità):

- Il generatore di numeri casuali hardware (TRNG) di Secure Enclave
- I valori del jitter del momento raccolti durante l'avvio
- I valori relativi all'entropia raccolti dagli interrupt hardware
- Un file seed usato per far perdurare l'entropia tra gli avvii
- Istruzioni casuali Intel, come ad esempio RDSEED e RDRAND (solo sui Mac dotati di processore Intel)

Il CPRNG del kernel

Il CPRNG del kernel è un design di tipo Fortuna che punta a un livello di sicurezza a 256 bit. Fornisce numeri casuali di alta qualità ai consumatori dello spazio utente tramite le seguenti API:

- La chiamata di sistema `getentropy`(2)
- Il dispositivo casuale (/dev/random)

Il CPRNG del kernel accetta l'entropia fornita dall'utente scrivendo sul dispositivo casuale.

Dispositivo Apple per la ricerca sulla sicurezza

Il dispositivo Apple per la ricerca sulla sicurezza è un iPhone con fusibili speciali che consente a chi compie ricerche su iOS di operare senza dover superare o disabilitare le funzionalità di sicurezza della piattaforma di iPhone. Tale dispositivo consente ai ricercatori il sideload di contenuti che vengono eseguiti con permessi equivalenti a quelli della piattaforma, rendendo possibili ricerche su una piattaforma più simile a quella dei dispositivi destinati alle operazioni di produzione.

Per aiutare a garantire che la politica di esecuzione del dispositivo per la ricerca sulla sicurezza non abbia effetto sui dispositivi per l'utente, le modifiche alla politica vengono implementate in una variante di iBoot e della raccolta del kernel di avvio. Il loro avvio non è possibile sull'hardware per utenti. La variante di iBoot per la ricerca verifica la presenza di un nuovo stato del fusibile ed entra in un loop di kernel panic se viene eseguito su un hardware con fusibile non per la ricerca.

Il sottosistema cryptex consente a un ricercatore di caricare una cache di attendibilità personalizzata e un'immagine disco con contenuti corrispondenti. Per aiutare a garantire che questo sottosistema non consenta l'esecuzione su dispositivi per utenti, sono state implementate approfondite misure di difesa:

- `launchd` non carica l'elenco di proprietà launchd di `cryptexd` se rileva un dispositivo utente ordinario.
- `cryptexd` viene abortito se rileva un dispositivo utente ordinario.
- `AppleImage4` non fornisce il valore anti-replay utilizzato per verificare un cryptex di ricerca su un dispositivo utente ordinario.
- Il server di firma rifiuta di personalizzare le immagini disco cryptex per un dispositivo che non compare in un esplicito elenco approvato.

Per rispettare la privacy del ricercatore, solo le misurazioni (ad esempio, gli hash) degli eseguibili o la cache del kernel e gli identificativi del dispositivo per la ricerca sulla sicurezza vengono inviati ad Apple durante la personalizzazione. Apple non riceve il contenuto del cryptex che viene caricato sul dispositivo.

Per evitare situazioni in cui un hacker potrebbe tentare di far passare un dispositivo per la ricerca per un dispositivo per utenti e fare in modo che una vittima lo adotti per uso quotidiano, il dispositivo per la ricerca presenta le seguenti differenze:

- Il dispositivo per la ricerca sulla sicurezza si avvia solo mentre è in carica. Questa può essere effettuata tramite cavo Lightning o tramite caricatore compatibile con lo standard Qi. Se il dispositivo non è in carica durante l'avvio, entra in modalità di recupero. Se l'utente inizia la ricarica e riavvia il dispositivo, questo si avvierà normalmente. Appena XNU ha eseguito l'avvio del dispositivo, questo non deve essere in carica per continuare l'operazione.
- Durante l'avvio di iBoot, sotto il logo Apple, viene mostrata la scritta "*Security Research Device*".
- Il kernel XNU si avvia in modalità "Verbose".
- Sul lato del dispositivo è inciso il messaggio: "Property of Apple. Confidential and Proprietary. Call +1 877 595 1125".

Quelle di seguito sono misure aggiuntive implementate nel software che vengono mostrate dopo l'avvio:

- Durante la configurazione del dispositivo viene mostrata la scritta "*Security Research Device*".
- Nella schermata di blocco e nell'app Impostazioni viene mostrata la scritta "*Security Research Device*".

Il dispositivo per la ricerca sulla sicurezza consente ai ricercatori di eseguire le seguenti operazioni, non permesse sui dispositivi per utenti. I ricercatori possono:

- Effettuare il sideload sul dispositivo di codice eseguibile con permessi arbitrari dello stesso livello di quello dei componenti del sistema operativo Apple.
- Avviare i servizi all'avvio.
- Mantenere contenuti tra un riavvio e l'altro.
- Utilizza il permesso `research.com.apple.license-to-operate` per consentire a un processo di eseguire il debug di qualsiasi altro processo in esecuzione sul sistema, inclusi i processi di sistema.

  Il namespace `research.` viene rispettato soltanto dalla variante RESEARCH dell'estensione del kernel AppleMobileFileIntegrity; durante la convalida della firma su un dispositivo utente, tutti i processi con questo permesso vengono terminati.
- Personalizzare e ripristinare una cache del kernel personalizzata.

Codifica e protezione dati

Panoramica della codifica e protezione dati

La catena di avvio protetto, la sicurezza del sistema e le funzionalità delle app contribuiscono tutte a verificare che su un dispositivo siano eseguiti solo codice e app autorizzati. I dispositivi Apple sono dotati di funzionalità di codifica aggiuntive che proteggono i dati dell'utente anche nel caso in cui altre parti dell'infrastruttura di sicurezza siano state compromesse (per esempio, se un dispositivo è stato smarrito o esegue codice non autorizzato). Tutte queste funzionalità apportano importanti benefici sia agli utenti che agli amministratori IT, in quanto forniscono protezione di tutte le informazioni aziendali e personali e metodi per la cancellazione immediata e totale a distanza in caso di furto o smarrimento del dispositivo.

iPhone e iPad usano una metodologia di codifica dei file chiamata *protezione dati*, mentre i dati dei Mac dotati di processore Intel vengono protetti con una tecnologia di codifica chiamata *FileVault*. I Mac dotati di chip Apple utilizzano un modello ibrido che supporta la protezione dati, con due condizioni: il livello di protezione più basso (classe D) non è supportato e il livello di default (classe C) utilizza una chiave di volume e si comporta esattamente come FileVault sui Mac dotati di processore Intel. In ogni caso, le gerarchie di gestione delle chiavi hanno la propria radice nell'apposita sezione di Secure Enclave e un motore AES dedicato supporta la codifica senza perdita di velocità e aiuta a garantire che le chiavi di codifica di lunga durata non vengano mai esposte al sistema operativo del kernel o alla CPU (dove potrebbero venire compromesse). (I Mac dotati di processore Intel con chip T1 o sprovvisti di Secure Enclave non utilizzano un chip dedicato per proteggere le chiavi di codifica di FileVault).

Oltre all'utilizzo della protezione dati e di FileVault per aiutare a impedire l'accesso non autorizzato ai dati, Apple usa i *kernel dei sistemi operativi* per implementare misure di protezione e sicurezza. Il kernel utilizza il controllo degli accessi per racchiudere ogni app in una sandbox (che limita i dati a cui un'app può accedere) e un meccanismo chiamato *data vault* (che invece di limitare le chiamate che un'app può effettuare, limita l'accesso ai dati di un'app da parte di tutte le altre app che possono richiederli).

Codici e password

Per proteggere i dati degli utenti da attacchi malevoli, Apple utilizza i codici in iOS e iPadOS e le password in macOS. A password e codici più lunghi corrisponde una maggiore efficacia, che contribuisce a dissuadere gli attacchi di forza bruta. Ulteriori misure dissuasive implementate Apple sono l'adozione di ritardi temporali (per iOS e iPadOS) e la limitazione del numero di tentativi consentiti per inserire la password (per il Mac).

In iOS e iPadOS, impostando il codice o la password, l'utente abilita automaticamente la protezione dei dati. La protezione dei dati è abilitata anche sugli altri dispositivi che presentano un SoC Apple, come i Mac con chip Apple, Apple TV e Apple Watch. In macOS, Apple si avvale di *FileVault*, un programma integrato per la crittografia dei volumi.

In che modo codici e password efficaci possono aumentare la sicurezza

iOS e iPadOS supportano codici alfanumerici a sei e quattro cifre, così come quelli di lunghezza arbitraria. Oltre a sbloccare il dispositivo, un codice o una password forniscono entropia per determinate chiavi di codifica. Ciò significa che un hacker in possesso di un dispositivo non potrà accedere ai dati conservati in classi di protezione specifiche senza il codice.

Il codice o la password sono legati all'UID del dispositivo, quindi eventuali attacchi di forza bruta devono essere realizzati sul dispositivo stesso. Per rendere ogni tentativo più lento viene utilizzato un numero di iterazioni alto. Il numero di iterazioni è calibrato in modo da far durare ogni tentativo circa 80 millisecondi. Ciò significa che ci vorrebbero più di cinque anni e mezzo per provare tutte le combinazioni di un codice alfanumerico a sei caratteri con lettere minuscole e numeri.

Quanto più è sicuro il codice impostato dall'utente, tanto più diventa sicura la chiave di codifica. E utilizzando Face ID e Touch ID, l'utente ha la possibilità di stabilire un codice molto più sicuro che altrimenti sarebbe poco pratico. Un codice più sicuro consente di ottenere la più alta entropia possibile con l'obiettivo di proteggere le chiavi di codifica utilizzate per la protezione dati, senza influire negativamente sulla praticità di utilizzo da parte dell'utente che si trova a sbloccare un dispositivo svariate volte durante la giornata.

Se viene inserita una password lunga che contiene solo numeri, in "Blocco schermo" compare un tastierino numerico anziché la tastiera completa. Un codice numerico lungo può essere più facile da inserire rispetto a un codice alfanumerico breve, pur fornendo un livello di sicurezza equivalente.

Gli utenti possono specificare un codice alfanumerico più lungo selezionando "Codice alfanumerico personalizzato" nelle opzioni relative al codice in Impostazioni > Touch ID e codice o Impostazioni > Face ID e codice.

In che modo i ritardi di tempo incrementali contribuiscono a dissuadere gli attacchi di forza bruta

In iOS, iPadOS e macOS, per dissuadere ulteriormente eventuali hacker dal tentare di decifrare i codici, vengono applicati ritardi sempre più lunghi dopo l'inserimento di codice, password o PIN (a seconda del dispositivo e dello stato in cui si trova) come mostrato nella tabella seguente.

Tentativi	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10 o più**
Schermata di blocco di iOS e iPadOS	Nessuno	1 minuto	5 minuti	15 minuti	1 ora	3 ore	8 ore	Il dispositivo è disattivato e deve connettersi a un Mac o PC
Schermata di blocco di watchOS	Nessuno	1 minuto	5 minuti	15 minuti	1 ora	3 ore	8 ore	Il dispositivo è disattivato e deve connettersi a un iPhone
Finestra di login e schermata di blocco di macOS	Nessuno	1 minuto	5 minuti	15 minuti	1 ora	3 ore	8 ore	8 ore
Modalità di recupero macOS	Nessuno	1 minuto	5 minuti	15 minuti	1 ora	3 ore	8 ore	Consulta "In che modo i ritardi di tempo incrementali contribuiscono a dissuadere gli attacchi di forza bruta (macOS)" sotto
FileVault con chiave di recupero (personale, istituzionale o iCloud)	Nessuno	1 minuto	5 minuti	15 minuti	1 ora	3 ore	8 ore	Consulta "In che modo i ritardi di tempo incrementali contribuiscono a dissuadere gli attacchi di forza bruta (macOS)" sotto
Codice PIN del blocco remoto di macOS	1 minuto	5 minuti	15 minuti	30 minuti	1 ora	1 ora	1 ora	1 ora

Se l'opzione "Inizializza i dati" è attivata su iPhone o iPad (in Impostazioni > [Face ID o [Touch ID e codice]), dopo 10 tentativi consecutivi errati di inserimento del codice, tutti i contenuti e le impostazioni vengono cancellati dallo spazio di archiviazione. Tentativi consecutivi con lo stesso codice errato non vengono conteggiati per il raggiungimento del limite. Questa impostazione è anche disponibile come policy amministrativa tramite una soluzione MDM che la supporti e tramite Microsoft Exchange ActiveSync, e può essere impostata su una soglia più bassa.

Sui dispositivi con Secure Enclave, i ritardi sono comandati da Secure Enclave. Se il dispositivo viene riavviato durante un ritardo, tale ritardo viene comunque applicato e il timer comincia da capo per il periodo attuale.

In che modo i ritardi di tempo incrementali contribuiscono a dissuadere gli attacchi di forza bruta in macOS

Per impedire gli attacchi di forza bruta, all'avvio del Mac non sono consentiti più di 10 tentativi di inserimento della password nella finestra di login e, dopo vari tentativi non corretti, vengono applicati ritardi sempre più lunghi. I ritardi sono comandati da Secure Enclave. Se il Mac viene riavviato durante un ritardo, tale ritardo viene comunque applicato e il timer comincia da capo per il periodo attuale.

Per impedire che il malware causi la perdita irreversibile dei dati cercando di attaccare la password dell'utente, questi limiti non vengono applicati se l'utente ha effettuato correttamente il login al Mac, ma vengono reimpostati dopo il riavvio. Se vengono esauriti i 10 tentativi, l'utente dispone di altri 10 tentativi dopo il riavvio in recoveryOS. Se anche quei tentativi vengono esauriti, sono disponibili altri 10 tentativi per ogni meccanismo di recupero FileVault (recupero iCloud, chiave di recupero di FileVault e chiave istituzionale), per un massimo di 30 tentativi aggiuntivi. Una volta esauriti anche quei tentativi aggiuntivi, Secure Enclave non elabora più nessuna richiesta di decrittografia del volume o di verifica della password e i dati presenti nell'unità non possono più essere recuperati.

Per contribuire a proteggere i dati in ambiente aziendale, gli addetti IT dovrebbero definire e applicare delle policy di configurazione di FileVault tramite una soluzione MDM. Le organizzazioni dispongono di svariate opzioni per la gestione dei volumi codificati, tra cui le chiavi di recupero istituzionali, le chiavi di recupero personali (che possono facoltativamente essere archiviate con la MDM) o un insieme di entrambe. Anche la rotazione delle chiavi può essere impostata come policy nella MDM.

Nei Mac con chip di sicurezza Apple T2, la password assolve una funzione simile, salvo per il fatto che la chiave generata è usata per la codifica con FileVault invece che per la protezione dati. Inoltre, macOS offre delle opzioni aggiuntive per il recupero delle password:

- Recupero di iCloud
- Recupero di FileVault
- Chiave istituzionale di FileVault

Protezione dei dati

Panoramica della protezione dati

Apple usa una tecnologia chiamata protezione dati per proteggere i dati archiviati nella memoria flash sui dispositivi dotati di SoC Apple come iPhone, iPad, Apple Watch, Apple TV e sui Mac dotati di chip Apple. La protezione dati consente al dispositivo di rispondere a eventi comuni quali le chiamate in entrata, offrendo allo stesso tempo anche un alto livello di crittografia per i dati utente. Alcune app di sistema (come Messaggi, Mail, Calendario, Contatti e Foto) e i dati relativi allo stato di salute utilizzano la protezione dei dati di default. Le app di terze parti ricevono questa protezione automaticamente.

Implementazione

La protezione dati è implementata creando e gestendo una gerarchia di chiavi e si basa su tecnologie di codifica hardware integrate in ogni dispositivo Apple. La protezione dati è controllata per ogni singolo file e assegna a ognuno di essi una classe; l'accessibilità dei file è determinata in base allo stato, sbloccato o meno, delle chiavi della classe a cui appartengono. Con Apple File System (APFS), il file system è in grado di suddividere ulteriormente le chiavi "per entità", dove porzioni diverse di un file possono avere chiavi diverse.

Ogni volta che viene creato un file sul volume di dati, la protezione dati crea una nuova chiave a 256 bit (la *chiave "per file"*) e la consegna al motore AES hardware, che utilizza la chiave per crittografare il file mentre viene scritto nella memoria flash. Sui dispositivi dotati di chip da A14 ad A17 e da M1 a M3, la codifica avviene tramite l'algoritmo AES-256 in modalità XTS, dove la chiave per file da 256 bit passa attraverso una funzione di derivazione (NIST Special Publication 800-108) da cui si ricava un tweak da 256 bit e una chiave crittografica da 256 bit. Sui dispositivi dotati di chip da A9 ad A13 e da S5 a S9, la crittografia utilizza l'algoritmo AES-128 in modalità XTS, dove la chiave per file a 256 bit è divisa in due per fornire un tweak da 128 bit e una chiave crittografica da 128 bit.

Sui Mac dotati di chip Apple, l'opzione di default della protezione dati è la classe C (consulta Classi di protezione dati), ma viene utilizzata una chiave di volume piuttosto che una chiave per entità o per file, ricreando quindi il modello di sicurezza di FileVault per i dati dell'utente. Gli utenti devono comunque attivare FileVault per ottenere la protezione completa garantita dal fatto di legare la password alla gerarchia delle chiavi crittografiche. Gli sviluppatori possono anche attivare una classe di protezione più alta che utilizza chiavi per file e per entità.

Protezione dei dati nei dispositivi Apple

Sui dispositivi Apple che utilizzano la protezione dei dati, ogni file è protetto da una chiave per file (o per entità) unica. La chiave, cifrata tramite l'algoritmo NIST AED, è ulteriormente cifrata con una delle varie chiavi di classe, a seconda del modo in cui si prevede di accedere al file. La chiave per file cifrata è quindi memorizzata nei metadati del file.

I dispositivi con il formato APFS possono supportare la clonazione dei file (copie a costo zero utilizzando la tecnologia copy-on-write). Se un file viene clonato, ciascuna metà del clone ottiene una nuova chiave per accettare le scritture in arrivo, in modo tale che i nuovi dati vengano scritti sul supporto con una nuova chiave. Con il tempo, il file può diventare composto da varie entità (o frammenti), ognuna associata a una chiave diversa. Tuttavia, tutte le entità che compongono un file vengono protette dalla stessa chiave di classe.

Quando viene aperto un file, i suoi metadati sono decrittografati con la chiave del file system, rivelando la chiave per file cifrata e una nota sulla classe che la protegge. La cifratura della chiave per file (o per entità) viene tolta con la chiave di classe e quindi fornita al motore AES hardware che a sua volta decrittografa il file mentre viene letto dalla memoria flash. La gestione delle chiavi dei file cifrate avviene interamente in Secure Enclave; la chiave per i file non viene mai esposta direttamente al processore per le applicazioni. All'avvio, Secure Enclave negozia una chiave effimera con il motore AES. Quando Secure Enclave rimuove la cifratura dalle chiavi di un file, queste vengono di nuovo cifrate con la chiave effimera e inviate di nuovo al processore per le applicazioni.

I metadati di tutti i file nel file system del volume di dati sono codificati con una chiave di volume casuale, creata quando il sistema operativo viene installato per la prima volta o quando il dispositivo viene cancellato dall'utente. Tale chiave è codificata e cifrata tramite una chiave di cifratura della chiave conosciuta solo da Secure Enclave per l'archiviazione a lungo termine. La chiave di cifratura della chiave cambia ogni volta che l'utente inizializza il dispositivo. Sui SoC A9 (o successivi), Secure Enclave si affida all'entropia, rafforzata da sistemi anti-replay, per raggiungere la cancellabilità e proteggere la sua chiave di cifratura della chiave, tra altre risorse. Per ulteriori informazioni, consulta Archiviazione non volatile protetta.

Proprio come avviene per le chiavi per file o per entità, la chiave dei metadati del volume di dati non viene mai esposta direttamente al processore per le applicazioni; Secure Enclave ne fornisce invece una versione effimera diversa a ogni avvio. Quando è archiviata, la chiave del file system codificata viene ulteriormente cifrata tramite una chiave effimera archiviata in Effaceable Storage o tramite una chiave multimediale, protetta del meccanismo anti-replay di Secure Enclave. Tale chiave non è stata progettata per garantire maggiore riservatezza dei dati, ma piuttosto per poter essere cancellata velocemente su richiesta (dall'utente, tramite l'opzione "Inizializza contenuto e impostazioni", oppure da un utente o un amministratore, inviando il comando di cancellazione remota da una soluzione di gestione dei dispositivi mobili (MDM), Microsoft Exchange ActiveSync o iCloud). La cancellazione della chiave secondo questa modalità rende tutti i file inaccessibili a causa della codifica.

Il contenuto di un file può essere codificato con una o più chiavi per file (o per entità), cifrate con una chiave di classe e archiviate nei metadati di un file, a sua volta codificato con la chiave del file system. La chiave di classe è protetta con l'UID dell'hardware e, per alcune classi, con il codice dell'utente. Questa gerarchia fornisce flessibilità e prestazioni ottimali. Ad esempio, per modificare la classe di un file occorre solo cifrare nuovamente la sua chiave per file; la modifica del codice di accesso cifra di nuovo la chiave di classe.

Classi di protezione dati

Quando viene creato un file nuovo su un dispositivo che supporta la protezione dei dati, gli viene assegnata una classe dall'app che l'ha creato. Ogni classe utilizza diverse policy che stabiliscono quando i dati sono accessibili. Le classi e le policy di base sono descritte nelle sezioni seguenti. I Mac dotati di chip Apple non supportano la "Classe D: Nessuna protezione" e viene stabilito un limite di sicurezza al momento del login e del logout (non al momento del blocco o dello sblocco come su iPhone e iPad).

Classe	Tipo di protezione
Classe A: Protezione completa	NSFileProtectionComplete
Classe B: Protetto se non è aperto	NSFileProtectionCompleteUnlessOpen
Classe C: Protetto fino alla prima autenticazione utente *Nota:* macOS utilizza una chiave di volume per ricreare le funzionalità della protezione di FileVault.	NSFileProtectionCompleteUntilFirstUserAuthentication
Classe D: Nessuna protezione *Nota:* non supportata su macOS.	NSFileProtectionNone

Protezione completa

NSFileProtectionComplete la chiave di classe è protetta da una chiave derivata dal codice o dalla password utente e dall'UID del dispositivo. Poco dopo che l'utente ha bloccato il dispositivo (10 secondi se l'opzione "Richiedi password" è impostata su Subito), la classe decrittografata viene eliminata, rendendo tutti i dati in essa contenuti inaccessibili finché l'utente non inserisce di nuovo il codice o sblocca il dispositivo (oppure effettua il login) tramite Face ID o Touch ID.

In macOS, poco dopo che l'ultimo utente ha eseguito il logout dal dispositivo, la classe decrittografata viene eliminata, rendendo tutti i dati in essa contenuti inaccessibili finché un utente non inserisce di nuovo il codice o effettua il login al dispositivo tramite Touch ID.

Protetto se non è aperto

NSFileProtectionCompleteUnlessOpen: potrebbe essere necessario scrivere alcuni file mentre il dispositivo è bloccato oppure mentre l'utente non ha eseguito il login, come ad esempio nel caso di un allegato e-mail che viene scaricato in background. Questo comportamento si ottiene utilizzando una codifica a curva ellittica asimmetrica (ECDH su Curve25519). La normale chiave per file è protetta da una chiave generata tramite l'accordo base One-Pass Diffie-Hellman, come descritto in NIST SP 800-56A.

La chiave pubblica effimera per l'accordo delle chiavi è archiviata insieme alla chiave per file protetta. KDF è la funzione di derivazione della chiave di concatenazione (alternativa 1 approvata) come descritto al punto 5.8.1 di NIST SP 800-56A. AlgorithmID è omesso. PartyUInfo e PartyVInfo sono chiavi pubbliche effimere e statiche, rispettivamente. SHA256 è usato come funzione di hashing. Non appena viene chiuso il file, la chiave per file viene cancellata dalla memoria. Per potere aprire nuovamente il file, il segreto condiviso è ricreato utilizzando la chiave privata della classe "Protetto se non è aperto" e la chiave pubblica effimera, che sono usate per aprire la chiave per file utilizzata per decrittografare il file.

In macOS la parte privata di NSFileProtectionCompleteUnlessOpen è accessibile finché qualsiasi utente sul sistema ha eseguito l'accesso o è autenticato.

Protetto fino alla prima autenticazione utente

NSFileProtectionCompleteUntilFirstUserAuthentication: questa classe si comporta nello stesso modo di "Protezione completa", l'unica differenza è che la chiave di classe decrittografata non viene rimossa dalla memoria quando il dispositivo è bloccato o l'utente ha eseguito il logout. La protezione in questa classe ha proprietà simili alla codifica desktop full-volume e protegge i dati dagli attacchi che prevedono un riavvio. Questa classe è quella di default per tutti i dati delle app di terze parti che non sono stati assegnati a una classe di protezione dati specifica.

In macOS questa classe utilizza una chiave di volume che risulta accessibile finché il volume è attivato e funziona esattamente come FileVault.

Nessuna protezione

NSFileProtectionNone: questa chiave di classe è protetta solo con l'UID ed è conservata in Effaceable Storage. Dato che tutte le chiavi necessarie per decrittografare i file in questa classe sono archiviate sul dispositivo, la crittografia offre solo il vantaggio della cancellazione rapida a distanza. Se un file non è associato a una classe di protezione dati, è comunque archiviato in forma codificata (così come lo sono tutti i dati su un dispositivo iOS e iPadOS).

Questa opzione non è supportata in macOS.

Nota: in macOS, per i volumi che non corrispondono a un sistema operativo avviato, tutte le classi di protezione dati sono accessibili finché il volume è attivato. La classe di protezione dei dati di default è NSFileProtectionCompleteUntilFirstUserAuthentication. Le chiavi per entità sono disponibili sia per le app eseguite tramite Rosetta 2 sia per le app native.

Keybag per la protezione dei dati

Le chiavi per le classi di protezione dati dei file e del portachiavi sono raccolte e gestite nelle keybag su iOS, iPadOS, tvOS e watchOS. Tali sistemi operativi utilizzano le seguenti keybag: Utente, Dispositivo, Backup, Escrow e "Backup iCloud".

Keybag Utente

La keybag Utente è dove vengono archiviate le chiavi di classe cifrate usate durante il normale funzionamento del dispositivo. Ad esempio quando viene inserito un codice, la chiave *NSFileProtectionComplete* viene caricata dalla keybag Utente e viene decifrata. Si tratta di un file plist binario archiviato nella classe "Nessuna protezione".

Per i dispositivi con SoC precedenti all'A9, i contenuti del file plist sono codificati con una chiave conservata in Effaceable Storage. Per poter fornire maggiore sicurezza alle keybag, questa chiave viene cancellata e rigenerata ogni volta che l'utente cambia il codice.

Per i dispositivi con A9 o SoC successivi, il file plist contiene una chiave che indica che la keybag è archiviata in una posizione protetta dal valore anti-replay controllato da Secure Enclave.

Secure Enclave gestisce la keybag Utente e può essere interrogato sullo stato di blocco di un dispositivo. Riporterà che il dispositivo è sbloccato solo se tutte le chiavi di classe nella keybag Utente sono accessibili e sono state decifrate correttamente.

Keybag Dispositivo

La keybag Dispositivo è utilizzata per archiviare le chiavi di classe cifrate usate per le operazioni che includono dati specifici del dispositivo. I dispositivi iPadOS configurati per l'uso condiviso a volte hanno bisogno di accedere alle credenziali prima dell'accesso di qualsiasi utente, quindi occorre una keybag che non sia protetta dal codice dell'utente.

iOS e iPadOS non supportano la separazione crittografica dei contenuti del file system in base all'utente. Ciò significa che il sistema usa le chiavi di classe della keybag Dispositivo per cifrare le chiavi per file. Il portachiavi utilizza invece le chiavi delle classi della keybag Utente per proteggere gli elementi presenti nel portachiavi dell'utente. Sugli iPhone e iPad configurati per essere utilizzati da un solo utente (configurazione di default), la keybag Dispositivo e quella Utente coincidono e sono protette dal codice utente.

Keybag Backup

La keybag Backup viene creata quando il Finder (macOS 10.15 o versioni successive) o iTunes (macOS 10.14 o versioni precedenti) effettuano un backup codificato e viene archiviata sul computer che contiene il backup del dispositivo. Viene creata una nuova keybag con un nuovo gruppo di chiavi e i dati di cui è stato eseguito il backup sono nuovamente codificati con queste chiavi nuove. Come illustrato in precedenza, gli elementi del portachiavi non migratori rimangono cifrati con la chiave derivata dall'UID, il che ne consente il ripristino nel dispositivo da cui era stato eseguito il backup, rendendoli tuttavia inaccessibili se spostati su un dispositivo diverso.

Alla keybag, protetta dalla password impostata, vengono applicate 10 milioni di iterazioni della funzione di derivazione delle chiavi PBKDF2. Nonostante questo alto numero di iterazioni, non è presente alcun legame a un dispositivo specifico e, per questo motivo, la keybag Backup potrebbe essere oggetto di un tentativo di attacco di forza bruta effettuato in parallelo su molti computer. È possibile ovviare a questa vulnerabilità utilizzando una password sufficientemente sicura.

Se un utente decide di non codificare un backup, i file di backup non verranno codificati indipendentemente dalla classe di protezione dati a cui appartengono, ma il portachiavi rimane protetto con una chiave derivata dall'UID. Ecco perché gli elementi del portachiavi migrano su un nuovo dispositivo solo se è stata impostata una password di backup.

Keybag Escrow

La keybag Escrow è utilizzata per la sincronizzazione con il Finder (macOS 10.15 o versioni successive) o iTunes (macOS 10.14 o versioni precedenti) tramite USB e per la gestione dei dispositivi mobili (MDM). Questa keybag consente al Finder o ad iTunes di eseguire il backup e la sincronizzazione senza richiedere all'utente di inserire un codice e permette a una soluzione MDM di cancellare remotamente il codice di un utente. È archiviata nel computer utilizzato per la sincronizzazione con il Finder o con iTunes o sulla soluzione MDM che gestisce il dispositivo da remoto.

La keybag Escrow migliora l'esperienza utente durante la sincronizzazione del dispositivo, operazione che potenzialmente potrebbe richiedere l'accesso a qualsiasi classe di dati. Quando un dispositivo bloccato da codice è connesso al Finder o ad iTunes per la prima volta, all'utente viene chiesto di inserire un codice. Il dispositivo crea quindi una keybag Escrow contenente le stesse chiavi di classe utilizzate sul dispositivo, protette da una chiave generata ex novo. La keybag Escrow e la chiave che la protegge sono divise tra il dispositivo e l'host o il server, e i dati sono archiviati sul dispositivo nella classe "Protetto fino alla prima autenticazione utente". Questo è il motivo per cui è necessario inserire il codice prima che l'utente esegua un backup con il Finder o con iTunes per la prima volta dopo un riavvio.

Nel caso di un aggiornamento software in modalità wireless, all'utente viene richiesto di inserire il codice all'avvio dell'aggiornamento. Questa procedura viene utilizzata per creare un token di sblocco, utilizzabile una sola volta, che sblocca la keybag Utente dopo l'aggiornamento. Il token non può essere generato senza inserire il codice dell'utente e qualsiasi token generato in precedenza viene invalidato se il codice dell'utente è cambiato.

I token di sblocco utilizzabili una sola volta possono essere utilizzati per l'installazione assistita oppure non assistita di un aggiornamento software. Vengono codificati con una chiave derivata dal valore attuale di un contatore monotonico in Secure Enclave, l'UUID della keybag e l'UID di Secure Enclave.

Sui SoC A9 (o modelli successivi), il token di sblocco utilizzabile una sola volta non si affida più a contatori o a Effaceable Storage. Esso è invece protetto dal valore anti-replay controllato da Secure Enclave.

Il token di sblocco utilizzabile una sola volta per gli aggiornamenti software assistiti scade dopo 20 minuti. In iOS 13 e iPadOS 13.1 o versioni successive, il token è archiviato in una posizione protetta da Secure Enclave. Prima di iOS 13, questo token veniva esportato da Secure Enclave e veniva scritto in Effaceable Storage o protetto dal meccanismo anti-replay di Secure Enclave. Se il dispositivo non veniva riavviato entro 20 minuti, il timer per la validità faceva incrementare il contatore.

Gli aggiornamenti software automatici avvengono quando il sistema rileva che è disponibile un aggiornamento e quando una delle seguenti condizioni è vera:

- Gli aggiornamenti automatici sono configurati su iOS 12 o versioni successive.
- L'utente sceglie "Installa più tardi" quando riceve una notifica dell'aggiornamento.

Una volta che l'utente ha inserito il codice, viene generato un token di sblocco una tantum che può restare valido in Secure Enclave per 8 ore. Se l'aggiornamento non si è ancora verificato, questo token di sblocco viene distrutto a ogni blocco e creato nuovamente a ogni sblocco successivo. Ogni sblocco riavvia la finestra di 8 ore. Trascorse 8 ore, un timer renderà il token di sblocco non valido.

Keybag "Backup iCloud"

La keybag "Backup iCloud" è simile alla keybag Backup. Tutte le chiavi di classe in questa keybag sono asimmetriche (utilizzano Curve25519, come la classe di protezione dati "Protetto se non è aperto"). Anche per la protezione del portachiavi incluso nel backup per il recupero del portachiavi iCloud viene usata una keybag asimmetrica.

Protezione delle chiavi nelle modalità di avvio alternative

La protezione dei dati è progettata in modo da fornire accesso ai dati dell'utente solo dopo una corretta autenticazione e solo all'utente autorizzato. Le classi di protezione dati sono progettate per supportare una vasta gamma di casi, come l'abilità di leggere e scrivere alcuni dati anche quando un dispositivo è bloccato (ma in seguito a un primo sblocco). Per proteggere l'accesso ai dati dell'utente durante modalità di avvio alternative come la modalità DFU, la modalità di recupero, la modalità di diagnosi Apple o persino durante gli aggiornamenti software, vengono implementati dei passaggi aggiuntivi. Tali funzionalità si basano su una combinazione di caratteristiche hardware e software e sono state ampliate di pari passo con l'evoluzione dei chip progettati da Apple.

Funzionalità	A10	A11 - A17 S3 - S9 M1, M2, M3
Recupero: tutte le classi di protezione dati	✓	✓
Avvii alternativi per modalità DFU, modalità di recupero e aggiornamenti software: classi di protezione dati A, B e C	✗	✓

Il motore AES di Secure Enclave è dotato di bit seed del software bloccabili. Quando le chiavi vengono create dall'UID, questi bit seed vengono inclusi nella funzione di derivazione della chiave per creare gerarchie di chiave aggiuntive. Il modo in cui il bit seed viene usato varia a seconda dei SoC:

- A partire dai SoC Apple A10 e S3, un bit seed serve a distinguere quali chiavi sono protette dal codice di accesso dell'utente. Il bit seed è impostato per le chiavi che richiedono il codice dell'utente (incluse le chiavi per le classi di protezione dati A, B e C), mentre viene azzerato per le chiavi che non richiedono il codice dell'utente (incluse la chiave per i metadati del file system e le chiavi per la classe D).
- Quando i dispositivi con chip A10 o modelli successivi che eseguono iOS 13 o versioni successive e iPadOS 13.1 o versioni successive vengono avviati in modalità di diagnosi, tutti i dati dell'utente sono resi crittograficamente inaccessibili. Questo risultato è possibile grazie all'uso di un bit seed aggiuntivo configurato per gestire la possibilità di accedere alla chiave multimediale, necessaria per accedere ai metadati (e quindi ai contenuti di tutti i file) sul volume di dati codificato tramite la protezione dei dati. Questo tipo di protezione include tutti i file protetti di tutte le classi (A, B, C e D), non solo quelli per cui è necessario il codice dell'utente.
- Sul processore A12, la ROM di avvio di Secure Enclave blocca il bit seed del codice se il processore per le applicazioni è entrato in modalità DFU o Modalità di recupero. Quando il bit seed del codice è bloccato, non è consentita nessuna operazione che possa modificarlo. Questo meccanismo è progettato per impedire l'accesso a dati protetti con il codice dell'utente.

Il ripristino di un dispositivo in seguito all'attivazione della modalità DFU consente di riportarlo a uno stato sicuramente funzionante, con la certezza che contenga solo codice firmato da Apple e non modificato. La modalità DFU può essere attivata manualmente.

Consulta i seguenti articoli del supporto Apple per informazioni sul modo in cui far entrare un dispositivo in modalità DFU:

Dispositivo	Articolo del supporto Apple
iPhone, iPad	Se hai dimenticato il codice di iPhone
Apple TV	Se vedi un simbolo di avviso su Apple TV
Un Mac dotato di chip Apple	Come riattivare o ripristinare il firmware del Mac

Protezione dei dati dell'utente dagli attacchi

Gli hacker che tentano di estrarre i dati dell'utente utilizzano solitamente una serie di tecniche, come ad esempio estrarre i dati codificati su un altro supporto per eseguire un attacco di forza bruta, manipolare la versione del sistema operativo o modificare o ridurre le politiche di sicurezza del dispositivo per facilitare l'attacco. Attaccare i dati su un dispositivo richiede solitamente una comunicazione tramite un'interfaccia fisica come Thunderbolt, Lightning o USB-C. I dispositivi Apple includono delle funzionalità che aiutano a impedire questo tipo di attacchi.

I dispositivi Apple supportano una tecnologia chiamata *SKP (Sealed Key Protection)*, progettata per garantire che il materiale crittografico venga reso non disponibile fuori dal dispositivo o che viene utilizzata a seguito di manipolazioni alle versioni dei sistemi operativi o alle impostazioni di sicurezza senza una corretta autorizzazione da parte dell'utente. Tale funzionalità *non* è fornita da Secure Enclave. È invece supportata da registri hardware presenti a un livello inferiore per poter fornire un livello di protezione aggiuntivo alle chiavi necessarie a decrittografare i dati dell'utente, a prescindere da Secure Enclave.

Nota: la protezione SKP è disponibile solo sui dispositivi dotati di SoC progettati da Apple.

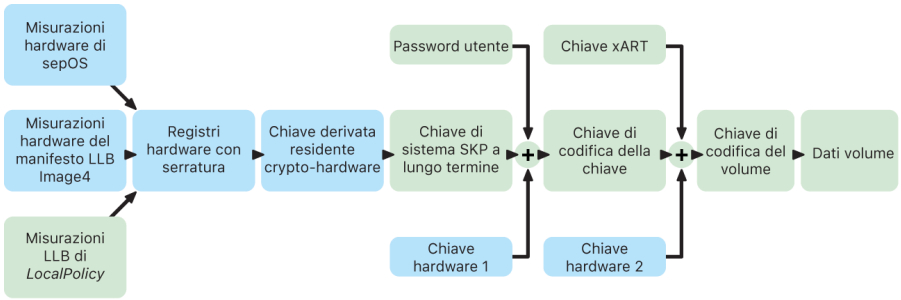
Funzionalità	A11 - A17 S3 - S9 M1, M2, M3
Protezione SKP	✅

iPhone e iPad possono anche essere configurati in modo da attivare le connessioni dati solo in condizioni che indicano in maniera più probabile che il dispositivo si trova ancora sotto il controllo fisico del proprietario autorizzato.

Protezione SKP (Sealed Key Protection)

Sui dispositivi Apple che supportano la protezione dei dati, la chiave di codifica delle chiavi è protetta da misurazioni del software sul sistema ed è legata all'UID fornito solo da Secure Enclave. Sui Mac dotati di chip Apple, la protezione della chiave di codifica delle chiavi è ulteriormente rafforzata incorporando informazioni sulla politica di sicurezza presente sul sistema. Ciò dipende dal fatto che macOS supporta l'applicazione di modifiche a politiche di sicurezza importanti (come la disattivazione dell'avvio protetto o della protezione dell'integrità del sistema) che non sono supportate su altre piattaforme. Sui Mac dotati di chip Apple, questa protezione include anche le chiavi di FileVault, dal momento che FileVault è implementato utilizzando la classe C di protezione dei dati.

La chiave risultante dalla combinazione tra la password dell'utente, la chiave SKP a lungo termine e la chiave hardware 1 (l'UID da Secure Enclave) viene chiamata *chiave derivata dalla password*. Questa chiave è utilizzata per proteggere la keybag dell'utente (sulle piattaforme supportate) e la chiave di codifica delle chiavi (solo su macOS), quindi consente lo sblocco tramite i sensori biometrici o lo sblocco automatico tramite altri dispositivi come Apple Watch.



Il monitor di avvio di Secure Enclave rileva le misurazioni del sistema operativo di Secure Enclave caricato. Quando la ROM di avvio del processore per le applicazioni misura il manifesto Image4 collegato al bootloader di livello inferiore, tale manifesto contiene anche una misurazione di qualsiasi altro firmware abbinato al sistema caricato. LocalPolicy contiene le configurazioni di sicurezza centrali caricate per macOS. LocalPolicy contiene anche il campo `nsih`, che è un hash del manifesto Image4 di macOS. Il manifesto Image4 di macOS contiene le misurazioni di tutti i firmware abbinati a macOS e gli oggetti di avvio principali come la raccolta del kernel di avvio e l'hash root del volume di sistema firmato.

Se un hacker è in grado di modificare in modo inatteso uno qualsiasi di tali componenti firmware, software o di configurazione di sicurezza misurati, modifica le misurazioni archiviate nei registri hardware. La modifica delle misurazioni fa in modo che la *chiave root per le misurazioni del sistema* derivata dall'hardware crittografico risulti in un valore diverso, rompendo il sigillo sulla gerarchia delle chiavi. Ciò rende inaccessibile la *chiave del dispositivo per le misurazioni del sistema*, che a sua volta rende inaccessibile la chiave per la codifica delle chiavi e, di conseguenza, i dati.

Tuttavia, quando il sistema non è sotto attacco, esso deve consentire gli aggiornamenti software legittimi che modificano le misurazione del firmware e il campo `nsih` in LocalPolicy affinché punti a nuove misurazioni di macOS. In altri sistemi che tentano di incorporare le misurazioni del firmware, ma non hanno una sorgente di attendibilità sicura, l'utente deve disabilitare la sicurezza, aggiornare il firmware e quindi riabilitarla perché le nuove misurazioni di base possano essere rilevate. Ciò aumenta considerevolmente il rischio che un hacker possa manomettere il firmware durante un aggiornamento software. Il sistema è aiutato dal fatto che il manifesto Image4 contiene tutte le misurazioni necessarie. L'hardware che decrittografa la chiave del dispositivo per le misurazioni del sistema con la chiave root per le misurazioni del sistema quando è presente una corrispondenza durante un avvio normale, può anche crittografare la chiave del dispositivo in una chiave root da proporre in futuro. Specificando le misurazioni previste dopo un aggiornamento software, l'hardware può codificare una chiave root accessibile in un sistema operativo attuale, in modo che rimanga accessibile in un sistema operativo futuro. In modo analogo, quando un utente modifica in modo legittimo le impostazioni di sicurezza in LocalPolicy, la chiave del dispositivo per le misurazioni del sistema deve essere codificata in una chiave root per le misurazioni del sistema futura in base alle misurazioni per LocalPolicy che il bootloader di livello inferiore calcolerà al prossimo riavvio.

Ruolo di Apple File System

Apple File System (APFS) è un file system proprietario creato per la codifica. APFS funziona su tutte le piattaforme: iPhone, iPad, Mac, Apple TV e Apple Watch. Ottimizzato per l'archiviazione Flash/SSD, è dotato delle seguenti funzionalità: crittografia sicura, metadati copy-on-write, condivisione dello spazio, clonazione di file e directory, istantanee, ridimensionamento rapido delle directory, primitive atomiche di salvataggio sicuro e basi di file system migliorate; inoltre vanta un design copy-on-write unico che si serve della coalescenza I/O per offrire le massime prestazioni e garantire al tempo stesso l'affidabilità dei dati.

Condivisione dello spazio

APFS assegna spazio di archiviazione su richiesta. Quando un singolo container APFS ha più volumi, lo spazio libero di quel container viene condiviso e può essere assegnato ai vari volumi in base alle esigenze di spazio. Ogni volume usa solo parte dell'intero container, quindi lo spazio disponibile è rappresentato dalle dimensioni totali del container, meno lo spazio utilizzato in tutti i volumi del container.

Volumi multipli

In macOS 10.15 o versioni successive, un container APFS utilizzato per avviare il Mac deve contenere almeno cinque volumi, i primi tre dei quali sono nascosti all'utente:

- *Volume di pre-avvio:* il volume non è crittografato e contiene i dati necessari per l'avvio di ogni volume di sistema presente nel container.
- *Volume VM:* il volume non è crittografato ed è utilizzato da macOS per l'archiviazione dei file di scambio crittografati.
- *Volume di recupero:* il volume non è crittografato e deve essere disponibile senza dover sbloccare un volume di sistema per eseguire recoveryOS.
- *Volume di sistema:* contiene quanto segue:
  - Tutti i file necessari per l'avvio del Mac.
  - Tutte le app native installate da macOS (che prima si trovavano nella cartella /Applicazioni e adesso si trovano nella cartella /Sistema/Applicazioni).

  Nota: di default, nessun processo può scrivere sul volume di sistema, nemmeno i processi di sistema Apple.
- *Volume di dati:* contiene i dati soggetti a cambiare, come ad esempio:
  - Tutti i dati all'interno della cartella dell'utente, tra cui foto, musica, video e documenti.
  - App installate dall'utente, incluse AppleScript e le app di Automator.
  - Framework e daemon personalizzati installati dall'utente, dall'organizzazione o da app di terze parti.
  - Altre posizioni di proprietà dell'utente e scrivibili da parte dell'utente, come ad esempio /Applicazioni, /Libreria, /Utenti, /Volumi, /usr/local, /private, /var e /tmp.

Per ogni volume di sistema aggiuntivo viene creato un volume di dati. I volumi di pre-avvio, VM e di recupero sono condivisi e non duplicati.

In macOS 11 o versioni successive viene utilizzata un'istantanea del volume di sistema. Il sistema operativo si avvia da un'istantanea del volume di sistema, non semplicemente da un'attivazione in sola lettura del volume di sistema mutabile.

In iOS e iPadOS, l'archiviazione è divisa in almeno due volumi APFS:

- Volume di sistema
- Volume di dati

Protezione dati del portachiavi

Molte app devono gestire password e altri dati non di grandi dimensioni ma sensibili, quali ad esempio chiavi e token di login. Il portachiavi fornisce un modo sicuro per conservare questi elementi. I vari sistemi operativi Apple usano diversi meccanismi per implementare le misure associate alle varie classi di protezione del portachiavi. In macOS (compresi i Mac dotati di chip Apple) la protezione dei dati non è utilizzata direttamente per implementare queste misure.

Panoramica

Gli elementi del portachiavi sono codificati tramite due diverse chiavi AES-256-GCM: una chiave per la tabella (metadati) e una chiave per ciascuna riga (chiave del valore segreto). I metadati del portachiavi (tutti gli attributi diversi da kSecValue) sono codificati con l'apposita chiave per velocizzare le ricerche, mentre i valori segreti (kSecValueData) vengono codificati con la chiave del valore segreto. La chiave dei metadati è protetta da Secure Enclave, ma è archiviata nella cache del processore per le applicazioni per consentire ricerche rapide del portachiavi. La chiave del valore segreto deve passare attraverso Secure Enclave.

Il portachiavi è implementato come un database SQLite archiviato nel file system. Esiste solo un database e il daemon `securityd` determina quali sono gli elementi del portachiavi a cui possono avere accesso i processi o l'app. Le API di accesso al portachiavi eseguono chiamate al daemon, che a sua volta esegue la richiesta alle autorizzazioni "keychain-access-groups", "application-identifier" e "application-group" per l'app. I gruppi di accesso, piuttosto che limitare l'accesso a un singolo processo, consentono la condivisione tra app degli elementi del portachiavi.

Gli elementi del portachiavi possono essere condivisi solo tra app dello stesso sviluppatore. Perché questo sia possibile, alle app di terze parti viene chiesto di utilizzare gruppi di accesso con un prefisso che viene assegnato nell'ambito dell'Apple Developer Program attraverso gruppi di app. La richiesta di prefisso e l'unicità di appartenenza a un gruppo di app sono applicate attraverso la firma del codice, i profili di provisioning e l'Apple Developer Program.

I dati del portachiavi sono protetti utilizzando una struttura a classi simile a quella usata nella protezione dati dei file. Queste classi hanno comportamenti equivalenti alle classi di protezione dati dei file, ma usano chiavi e funzioni distinte.

Disponibilità	Protezione dati dei file	Protezione dati del portachiavi
Quando sbloccato	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Quando bloccato	NSFileProtectionComplete UnlessOpen	✕
Dopo primo sblocco	NSFileProtectionComplete UntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Sempre	NSFileProtectionNone	kSecAttrAccessibleAlways
Codice abilitato	✕	kSecAttrAccessibleWhen PasscodeSetThisDeviceOnly

Le app che utilizzano servizi di aggiornamento in background possono usare *kSecAttrAccessibleAfterFirstUnlock* per quegli elementi del portachiavi a cui è necessario accedere durante gli aggiornamenti in background.

La classe *kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly* si comporta come *kSecAttrAccessibleWhenUnlocked*, tuttavia è disponibile solo quando il dispositivo è configurato con un codice. Questa classe esiste soltanto nella keybag di sistema. Queste classi:

- Non vengono sincronizzate sul portachiavi iCloud.
- Non vengono incluse nei backup.
- Non vengono incluse nelle keybag Escrow.

Se il codice viene rimosso o reimpostato, gli elementi vengono resi inutilizzabili eliminando le chiavi di classe.

Altre classi del portachiavi hanno una classe equivalente "Solo questo dispositivo", sempre protetta con l'UID mentre viene copiata dal dispositivo durante un backup, per renderla inutilizzabile se ripristinata su un dispositivo diverso. Apple ha trovato l'equilibrio perfetto tra sicurezza e facilità d'uso scegliendo classi del portachiavi che variano in base al tipo di informazione di cui si vuole garantire la sicurezza e da quando iOS e iPadOS la richiedono.

Protezioni delle classi di dati del portachiavi

Le protezioni delle classi elencate di seguito vengono implementate per gli elementi del portachiavi.

Elemento	Disponibile
Password Wi-Fi	Dopo primo sblocco
Account di posta	Dopo primo sblocco
Account Microsoft Exchange ActiveSync	Dopo primo sblocco
Password VPN	Dopo primo sblocco
LDAP, CalDAV, CardDAV	Dopo primo sblocco
Token account social network	Dopo primo sblocco
Chiavi codifica annunci Handoff	Dopo primo sblocco
Token iCloud	Dopo primo sblocco
Chiavi iMessage	Dopo primo sblocco
Password "In casa"	Quando sbloccato
Password Safari	Quando sbloccato
Segnalibri Safari	Quando sbloccato
Backup del Finder o di iTunes	Quando sbloccato, non migratorio
Certificati VPN	Dopo il primo sblocco, non migratorio
Chiavi Bluetooth®	Sempre, non migratorio
Token del servizio di notifiche push di Apple (APN)	Sempre, non migratorio

Elemento	Disponibile
Certificati iCloud e chiave privata	Sempre, non migratorio
PIN SIM	Sempre, non migratorio
Token Dov'è	Sempre
Segreteria	Sempre

Su macOS, tutti gli elementi di portachiavi installati da profili di configurazione sono *sempre* disponibili. Su iOS e iPadOS, gli elementi di portachiavi installati da profili di configurazione hanno diverse opzioni di accesso a seconda del tipo, del modo in cui viene fatto riferimento a essi e di quando sono stati installati. Di default, gli elementi di portachiavi installati tramite profili di configurazione sono *disponibili dopo il primo sblocco e non migratori*. Tuttavia, un elemento di portachiavi installato da un profilo di configurazione è *sempre* disponibile se:

- È stato installato prima di eseguire l'aggiornamento ad iOS 15, iPadOS 15 o versioni successive.
- È un certificato (non un'identità).
- È un'identità a cui viene fatto riferimento dal campo `IdentityCertificateUUID` in un payload `com.apple.mdm`

Controllo accesso portachiavi

I portachiavi possono usare elenchi di controllo degli accessi (ACL) per impostare le policy di accessibilità e i requisiti di autenticazione. Gli elementi possono stabilire delle condizioni che richiedono la presenza dell'utente specificando che non è possibile fornire l'accesso senza l'autenticazione tramite Face ID, Touch ID oppure inserendo il codice o la password del dispositivo. L'accesso agli elementi può essere limitato specificando che la registrazione tramite Face ID o Touch ID non ha subito modifiche dal momento in cui l'elemento è stato aggiunto. Questa restrizione aiuta a impedire che un hacker possa aggiungere la propria impronta digitale per accedere a un elemento del portachiavi. Gli elenchi ACL sono valutati all'interno di Secure Enclave e vengono rilasciati al kernel solo se si soddisfano i vincoli specificati.

Architettura del portachiavi in macOS

macOS offre l'accesso al portachiavi per archiviare in modo comodo e sicuro i nomi utente e le password, comprese identità digitali, chiavi di codifica e note protette. È accessibile aprendo l'app Accesso Portachiavi in /Applicazioni/Utility/. L'uso del portachiavi elimina la necessità di inserire (o persino di ricordare) le credenziali di ogni risorsa. Per ogni utente del Mac viene creato un portachiavi di default iniziale, ma gli utenti possono crearne altri per determinati scopi.

Oltre ai portachiavi dell'utente, macOS si affida a una serie di portachiavi di sistema che conservano le risorse di autenticazione non specifiche di un utente, come le credenziali di rete e le identità di infrastruttura della chiave pubblica (PKI). Uno di questi portachiavi, "Root di sistema", è immutabile e conserva i certificati della CA root della PKI internet per semplificare attività comuni come le operazioni di online banking e l'e-commerce. Allo stesso modo, l'utente può distribuire ai computer Mac gestiti dei certificati CA di cui è stato eseguito il provisioning internamente, per facilitare la convalida di siti e servizi interni.

FileVault

Codifica del volume con FileVault in macOS

I computer Mac offrono FileVault, una funzionalità di codifica integrata pensata per proteggere tutti i dati a riposo. FileVault usa l'algoritmo di codifica dei dati AES-XTS per proteggere interi volumi sia interni che su dispositivi di archiviazione rimovibili.

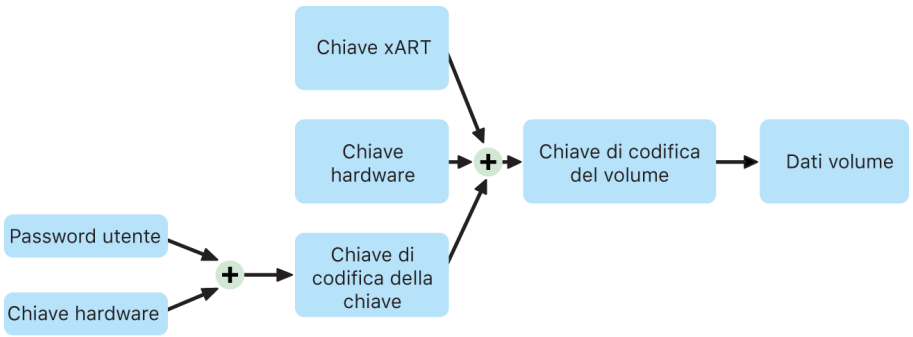
Sui Mac dotati di chip Apple, FileVault viene implementato utilizzando la classe C di protezione dati con una chiave di volume. Sui Mac con chip Apple e chip di sicurezza Apple T2, i dispositivi di archiviazione interni connessi direttamente a Secure Enclave sfruttano le funzionalità di sicurezza hardware di quest'ultimo e del motore AES. Quando un utente attiva FileVault su un Mac, durante il processo di avvio sono necessarie le sue credenziali.

Nota: per i modelli di Mac (1) *precedenti a quelli con chip T2*, (2) con spazio di archiviazione interno *che non era originariamente incluso nel Mac* o (3) con una memoria esterna collegata: in seguito all'attivazione di FileVault, tutti i file esistenti ed eventuali altri dati scritti verranno crittografati. I dati che sono stati aggiunti e poi eliminati prima dell'attivazione di FileVault non sono crittografati e possono essere recuperati con strumenti legali per il recupero dei dati.

Archiviazione interna con FileVault attivato

Senza credenziali di login valide o una chiave di recupero crittografica, i volumi APFS interni restano codificati e sono protetti da accessi non autorizzati anche quando il supporto fisico di archiviazione viene rimosso e collegato a un altro computer. In macOS 10.15, ciò include sia il volume di sistema che il volume di dati. A partire da macOS 11, il volume di sistema è protetto dalla funzionalità "Volume di sistema firmato", ma il volume di dati resta protetto dalla codifica. Sui Mac dotati di chip Apple e su quelli con chip T2, la codifica del volume interno è implementata tramite la creazione e gestione di una gerarchia di chiavi e si basa sulle tecnologie di codifica hardware integrate nel chip. Questa gerarchia di chiavi è progettata per raggiungere quattro obiettivi contemporaneamente:

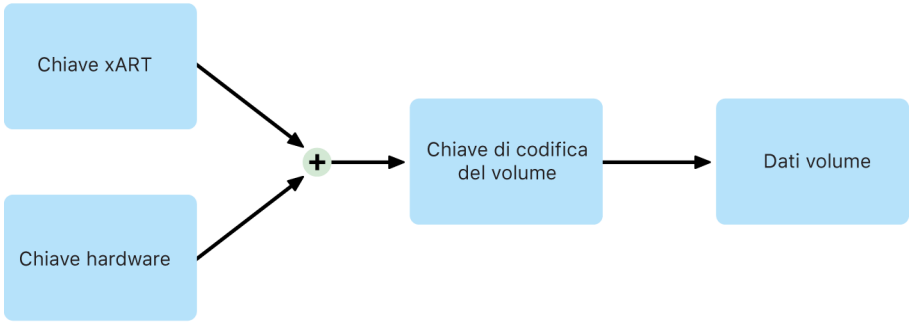
- Richiedere la password dell'utente per la decrittografia.
- Proteggere il sistema da un attacco di forza bruta al supporto di archiviazione rimosso dal Mac.
- Fornire un metodo sicuro e rapido per l'inizializzazione dei contenuti tramite l'eliminazione del materiale crittografico necessario.
- Consentire agli utenti di modificare le proprie password (e, a turno, le chiavi crittografiche usate per proteggere i file) senza richiedere l'ulteriore codifica dell'intero volume.



Sui Mac dotati di chip Apple e su quelli con chip T2, la gestione delle chiavi di FileVault si verifica interamente in Secure Enclave; le chiavi di codifica non vengono mai esposte direttamente alla CPU Intel. Di default, tutti i volumi APFS vengono creati con una chiave di codifica per il volume. I contenuti del volume e i metadati sono codificati con questa chiave, cifrata con una chiave di crittografia delle chiavi. Quando FileVault è attivo, questa chiave di crittografia delle chiavi è protetta dalla combinazione di password dell'utente e UID hardware.

Archiviazione interna con FileVault non attivato

Se durante il processo iniziale con Impostazione Assistita su un Mac dotato di chip Apple o su un Mac con il chip T2 non viene attivato FileVault, il volume è comunque codificato, ma la chiave di codifica del volume è protetta solo dall'UID hardware di Secure Enclave.



Se FileVault viene attivato in seguito (processo che risulta immediato, visto che i dati erano già crittografati), un meccanismo anti-replay aiuta a impedire che la vecchia chiave (basata solo sull'UID hardware) sia utilizzata per decrittografare il volume. Quando FileVault è abilitato, il volume è protetto dalla combinazione di password dell'utente e UID hardware, come descritto sopra.

Eliminare i volumi FileVault

Quando l'utente elimina un volume, la relativa chiave di codifica viene eliminata in modo sicuro da Secure Enclave. Questo meccanismo aiuta a impedire accessi futuri con quella chiave anche da parte di Secure Enclave. Inoltre, tutte le chiavi di codifica del volume vengono cifrate con una chiave multimediale, che non garantisce confidenzialità aggiuntiva ai dati, ma è progettata per consentire l'eliminazione sicura e rapida dei dati, la cui decrittografia senza tale chiave è impossibile.

Sui Mac dotati di chip Apple e su quelli con chip T2, la cancellazione della chiave multimediale è garantita dalla tecnologia supportata da Secure Enclave, come ad esempio i comandi MDM da remoto. La cancellazione della chiave multimediale secondo questa modalità rende il volume inaccessibile a causa della codifica.

Dispositivi di archiviazione rimovibili

La codifica dei dispositivi di archiviazione rimovibili non usa le funzionalità di sicurezza di Secure Enclave e viene eseguita nello stesso modo in cui avviene sui Mac dotati di processore Intel e sprovvisti di chip T2.

Gestire FileVault in macOS

In macOS, le organizzazione possono gestire FileVault tramite SecureToken o token Bootstrap.

Utilizzare SecureToken

Apple File System (APFS) in macOS 10.13 o versione successiva modifica il modo in cui vengono generate le chiavi di codifica di FileVault. Nelle versioni precedenti di macOS sui volumi CoreStorage, le chiavi usate nel processo di codifica di FileVault venivano create quando un utente o un'organizzazione attivava FileVault su un Mac. In macOS sui volumi APFS, le chiavi vengono generate durante la creazione dell'utente, durante l'impostazione della prima password utente o durante il primo login di un utente del Mac. Questa implementazione delle chiavi di codifica, il momento in cui vengono generate e il modo in cui vengono archiviate fanno parte di una funzionalità chiamata SecureToken. In particolare, un SecureToken è una versione cifrata di una KEK (Key Encryption Key) protetta da una password utente.

Durante il deployment di FileVault sull'APFS, l'utente può continuare a:

- Usare i processi e gli strumenti esistenti, come l'escrow di una chiave di recupero personale (PRK) su una soluzione di gestione dei dispositivi mobili (MDM).
- Ritardare l'abilitazione di FileVault fino al login o logout di un utente sul Mac.
- Creare e usare una chiave di recupero istituzionale (IRK).

In macOS 11, quando si imposta la password iniziale per il primo utente del Mac, a tale utente viene fornito un SecureToken. In alcune situazioni, tale comportamento potrebbe non essere desiderato, poiché in precedenza, per fornire il primo SecureToken, era necessario accedere all'account utente. Per impedirlo, aggiungi `;DisabledTags;SecureToken` all'attributo utente creato in automatico `AuthenticationAuthority` prima di impostare la password, come mostrato di seguito.

```
sudo dscl . append /Users/<user name> AuthenticationAuthority
";DisabledTags;SecureToken"
```

Utilizzare il token Bootstrap

macOS 10.15 ha introdotto una nuova funzionalità, il *token Bootstrap*, per contribuire a dare un SecureToken sia agli account mobili che all'account facoltativo di amministratore creato durante la registrazione del dispositivo ("amministratore gestito"). In macOS 11, un token Bootstrap può fornire un SecureToken a qualsiasi utente che accede a un Mac, inclusi gli account utente locali. L'uso della funzionalità del token Bootstrap di macOS 10.15 o versioni successive richiede:

- Registrazione del Mac in una soluzione MDM tramite Apple School Manager o Apple Business Manager, operazione che rende il Mac supervisionato.
- Supporto del fornitore della MDM.

In macOS 10.15.4 o versioni successive, un token Bootstrap viene generato e viene depositato presso la soluzione MDM al primo accesso da parte di qualsiasi utente abilitato all'utilizzo di SecureToken, se la soluzione MDM supporta tale funzionalità. Un token Bootstrap può essere generato e depositato presso la soluzione MDM anche utilizzando lo strumento a riga di comando `profiles`, se necessario.

In macOS 11, un token Bootstrap può essere usato anche per altre operazioni, oltre che per fornire SecureToken agli account utente. Sui Mac dotati di chip Apple, un token Bootstrap, se disponibile, può essere usato per autorizzare l'installazione delle estensioni del kernel e degli aggiornamenti software quando sono gestiti tramite MDM.

Chiavi di recupero istituzionali e personali

FileVault, su volumi sia CoreStorag che APFS, supporta l'uso di una chiave di recupero istituzionale (precedentemente conosciuta come *identità master di FileVault*) per sbloccare il volume. Sebbene una chiave di recupero istituzionale sia utile per le operazioni da riga di comando al fine di sbloccare un volume o disattivare del tutto FileVault, la sua utilità per le organizzazioni è limitata, specialmente nelle versioni più recenti di macOS. Inoltre, sui Mac dotati di chip Apple, la chiave di recupero istituzionale non ha valore a livello funzionale, per due principali motivi: in primo luogo, le chiavi di recupero istituzionali non possono essere usate per accedere a recoveryOS; in secondo luogo, dato che la modalità disco di destinazione non è più supportata, il volume non può essere sboccato mediante il collegamento a un altro Mac. Per queste e altre ragioni, *l'uso delle chiavi di recupero istituzionali non è più consigliato per la gestione istituzionale di FileVault sui computer Mac*. È preferibile utilizzare piuttosto una chiave di recupero personale (PRK).

Informazioni sul modo in cui Apple protegge i dati personali degli utenti

Protezione dell'accesso delle app ai dati utente

Oltre a codificare i dati a riposo, i dispositivi Apple impediscono alle app di accedere senza permesso alle informazioni personali dell'utente tramite varie tecnologie, inclusi i data vault. Da Impostazioni in iOS e iPadOS e da Impostazioni di Sistema (macOS 13 o versioni successive) o Preferenze di Sistema (macOS 12 o versioni precedenti), gli utenti possono vedere l'elenco delle app a cui hanno consentito di accedere a determinate informazioni, nonché concedere o revocare l'autorizzazione. L'accesso è applicato nei seguenti casi:

- *iOS, iPadOS e macOS:* Calendario, Fotocamera, Contatti, microfono, Foto, Promemoria e riconoscimento vocale
- *iOS e iPadOS:* Bluetooth, Casa, file multimediali, app multimediali e Apple Music, movimento e fitness
- *iOS e watchOS:* Salute
- *macOS:* monitoraggio degli input (ad esempio, pressione dei tasti della tastiera), richiesta, registrazione dello schermo (ad esempio, video e istantanee schermo statiche) e Impostazioni di Sistema (macOS 13 o versioni successive) o Preferenze di Sistema (macOS 12 o versioni precedenti).

In iOS 13.4 o versioni successive e iPadOS 13.4 o versioni successive, i dati di tutte le app di terze parti sono automaticamente protetti in un data vault. Questo aiuta a proteggere dall'accesso non autorizzato ai dati anche da parte di processi che non sono in sandbox. In iOS 15 o versioni successive sono incluse delle classi aggiuntive, tra cui "Rete locale", "Interazioni nelle vicinanze", "Dati di sensori e utilizzo di Ricerca" e full immersion.

Se l'utente accede a iCloud, le app di iOS e iPadOS avranno accesso di default a iCloud Drive. Gli utenti possono controllare l'accesso di ciascuna app in iCloud in Impostazioni. iOS e iPadOS forniscono inoltre delle restrizioni progettate per impedire lo spostamento di dati tra le app e gli account installati dalla soluzione di gestione dei dispositivi mobili (MDM) e quelli installati dall'utente.

Protezione dell'accesso ai dati dati relativi allo stato di salute dell'utente

HealthKit fornisce un punto di raccolta centrale per i dati relativi a stato di salute e attività fisica su iPhone e Apple Watch. Funziona anche direttamente con i dispositivi per salute e fitness, come i cardiofrequenzimetri compatibili con Bluetooth Low Energy (BLE) e i coprocessori di movimento integrati in molti dispositivi iOS. Tutte le interazioni di HealthKit con le app di salute e fitness, istituti sanitari e dispositivi di salute e fitness richiedono il permesso dell'utente. Tali dati sono archiviati nella classe di protezione dati "Protetto se non è aperto". L'accesso ai dati viene revocato 10 minuti dopo il blocco del dispositivo e i dati tornano accessibili la volta successiva che l'utente inserisce il codice o utilizza Face ID o Touch ID per sbloccare il dispositivo.

Raccogliere e archiviare i dati su salute e attività fisica

HealthKit raccoglie e archivia anche dei dati di gestione, come i permessi di accesso per le app, i nomi dei dispositivi connessi a HealthKit e le informazioni sulla programmazione utilizzate per aprire le app quando sono disponibili nuovi dati. Tali dati sono archiviati nella classe di protezione dati "Protetto fino alla prima autenticazione utente". I file journal temporanei archiviano le informazioni sanitarie generate quando il dispositivo è bloccato, ad esempio quando l'utente sta facendo esercizio fisico. Tali informazioni sono archiviate nella classe di protezione dati "Protetto se non è aperto". Quando il dispositivo è sbloccato, i file journal temporanei vengono importati nel database sanitario di base e successivamente eliminati una volta completato il processo.

I dati sanitari possono essere archiviati su iCloud. La codifica end-to-end per i dati relativi allo stato di salute richiede iOS 12 o versioni successive e l'autenticazione a due fattori. Negli altri casi, i dati dell'utente sono comunque codificati durante l'archiviazione e la trasmissione, ma non con una codifica end-to-end. Una volta attivata l'autenticazione a due fattori ed eseguito l'aggiornamento a iOS 12 o versioni successive, ai dati sanitari verrà applicata la codifica end-to-end.

Se l'utente effettua il backup del dispositivo usando il Finder (macOS 10.15 o versione successiva) o iTunes (macOS 10.14 o versione precedente), i dati sanitari vengono archiviati solo se il backup è codificato.

Dati sanitari clinici

Gli utenti possono accedere a sistemi sanitari supportati all'interno dell'app Salute per ottenere una copia dei propri dati sanitari clinici. Durante la connessione a un sistema sanitario, l'utente effettua l'autenticazione tramite credenziali client OAuth 2. Dopo la connessione, i dati sanitari clinici vengono scaricati direttamente dall'istituto sanitario tramite una connessione protetta tramite TLS 1.3. Una volta scaricati, tali dati vengono archiviati in maniera sicura assieme ai dati sanitari.

Autenticità dei dati sanitari

I dati archiviati nel database includono metadati per rintracciare la provenienza di ogni record di dati. Questi metadati includono a loro volta un identificatore per l'app che identifica l'app che ha archiviato il record. In aggiunta a questo, un elemento di metadati opzionale può contenere una copia digitalmente firmata del record. Questo accorgimento ha lo scopo di garantire l'autenticità dei dati per i record generati da un dispositivo attendibile. Il formato utilizzato per la firma digitale è la Cryptographic Message Syntax (CMS) specificata nella RFC 5652.

Accesso ai dati sanitari da parte delle app di terze parti

L'accesso all'API di HealthKit è controllato attraverso autorizzazioni e le app si devono adeguare alle restrizioni che riguardano l'uso dei dati. Le app non sono ad esempio autorizzate ad utilizzare i dati sanitari a fini pubblicitari. Inoltre viene loro richiesto di fornire agli utenti le informazioni relative alla politica sulla privacy, in cui si espone come vengono usati i dati sanitari.

L’accesso ai dati sanitari da parte delle app è controllato dalle impostazioni sulla privacy dell’utente. Agli utenti viene chiesto di concedere l’accesso ai dati sanitari quando le app lo richiedono, così come accade anche per Contatti, Foto e altre sorgenti di dati in iOS. Tuttavia, nel caso dei dati sanitari, alle app viene concesso un accesso separato per la lettura e la scrittura dei dati, e un altro distinto per ogni tipo di informazione sanitaria. In Impostazioni > Salute > Accesso dati e dispositivi, gli utenti possono visualizzare e revocare i permessi precedentemente concessi per accedere ai dati sanitari.

Se alle app è stato consentito di scrivere i dati, significa anche che possono leggere quelli scritti da loro. Se è stato loro consentito di leggere i dati, possono leggere quelli scritti da tutte le fonti. Le app non possono tuttavia conoscere il tipo di accesso consentito ad altre app. Inoltre, non sono in grado di sapere in modo definitivo se è stato loro concesso l’accesso per la lettura dei dati sanitari. Quando un’app non dispone dell’accesso in lettura, tutte le risposte alle richieste non restituiranno alcun dato (la stessa risposta che darebbe un database vuoto). Questo meccanismo è progettato per impedire alle app di dedurre lo stato di salute dell’utente leggendo i tipi di dati di cui sta tenendo traccia.

Cartella clinica per gli utenti

L’app Salute offre all’utente la possibilità di compilare una cartella clinica con le informazioni che potrebbero essere importanti nel caso di un’emergenza medica. Le informazioni sono inserite o aggiornate manualmente e non vengono sincronizzate con quelle disponibili nei database sanitari.

Le informazioni della cartella clinica possono essere visualizzate toccando il pulsante Emergenza in “Blocco schermo”. Le informazioni sono archiviate sul dispositivo utilizzando la classe di protezione dati “Nessuna protezione” affinché possano essere accessibili senza dover inserire il codice del dispositivo. La cartella clinica è una funzionalità opzionale che consente agli utenti di trovare il giusto equilibrio tra sicurezza e privacy. Questi dati vengono inclusi nel backup di iCloud in iOS 13 o versioni precedenti. In iOS 14, la cartella clinica viene sincronizzata tra i dispositivi tramite CloudKit e usufruisce delle stesse caratteristiche di codifica di tutto il resto dei dati sanitari.

Condivisione dell’app Salute

In iOS 15, nell’app Salute gli utenti hanno la possibilità di condividere i dati sanitari con altre persone. Tali dati possono essere condivisi tra due utenti che utilizzano la crittografia end-to-end di iCloud. Apple non è in grado di accedere ai dati che vengono condivisi tramite l’app Salute. Per utilizzare la funzionalità, sia il mittente che il ricevente devono avere installato iOS 15 o versioni successive e aver abilitato l’autenticazione a due fattori.

Inoltre, è possibile scegliere di condividere i propri dati sanitari anche con la propria struttura sanitaria di riferimento tramite l’apposita funzionalità nell’app Salute. I dati condivisi mediante questa funzionalità vengono resi disponibili con crittografia end-to-end soltanto agli istituti sanitari selezionati dall’utente e Apple non aggiorna né ha accesso alle chiavi di crittografia per decrittografare, visualizzare o accedere in altro modo ai dati condivisi tramite la funzionalità di condivisione con la struttura sanitaria. Ulteriori dettagli sul modo in cui questo servizio è stato concepito per proteggere i dati sanitari degli utenti sono disponibili nella sezione dedicata alla sicurezza e alla privacy della guida alla registrazione di Apple per le organizzazioni sanitarie.

Codifica e firma digitale

Elenchi di controllo degli accessi (ACL)

I dati del portachiavi vengono suddivisi in partizioni e protetti con gli elenchi di controllo degli accessi (ACL). In questo modo, senza esplicita approvazione da parte dell'utente, app che hanno identità diverse non possono accedere alle credenziali archiviate da app di terzi. Questa protezione è un meccanismo che tutela le credenziali di autenticazione sui dispositivi Apple per diversi servizi e app all'interno dell'organizzazione.

Mail

Nell'app Mail, gli utenti possono inviare messaggi codificati e firmati digitalmente. Mail rileva automaticamente, distinguendo tra maiuscole e minuscole, gli indirizzi email o i nomi alternativi RFC 5322 appropriati contenuti nei certificati di codifica e di firma digitale dei token di verifica dell'identificazione personale (PIV) allegati nelle smart card compatibili. Se un account email configurato corrisponde a un indirizzo email presente in un certificato di codifica o firma digitale presente su un token PIV allegato, Mail mostra automaticamente il pulsante per la firma nella barra degli strumenti della finestra per la composizione di un nuovo messaggio. Se Mail dispone del certificato di codifica del destinatario o può rilevarlo nell'elenco di indirizzi globale di Microsoft Exchange, visualizza l'icona di un lucchetto aperto nella barra degli strumenti della finestra per la composizione di un nuovo messaggio. L'icona di un lucchetto chiuso indica che il messaggio sarà inviato in forma codificata secondo la chiave pubblica del destinatario.

S/MIME per messaggio

iOS, iPadOS e macOS supportano la codifica S/MIME per messaggio. Ciò significa che gli utenti S/MIME possono scegliere di firmare e codificare sempre di default i propri messaggi oppure di farlo in modo selettivo per messaggi individuali.

Le identità usate con S/MIME possono essere consegnate ai dispositivi Apple tramite un profilo di configurazione, una soluzione di gestione dei dispositivi mobili (MDM), il protocollo SCEP (Simple Certificate Enrollment Protocol) o l'autorità di certificazione di Microsoft Active Directory.

Smart card

macOS 10.12 o versione successiva include il supporto nativo per le schede per la verifica dell'identità personale (PIV). Tali smart card sono largamente utilizzate da organizzazioni commerciali e governative per l'autenticazione a due fattori, la firma digitale e la codifica.

Le smart card includono una o più identità digitali con una coppia di chiavi (una chiave pubblica e una chiave privata) e un certificato associato. Sbloccando una smart card con il PIN si ottiene accesso alle chiavi private usate per le operazioni di autenticazione, codifica e firma. Il certificato determina per cosa possa essere utilizzata una chiave, quali attributi le sono associati e se è convalidata (firmata) dal certificato di un'autorità di certificazione.

Le smart card possono essere usate per l'autenticazione a due fattori. I due fattori necessari a sbloccare una card sono "un elemento di proprietà dell'utente" (la card) e "un elemento conosciuto dall'utente" (il PIN). macOS 10.12 o versioni successive offre supporto nativo per l'autenticazione con smart card nella finestra di login e per l'autenticazione dei certificati del client per i siti web in Safari. Supporta inoltre l'autenticazione basata su Kerberos tramite coppie di chiavi (PKINIT) per SSO sui dispositivi compatibili. Per ulteriori informazioni sulle smart card e macOS, consulta Introduzione all'integrazione delle smart card nella guida *Distribuzione della piattaforma Apple*.

Immagini disco codificate

In macOS, le immagini disco codificate funzionano da container protetti su cui gli utenti possono archiviare o trasferire documenti e altri file sensibili. Le immagini disco codificate sono create con Utility Disco, situata in /Applicazioni/Utility/ e possono essere codificate tramite codifica AES a 128 bit o 256 bit. Poiché un'immagine disco attiva viene trattata come volume locale connesso al Mac, gli utenti possono copiare, spostare e aprire i file e le cartelle archiviati su di essa. Come per FileVault, i contenuti di un'immagine disco sono crittografati e decrittografati in tempo reale. Con le immagini disco codificate, gli utenti possono scambiare documenti, file e cartelle in sicurezza salvando un'immagine disco codificata su un supporto rimovibile, inviandola in allegato a un messaggio email o archiviandola su un server remoto. Per ulteriori informazioni sulle immagini disco codificate, consulta il Manuale utente di Utility Disco.

Sicurezza delle app

Panoramica della sicurezza delle app

Attualmente le app sono gli elementi più critici all'interno di un'architettura di sicurezza. Se, da un lato, le app apportano agli utenti incredibili benefici dal punto di vista della produttività, dall'altro rappresentano un rischio potenziale per la sicurezza del sistema, la stabilità e i dati dell'utente se non sono gestite correttamente.

Per questo motivo, Apple fornisce diversi livelli di protezione affinché le app siano prive di malware noto e non siano state alterate. Inoltre, applica misure di protezione aggiuntive per garantire che l'accesso ai dati utente da parte delle app sia attentamente mediato. Questi controlli di sicurezza forniscono alle app una piattaforma stabile e sicura, permettendo a migliaia di sviluppatori di distribuire centinaia di migliaia di app su iOS, iPadOS e macOS senza compromettere l'integrità del sistema. Inoltre gli utenti possono accedere a tali app sui dispositivi Apple senza temere virus, malware o attacchi non autorizzati.

Su iPhone e iPad, tutte le app vengono scaricate da App Store e sono eseguite in sandbox in modo da essere sottoposte a controlli stringenti.

Sui Mac, molte app sono scaricate da App Store, ma gli utenti Mac possono anche scaricare e utilizzare le app da internet. Per supportare il download in sicurezza delle app da internet, macOS utilizza dei controlli aggiuntivi stratificati. In primo luogo, di default su macOS 10.15 o versione successiva, tutte le app per Mac devono essere autenticate da Apple per poter essere avviate. Questo requisito aiuta a garantire che le app non includano malware senza che debbano obbligatoriamente essere fornite mediante App Store. Inoltre, macOS include una protezione antivirus all'avanguardia per bloccare e, se necessario, rimuovere eventuali malware.

Come controllo aggiuntivo sulle piattaforme, l'esecuzione in sandbox contribuisce alla protezione dei dati utente dall'accesso non autorizzato da parte delle app. E in macOS, anche i dati presenti nelle zone critiche sono protetti e questo aiuta a garantire che gli utenti abbiano sempre il controllo dell'accesso ai file in Scrivania, Documenti, Download e in altre posizioni da parte di tutte le app, indipendentemente dal fatto che le app che tentano l'accesso siano eseguite in sandbox.

Funzionalità nativa	**Equivalente di terze parti**
Elenco di plugin non approvati, elenco di estensioni di Safari non approvate	Definizioni virus/malware
Quarantena file	Definizioni virus/malware
Firme XProtect/YARA	Definizioni virus/malware; protezione endpoint
Gatekeeper	Protezione endpoint; applica la firma del codice alle app per aiutare a garantire che venga eseguito solo software autorizzato.
eficheck (Necessario per i Mac sprovvisti di chip di sicurezza Apple T2)	Protezione endpoint; individuazione rootkit
Firewall applicazioni	Protezione endpoint; firewall
Filtro pacchetti	Soluzioni firewall
Protezione dell'integrità del sistema	Funzionalità integrata in macOS
Controlli di accesso obbligatori	Funzionalità integrata in macOS
Elenco esclusioni estensioni del kernel	Funzionalità integrata in macOS
Firma obbligatoria del codice delle app	Funzionalità integrata in macOS
Autenticazione app	Funzionalità integrata in macOS

Sicurezza delle app in iOS e iPadOS

Introduzione alla sicurezza delle app in iOS e iPadOS

A differenza di altre piattaforme mobili, iOS e iPadOS non consentono agli utenti di installare app non firmate potenzialmente nocive scaricate da siti web o di eseguire app non attendibili. Nei paesi non appartenenti all'UE, tutte le app devono essere scaricate dall'App Store, dove tutte provengono da sviluppatori certificati e devono superare una revisione sia automatica che manuale. In fase di esecuzione, durante il caricamento delle app vengono eseguiti controlli della firma del codice di tutte le pagine di memoria eseguibili, per aiutare a garantire che un'app non sia stata modificata dall'ultima volta che è stata installata o aggiornata.

Una volta verificato che l'app proviene da una fonte approvata, iOS e iPadOS applicano le misure di sicurezza progettate per evitare che altre app o il resto del sistema vengano compromessi.

Sicurezza dell'App Store

L'App Store è uno strumento affidabile in cui gli utenti possono scoprire e scaricare le app in tutta sicurezza. Le app disponibili sull'App Store provengono da sviluppatori noti che hanno accettato di attenersi alle linee guida Apple e vengono distribuite agli utenti in modo sicuro, poiché sono protette dalla crittografia che ne impedisce la modifica. Ciascuna app e i relativi aggiornamenti vengono sottoposti a revisione per verificare che soddisfino i requisiti previsti per privacy e sicurezza. Questa procedura, che viene costantemente ottimizzata, è stata concepita per tutelare gli utenti e per non permettere a malware, criminali informatici e scammer di penetrare nell'App Store. Inoltre, le app destinate all'infanzia devono attenersi a rigide linee guida in merito a sicurezza e raccolta dei dati pensate appositamente per proteggere questo pubblico vulnerabile e devono essere perfettamente integrate con i controlli parentali su iOS e iPadOS.

Tra le misure di protezione della sicurezza presenti sull'App Store rientrano:

- *Scansioni automatiche per malware noti:* per impedire che penetrino nell'App Store e che raggiungano e danneggino gli utenti.
- *Revisione da parte di un team di persone esperte:* per verificare l'accuratezza della descrizione delle app, inclusi i testi di marketing e le istantanee dello schermo. Questa misura costituisce una valida protezione dagli scam più comuni utilizzati per distribuire malware, che spesso utilizzano le strategie di rappresentazione ingannevole del malware come un'app di successo o presentazione di funzionalità accattivanti, che in realtà non sono disponibili.
- *Controlli manuali:* per verificare che l'app non richieda l'accesso ai dati sensibili quando non è necessario, nonché a valutare in modo più approfondito le app per l'infanzia, al fine di garantire che siano conformi alle rigide regole previste per raccolta dei dati e la sicurezza.

- *Recensioni da parte degli utenti centralizzate e affidabili:* per far emergere eventuali problematiche e ridurre le possibilità degli hacker di raggiungere un vasto numero di utenti. Anche se, durante la procedura di revisione, un'app dannosa riuscisse a celare completamente il proprio comportamento, gli utenti che rilevano e segnalano eventuali problemi avvisano anche altri, oltre ad Apple, offrendo un'ulteriore possibilità di identificare tali minacce. L'App Store contrasta attivamente le recensioni fraudolente per migliorare il valore del suo servizio.
- *Procedure per la correzione e la rimozione dei problemi:* nel caso in cui si verifichino. Se un'app viene ammessa nell'App Store, ma in seguito emerge una violazione delle linee guida, Apple collabora con lo sviluppatore per risolvere il problema tempestivamente. Nei casi di maggiore pericolo, che comportano attività fraudolente e dannose, l'app viene rimossa immediatamente dall'App Store e il comportamento nocivo dell'app verrà comunicato tramite notifica agli utenti che l'hanno scaricata.

La sicurezza delle app per iOS e iPadOS deriva dalla combinazione di una serie di fattori: una procedura affidabile di recensione delle app per impedire l'installazione delle app dannose e solidi strumenti di protezione della piattaforma per limitarne gli effetti nocivi. Le funzionalità di sicurezza integrate in iOS e iPadOS offrono agli utenti una protezione efficace e leader del settore, tuttavia non sono progettate per contrastare le scelte che gli utenti potrebbero essere indotti a fare in modo fraudolento. La funzionalità di revisione delle app applica le policy dell'App Store concepite per proteggere gli utenti dalle app che potrebbero danneggiarli o indurli a concedere l'accesso a dati sensibili. Inoltre, nei casi più gravi di app dannose che tentano di aggirare le protezioni sul dispositivo, la revisione delle app ostacola in modo significativo la possibilità di raggiungere il dispositivo dell'utente.

Sebbene le sole misure di sicurezza sull'App Store non possano riuscire a offrire una protezione perfetta, nel contesto della più ampia strategia di sicurezza della piattaforma contribuiscono a rendere più macchinosi gli attacchi diffusi contro gli utenti di iOS e iPadOS, ma soprattutto meno vantaggiosi dal punto di vista economico. Apple si impegna a proteggere la sicurezza dell'ecosistema e a offrire maggiore tranquillità ai propri clienti, sottoponendo ciascuna app a revisione prima di pubblicarla sull'App Store, per garantire che siano prive di malware e che le sue funzionalità siano descritte in modo veritiero per gli utenti, nonché rimuovendo tempestivamente le app dannose dalla distribuzione per limitare la diffusione di varianti future.

Processo di firma del codice delle app in iOS e iPadOS

In iOS e iPadOS, Apple garantisce la sicurezza delle app attraverso meccanismi come la firma obbligatoria del codice, la firma da parte degli sviluppatori e altro ancora.

Firma obbligatoria del codice

Il kernel di iOS e iPadOS, una volta avviato, controlla i processi utente e le app che possono venire eseguite. Per aiutare a garantire che tutte le app provengano da una fonte conosciuta e approvata, e che non siano state alterate, iOS e iPadOS richiedono che tutto il codice eseguibile venga firmato utilizzando un certificato emesso da Apple. Le app fornite con il dispositivo, come Mail e Safari, sono firmate da Apple. Anche le app di terze parti devono essere convalidate e firmate utilizzando un certificato emesso da Apple. La firma del codice obbligatoria amplia il concetto di catena di attendibilità dal sistema operativo alle app, e aiuta a impedire alle app di terze parti di caricare risorse codice non firmate o di usare codice auto modificante.

Firma delle app da parte degli sviluppatori

Gli sviluppatori possono firmare le proprie app attraverso la convalida dei certificati (tramite l'Apple Developer Program). Possono inoltre integrare dei framework all'interno delle proprie app e far convalidare tale codice con un certificato emesso da Apple (tramite una stringa che identifica il team).

- *Convalida dei certificati:* per poter sviluppare e installare app su iPhone o iPad, gli sviluppatori devono registrarsi presso Apple e prendere parte all'Apple Developer Program. Prima di emettere il certificato, Apple verifica l'identità reale di ogni sviluppatore, sia esso un individuo o un'azienda. Questo certificato consente agli sviluppatori di firmare le app e di inviarle ad App Store per la distribuzione. Il risultato è dunque che tutte le app presenti in App Store sono state consegnate da una persona o da un'organizzazione identificabile, e questo serve come deterrente per la creazione di app pericolose. Inoltre, le app sono state verificate da Apple per aiutare a garantire che in generale funzionino come descritto e che non contengano errori evidenti o altri problemi. Oltre alla tecnologia di cui abbiamo parlato poco fa, questo processo di selezione dà agli utenti la sicurezza che le app che acquistano siano di qualità.
- *Convalida della firma del codice:* iOS e iPadOS permettono agli sviluppatori di incorporare nelle proprie app dei framework che possono essere utilizzati dall'app stessa o da estensioni incorporate all'interno dell'app. Per proteggere il sistema e altre app ed evitare che carichino codice di terze parti all'interno del loro spazio di indirizzi, il sistema esegue una convalida della firma del codice di tutte le librerie dinamiche a cui un processo si collega all'avvio. Questa verifica si compie attraverso l'identificatore di team (Team ID), che viene estratto da un certificato emesso da Apple. Un identificatore di team è una stringa alfanumerica di lunghezza pari a 10 caratteri; ad esempio, 1A2B3C4D5F. Un programma può collegarsi a qualunque libreria della piattaforma fornita con il sistema o qualunque libreria che abbia nella firma del codice lo stesso identificatore di team dell'eseguibile principale. Dal momento che gli eseguibili forniti come parte del sistema non hanno un identificatore di team, tali programmi potranno collegarsi solo a librerie facenti parte del sistema stesso.

Verificare le app proprietarie sviluppate in-house

Le aziende considerate idonee in base ai requisiti sotto indicati hanno la possibilità di scrivere app proprietarie in-house da utilizzare all'interno dell'organizzazione e da distribuire ai propri dipendenti. Le aziende e le organizzazioni possono iscriversi al programma Apple Developer Enterprise Program (ADEP). Per ulteriori informazioni e per rivedere i requisiti di idoneità, visita il sito web dell'Apple Developer Enterprise Program. Dopo che un'organizzazione è entrata a far parte dell'ADEP, può registrarsi per ottenere un profilo di provisioning che permetta alle app proprietarie sviluppate in-house di essere eseguite sui dispositivi autorizzati.

Gli utenti devono a loro volta avere il profilo di provisioning installato per poter eseguire queste app. In questo modo si aiuta a garantire che solo gli utenti previsti dall'organizzazione siano in grado di caricare le app sui propri iPhone o iPad. Le app installate tramite soluzione MDM sono considerate implicitamente affidabili, perché la relazione tra l'organizzazione e il dispositivo è già stata stabilita. Negli altri casi, gli utenti devono approvare il profilo di provisioning dell'app in Impostazioni. Le organizzazioni possono anche impedire agli utenti di approvare le app provenienti da sviluppatori sconosciuti. Al primo avvio di qualsiasi app proprietaria sviluppata in-house, il dispositivo deve ricevere da Apple una conferma del fatto che l'esecuzione dell'app è autorizzata.

Sicurezza dei processi in esecuzione in iOS e iPadOS

iOS e iPadOS aiutano a garantire la sicurezza dei processi in esecuzione utilizzando le sandbox, le autorizzazioni dichiarate e il meccanismo ASLR (Address Space Layout Randomization).

Sandbox

Tutte le app di terze parti sono eseguite in sandbox, ovvero non possono accedere ai file archiviati da altre app o apportare delle modifiche al dispositivo. Il meccanismo di sandboxing è progettato per fare in modo che le app non possano raccogliere o modificare le informazioni archiviate da altre app. Ogni app dispone di una directory Inizio univoca per i propri file, che viene assegnata in maniera casuale al momento dell'installazione della app. Se un'app di terze parti deve accedere a informazioni diverse dalle proprie, lo può fare unicamente usando i servizi forniti specificamente da iOS e iPadOS.

Anche i file di sistema e le risorse sono separati rispetto alle app dell'utente. La maggior parte dei file di sistema e delle risorse di iOS e iPadOS viene eseguita come utente "mobile" non privilegiato, come succede per tutte le app di terze parti. L'intera partizione del sistema operativo è attivata come volume di sola lettura. Gli strumenti non necessari, come i servizi di login remoto, non sono inclusi nel software di sistema e le API non consentono alle app di far valere i propri privilegi per modificare altre app o gli stessi iOS e iPadOS.

Uso di autorizzazioni

L'accesso da parte delle app di terze parti alle informazioni dell'utente e a funzionalità come iCloud e l'estensibilità è controllato tramite autorizzazioni dichiarate. Le autorizzazioni sono coppie chiave-valore registrate in un'app che consentono l'autenticazione indipendentemente da altri fattori di esecuzione, come l'ID utente Unix. Dato che le autorizzazioni sono firmate digitalmente, non possono essere modificate. Le autorizzazioni sono ampiamente usate da app di sistema e daemon per eseguire operazioni privilegiate specifiche che richiederebbero altrimenti di eseguire il processo come root. In questo modo si riduce al minimo il rischio potenziale di sorpasso dei privilegi da parte di app di sistema o daemon compromessi.

Inoltre, le app possono solo eseguire processi in background tramite API fornite dal sistema. Ciò consente alle app di continuare a funzionare senza peggiorare le prestazioni o senza avere un impatto significativo sulla durata della batteria.

ASLR

L'ASLR (Address Space Layout Randomization) è un meccanismo che aiuta a proteggere il sistema contro lo sfruttamento di bug che causano il danneggiamento della memoria. Le app incorporate usano ASLR per aiutare a garantire che tutte le regioni della memoria vengano assegnate in modo casuale all'avvio. Oltre a funzionare all'avvio, l'ASLR organizza in modo casuale degli indirizzi di memoria del codice eseguibile, delle librerie di sistema e dei blocchi di programmazione relativi, riducendo ulteriormente la probabilità di molti tipi di attacchi. Ne sono un esempio i tentativi di attacco return-to-libc mirati a ingannare il dispositivo affinché esegua codice dannoso manipolando gli indirizzi di memoria delle librerie dello stack e del sistema. La posizione casuale degli indirizzi di memoria rende più difficile eseguire l'attacco, specialmente su diversi dispositivi. Xcode e gli ambienti di sviluppo per iOS e iPadOS, compilano automaticamente i programmi di terze parti con il supporto ASLR attivato.

Funzionalità “Execute Never”

iOS e iPadOS forniscono un ulteriore strumento di protezione utilizzando la funzionalità “Execute Never” (XN) di ARM, che contrassegna le pagine di memoria come non eseguibili. Le pagine di memoria contrassegnate come scrivibili ed eseguibili possono essere utilizzate solo da app sotto condizioni estremamente controllate. Il kernel verifica la presenza dell’autorizzazione per la firma del codice dinamica esclusiva di Apple. Dopo ciò, può comunque essere effettuata solo una singola chiamata `mmap` per richiedere una pagina scrivibile ed eseguibile, a cui viene assegnato un indirizzo casuale. Safari utilizza questa funzionalità per il compilatore JavaScript Just-in-Time (JIT).

Supporto di estensioni in iOS, iPadOS e macOS

iOS, iPadOS e macOS consentono alle app di fornire funzionalità ad altre app attraverso le estensioni. Le estensioni sono binari eseguibili firmati con uno scopo specifico, inseriti in un pacchetto all’interno di un’app. Durante l’installazione, il sistema rileva automaticamente le estensioni e le rende disponibili ad altre app tramite un sistema di corrispondenze.

Punti di estensione

L’area di sistema che supporta le estensioni è chiamata *punto di estensione*. Ogni punto di estensione fornisce delle API e applica delle politiche per quell’area specifica. Il sistema determina le estensioni disponibili basandosi su regole di corrispondenza specifiche per ciascun punto di estensione. Il sistema avvia automaticamente i processi di estensione quando necessario e ne gestisce la durata. Per limitare la disponibilità delle estensioni ad app di sistema specifiche, possono essere utilizzate le autorizzazioni. Ad esempio, un widget per la vista Oggi compare solo in Centro Notifiche e un’estensione di condivisione è disponibile solo dal pannello Condivisione. Esempi di punti di estensione sono i widget della vista Oggi, la condivisione, le azioni, la modifica delle foto, i provider di file e le tastiere personalizzate.

Comunicazione tra le estensioni

Le estensioni vengono eseguite nel proprio spazio di indirizzi. La comunicazione tra l’estensione e l’app da cui è stata attivata utilizza comunicazioni inter-process (IPC) mediate dal framework di sistema. Non hanno accesso ai rispettivi file o spazi di memoria. Le estensioni sono progettate per essere isolate l’una dall’altra, oltre che dalle app che le contengono e da quelle che le utilizzano. Sono eseguite in sandbox come ogni altra app di terze parti e dispongono di un contenitore separato da quello che contiene l’app. Condividono comunque lo stesso accesso ai controlli per la privacy. Quindi se un utente concede a un’app l’accesso a Contatti, questa concessione viene estesa alle estensioni che sono incorporate all’interno dell’app, ma non a quelle attivate dall’app.

Uso delle tastiere personalizzate

Le tastiere personalizzate sono un tipo speciale di estensione, abilitate dall’utente per l’intero sistema. Una volta abilitate, le estensioni per tastiera vengono usate per qualsiasi campo di testo, fatta eccezione per quello dedicato all’inserimento del codice ed eventuali viste sicure. Per limitare il trasferimento dei dati dell’utente, le tastiere personalizzate vengono eseguite di default in una sandbox molto restrittiva che blocca l’accesso alla rete, ai servizi che eseguono operazioni di rete per conto di un processo e ad API che permetterebbero all’estensione di far trapelare dati di digitazione. Gli sviluppatori di tastiere personalizzate possono richiedere che le loro estensioni abbiano Open Access, che permette al sistema di eseguire l’estensione nella sandbox di default dopo aver ottenuto il consenso dell’utente.

MDM ed estensioni

Per i dispositivi registrati in una soluzione di gestione dei dispositivi mobili (MDM), le estensioni di documenti e tastiere rispettano le regole Managed Open In. Ad esempio, la soluzione MDM può aiutare a impedire che un utente esporti un documento da un'app gestita a un provider di documenti non gestito, oppure che utilizzi una tastiera non gestita con un'app gestita. Inoltre, gli sviluppatori di app possono impedire l'uso di estensioni di tastiera di terze parti all'interno della propria app.

Protezione delle app e dei gruppi di app in iOS e iPadOS

In iOS e iPadOS, le organizzazioni possono proteggere le proprie app in modo sicuro utilizzando il kit SDK per iOS ed entrando in un gruppo di app nel portale Apple Developer.

Adozione della protezione dati nelle app

Il kit SDK (Software Development Kit) per iOS e iPadOS offre una suite completa di API grazie alla quale gli sviluppatori di terze parti e in-house possono adottare con estrema facilità la protezione dati, garantendo il massimo livello di protezione nelle app. La protezione dati è disponibile per API di file e di database, inclusi NSFileManager, CoreData, NSData e SQLite.

Il database dell'app Mail (inclusi gli allegati), i libri gestiti, i segnalibri di Safari, le immagini all'avvio delle app e i dati di localizzazione sono archiviati tramite codifica con chiavi protette mediante il codice dell'utente sul dispositivo. Calendario (esclusi gli allegati), Contatti, Promemoria, Note, Messaggi e Foto implementano la `Data Protection` *"Protetto fino alla prima autenticazione utente"*.

Le app installate dall'utente che non optano per una classe specifica di protezione dati ricevono automaticamente la classe "Protetto fino alla prima autenticazione utente".

Appartenenza a un gruppo di app

Le app e le estensioni possedute da un determinato account sviluppatore possono condividere i contenuti se configurate per fare parte di un gruppo di app. La creazione dei gruppi appropriati sul portale Apple Developer e l'aggiunta dell'insieme desiderato di app ed estensioni è compito dello sviluppatore. Le app, dopo essere state configurate come parte di un gruppo di app, hanno accesso a:

- Un contenitore sul volume condiviso a scopo di archiviazione che rimane sul dispositivo fino a quando almeno una delle app appartenenti al gruppo è installata.
- Preferenze condivise
- Elementi del portachiavi condivisi

Il portale Apple Developer aiuta a garantire che gli ID dei gruppi (GID) di app siano unici in tutto l'ecosistema di app.

Sicurezza delle app in macOS

Introduzione alla sicurezza delle app in macOS

La sicurezza delle app in macOS è garantita da una serie di livelli sovrapposti, il primo dei quali è rappresentato dall'opzione di eseguire solo app firmate e autorizzate di App Store. Inoltre, i vari livelli di protezione di macOS aiutano a garantire che le app scaricate da internet siano prive di malware noti. macOS offre tecnologie che rilevano e rimuovono il codice dannoso e offre protezioni aggiuntive progettate per impedire alle app non attendibili di accedere ai dati degli utenti. I servizi Apple come quello di autorizzazione e gli aggiornamenti XProtect sono concepiti per prevenire l'installazione di malware. In caso di necessità, questi servizi localizzano il malware, che in un primo momento potrebbe non essere stato rilevato, e lo rimuovono in modo rapido ed efficiente. Infine, gli utenti di macOS sono liberi di scegliere il modello di sicurezza più adatto alle loro esigenze, avendo anche la possibilità di eseguire codice totalmente non verificato e non firmato.

Processo di firma del codice delle app in macOS

Tutte le app di App Store sono firmate da Apple. La firma è progettata per garantire che non siano state manomesse o alterate. Apple firma ogni app fornita con i dispositivi Apple.

In macOS 10.15, per poter essere eseguite con le impostazioni Gatekeeper di default, tutte le app distribuite al di fuori di App Store devono essere firmate dallo sviluppatore tramite un certificato rilasciato da Apple e corredato da ID sviluppatore (insieme a una chiave privata), e devono inoltre essere autenticate da Apple. Anche le app sviluppate internamente devono essere firmate con un ID sviluppatore rilasciato da Apple in modo che gli utenti possano verificarne l'integrità.

In macOS, la firma del codice e l'autenticazione funzionano in modo indipendente per scopi diversi e possono essere effettuate da agenti diversi. La firma del codice viene effettuata dallo sviluppatore utilizzando il proprio certificato ID sviluppatore (emesso da Apple). La verifica di tale firma garantisce all'utente che il software di uno sviluppatore non sia stato manomesso dal momento in cui lo sviluppatore ha eseguito la build e l'ha firmato. L'autenticazione può essere effettuata da chiunque partecipi alla catena di distribuzione del software e provi che ad Apple è stata fornita una copia del codice perché verifichi la presenza di malware e che non è stato rilevato alcun malware conosciuto. Il risultato dell'autenticazione è un ticket, che viene archiviato sui server di Apple e può essere facoltativamente associato all'app (da chiunque) senza rendere nulla la firma dello sviluppatore.

I MAC (Mandatory Access Controls) richiedono la firma del codice per abilitare le autorizzazioni protette dal sistema. Per esempio, le app che richiedono l'accesso tramite il firewall devono avere la firma del codice con l'autorizzazione MAC appropriata.

Protezione in fase di esecuzione e Gatekeeper in macOS

macOS offre la tecnologia Gatekeeper e la protezione in fase di esecuzione per aiutare a garantire che sul Mac di un utente venga eseguito unicamente software attendibile.

Gatekeeper

macOS include una tecnologia di protezione *chiamata Gatekeeper*, progettata per garantire che sul Mac di un utente venga eseguito unicamente software attendibile. Quando un utente scarica e apre un'app, un plugin o un pacchetto di installazione che non proviene da App Store, Gatekeeper verifica che il software sia di uno sviluppatore verificato, indicato da Apple come privo di contenuti dannosi noti e quindi non alterato. Prima di aprire per la prima volta il software scaricato, Gatekeeper richiede inoltre l'approvazione dell'utente assicurandosi così che l'utente non sia stato indotto ad avviare del codice eseguibile che pensava invece essere un semplice file di dati. Gatekeeper monitora anche la provenienza dei file scritti da software scaricato.

Di default, Gatekeeper aiuta a garantire che tutto il software scaricato sia stato firmato da App Store oppure firmato da uno sviluppatore registrato e autenticato da Apple. Sia il processo di verifica di App Store che il flusso di autenticazione sono progettati per controllare che le app non contengano malware noti. Quindi, *quando viene aperto per la prima volta, di default tutto il software di macOS viene verificato per rilevare la presenza di contenuti dannosi conosciuti, a prescindere dal modo in cui è arrivato sul Mac*.

Gli utenti e le organizzazioni hanno la facoltà di consentire solo l'uso di software installato da App Store. In alternativa, gli utenti possono ignorare le politiche di Gatekeeper per l'apertura di qualsiasi software, salvo nel caso di limitazioni imposte da una soluzione di gestione dei dispositivi mobili (MDM). Le organizzazioni possono usare una soluzione MDM per configurare le impostazioni di Gatekeeper, compresa quella per consentire software firmato con identità alternative. Gatekeeper può anche essere disabilitato completamente, se necessario.

Gatekeeper protegge anche dalla distribuzione di plugin dannosi insieme ad app benigne. In questo caso, l'utilizzo dell'app attiva il caricamento di un plugin dannoso senza che l'utente ne sia a conoscenza. Quando è necessario, Gatekeeper apre le app da posizioni casuali di sola lettura. Questo meccanismo è progettato per impedire il caricamento automatico di plugin distribuiti insieme all'app.

Protezione durante l'esecuzione

I file, le risorse e il kernel di sistema sono separati rispetto allo spazio delle app dell'utente. Tutte le app di App Store sono eseguite in sandbox per limitare l'accesso ai dati archiviati dalle altre app. Se un'app di App Store ha bisogno di accedere ai dati di un'altra app, può farlo solo utilizzando le API e i servizi forniti da macOS.

Protezione dai malware in macOS

Apple implementa un processo basato sulla raccolta di informazioni riguardanti le minacce di sicurezza per identificare e bloccare rapidamente qualsiasi malware.

Tre livelli di difesa

Il meccanismo di difesa contro il malware è strutturato su tre livelli.

1. *Impedire l'avvio e l'esecuzione di malware:* App Store o Gatekeeper combinati con l'autorizzazione.

2. *Bloccare l'esecuzione del malware sui sistemi dei clienti:* Gatekeeper, autorizzazione e XProtect.

3. *Intervenire in caso di esecuzione di malware:* XProtect

Il primo livello di difesa è progettato per inibire la distribuzione del malware e impedirne l'avvio anche una sola volta. Questo è l'obiettivo di App Store e Gatekeeper, insieme al processo di autorizzazione.

Il livello di difesa successivo aiuta a garantire che, nel caso in cui un malware compaia su un Mac, questo venga rapidamente identificato e bloccato, sia per fermarne la diffusione sia per proteggere i sistemi Mac in cui ha già trovato un appiglio. XProtect va ad aggiungersi al meccanismo di difesa, insieme a Gatekeeper e al processo di autorizzazione.

Infine, XProtect agisce per eliminare il malware che è riuscito a essere eseguito.

Queste protezioni, descritte in maggiore dettaglio di seguito, si uniscono per supportare le linee guida sulla protezione da virus e malware. Nei Mac dotati di chip Apple sono presenti anche meccanismi di protezione aggiuntivi, mirati a limitare i potenziali danni causati dal malware che riesce ad essere eseguito. Consulta Protezione dell'accesso delle app ai dati utente per informazioni sul modo in cui macOS protegge i dati degli utenti dal malware e Integrità del sistema operativo per informazioni sul modo in cui macOS può limitare le azioni che un malware può compiere sul sistema.

Autorizzazione

L'*autorizzazione* è un servizio di scansione antimalware fornito da Apple. Gli sviluppatori che vogliono distribuire app per macOS al di fuori di App Store inviano le proprie app perché vengano scansionate come parte del processo di distribuzione. Apple scansiona tale software per verificare la presenza di malware noto e se non ne trova emette un ticket di autorizzazione. Solitamente gli sviluppatori allegano questo ticket alle proprie app, in modo che Gatekeeper possa verificarle e avviarle, anche quando il sistema non è in linea.

Apple può anche emettere un ticket di revoca per le app notoriamente dannose, anche se sono state precedentemente autorizzate. macOS verifica regolarmente la presenza di nuovi ticket di revoca, in modo che Gatekeeper abbia a disposizione le informazioni più recenti e possa bloccare l'avvio di tali file. Questo processo può bloccare le app dannose molto rapidamente, perché gli aggiornamenti avvengono in background persino molto più frequentemente degli aggiornamenti in background relativi alle nuove firme di XProtect. Inoltre questa protezione può essere applicata sia alle app precedentemente autorizzate sia a quelle che non lo sono state.

XProtect

macOS include una tecnologia antivirus integrata chiamata *XProtect*, pensata per il rilevamento e la rimozione del malware basata sulle firme. Il sistema utilizza le firme YARA, uno strumento adottato per condurre rilevazioni di malware basate sulle firme che Apple aggiorna regolarmente. Apple verifica la presenza di infezioni malware e alterazioni, e aggiorna automaticamente le firme, a prescindere dagli aggiornamenti di sistema, per contribuire alla difesa dei Mac dalle infezioni malware. XProtect rileva e blocca automaticamente l'esecuzione di malware noto. In macOS 10.15 o versioni successive, XProtect verifica la presenza di contenuti nocivi conosciuti ogni volta che:

- Un'app viene avviata per la prima volta.
- Un'app è stata modificata (nel file system).
- Le firme di XProtect vengono aggiornate.

Quando XProtect rileva malware noto, il software viene bloccato; l'utente riceve una notifica di tale blocco e gli viene chiesto se vuole spostare il software nel Cestino.

Nota: l'autorizzazione è efficace contro file (o hash di file) noti e può essere utilizzata su app che sono state avviate precedentemente. Le regole basate sulle firme di XProtect sono più generiche rispetto all'hash di un file specifico, in modo da consentirgli di rilevare varianti che Apple non conosce. XProtect scansiona soltanto le app che hanno subito delle modifiche o che vengono aperte per la prima volta.

Qualora il malware dovesse riuscire a insinuarsi in un Mac, XProtect include anche una tecnologia per rimediare alle infezioni. Ad esempio, include un meccanismo in grado di rimediare alle infezioni basato sugli aggiornamenti forniti automaticamente da Apple (come parte degli aggiornamenti automatici dei file di dati di sistema e degli aggiornamenti di sicurezza). Questo sistema rimuove il malware non appena riceve informazioni aggiornate e continua a controllare periodicamente la presenza di infezioni. Tuttavia, XProtect non riavvia il Mac automaticamente. Inoltre, XProtect include un engine avanzato per il rilevamento di malware sconosciuto sulla base dell'analisi del comportamento. Le informazioni sul malware rilevate da questo engine, tra cui il software con cui è stato scaricato, vengono utilizzate per migliorare le firme di XProtect e la sicurezza di macOS.

Aggiornamenti automatici di sicurezza per XProtect

Apple rilascia automaticamente degli aggiornamenti per XProtect sulla base delle informazioni più recenti disponibili riguardo alle minacce. Di default, macOS verifica quotidianamente la disponibilità di tali aggiornamenti. Gli aggiornamenti per il processo di autorizzazione, che vengono distribuiti tramite la sincronizzazione CloudKit, sono molto più frequenti.

La risposta di Apple quando un nuovo malware viene scoperto

Quando un malware viene scoperto, possono essere eseguiti vari passaggi:

- Qualsiasi certificato con ID sviluppatore associato viene revocato.
- Vengono emessi ticket di revoca dell'autorizzazione per tutti i file (app e file associati).
- Vengono sviluppate ed emesse firme per XProtect.

  Tali firme vengono anche applicate in modo retroattivo a software precedentemente autorizzati ed eventuali nuove rilevazioni di codice dannoso possono attivare una o più azioni tra quelle descritte sopra.

Infine, l'individuazione di un malware fa partire una serie di passaggi nei secondi, ore e giorni successivi che consentono di propagare le migliori protezioni possibili verso tutti gli utenti Mac.

Controllo dell’accesso delle app ai file in macOS

Apple crede che gli utenti debbano avere trasparenza, consapevolezza e controllo totali su ciò che fanno le app con i loro dati. In macOS 10.15, il sistema applica questo modello per aiutare garantire che tutte le app ottengano il consenso dell’utente prima di accedere ai file presenti in Documenti, Download, Scrivania, iCloud Drive e su volumi di rete. In macOS 10.13 o versioni successivi, le app che richiedono l’accesso all’intero dispositivo di archiviazione devono essere aggiunte espressamente in Impostazioni di Sistema (macOS 13 o versioni successive) o in Preferenze di Sistema (macOS 12 o versioni precedenti). Inoltre, le funzionalità di accessibilità e automazione richiedono l’autorizzazione dell’utente, per garantire che non possano eludere altre protezioni. In base alla politica di accesso, agli utenti potrebbe essere richiesto facoltativamente o obbligatoriamente di modificare l’impostazione in:

- In macOS 13 o versioni successive: Impostazioni di Sistema > Privacy e sicurezza > Privacy.
- In macOS 12 o versioni precedenti: Preferenze di Sistema > Sicurezza e privacy > Privacy.

Elemento	Richiesta dell’app all’utente	L’utente deve modificare le impostazioni di privacy di sistema
Accessibilità	✗	✓
Accesso a tutto il dispositivo di archiviazione interna	✗	✓
File e cartelle *Nota:* include Scrivania, Documenti, Download, volumi di rete e volumi rimovibili	✓	✗
Automazione (eventi Apple)	✓	✗

All’utente che attiva FileVault su un Mac viene chiesto di fornire delle credenziali valide prima di continuare il processo di avvio e ottenere l’accesso a modalità di avvio specifiche. Senza credenziali di login valide o una chiave di recupero, l’intero volume resta codificato ed è protetto da accessi non autorizzati anche quando il supporto fisico di archiviazione viene rimosso e collegato a un altro computer.

Per proteggere i dati in ambiente aziendale, gli addetti all’IT dovrebbero definire e applicare delle policy di configurazione di FileVault tramite la gestione dei dispositivi mobili (MDM). Le organizzazioni dispongono di svariate opzioni per la gestione dei volumi codificati, tra cui le chiavi di recupero istituzionali, le chiavi di recupero personali (che possono facoltativamente essere archiviate con la MDM) o un insieme di entrambe. Anche la rotazione delle chiavi può essere impostata come policy nella MDM.

Funzionalità di protezione nell'app Note

L'app Note include una funzionalità di protezione delle note (su iPhone, iPad, Mac e sito web di iCloud) che consente agli utenti di proteggere il contenuto di determinate note. Gli utenti possono anche condividere le note in modo sicuro.

Note protette

Le note protette vengono codificate end-to-end tramite una frase chiave fornita dall'utente, che viene richiesta per visualizzare le note sui dispositivi iOS, iPadOS, macOS e sul sito web di iCloud. Ogni account iCloud (compresi gli account "Su [dispositivo]") può avere una frase chiave.

Quando un utente protegge una nota, viene generata una chiave a 16 byte tramite PBKDF2 e SHA256 a partire dalla frase chiave dell'utente. La nota e tutti gli allegati che contiene sono codificati tramite AES-GCM (AES con modalità Galois/Counter). In Core Data e CloudKit vengono creati nuovi record per archiviare la nota codificata, gli allegati, l'etichetta e il vettore di inizializzazione e, in seguito a tale creazione, i dati originali decrittografati vengono eliminati. Gli allegati che supportano la codifica includono immagini, disegni, tabelle, mappe e siti web. Le note con altri tipi di allegati non potranno essere codificate e gli allegati non supportati non potranno essere aggiunti alle note protette.

Per visualizzare una nota protetta, l'utente deve inserire la propria frase chiave oppure eseguire l'autenticazione tramite Face ID o Touch ID. Dopo la corretta autenticazione dell'utente per visualizzare o creare una nota protetta, Note si apre in una sessione protetta, durante la quale l'utente può visualizzare le note protette o crearne di altre senza doversi autenticare ulteriormente. Tuttavia nella sessione sicura saranno visualizzate unicamente le note protette tramite la frase chiave attuale. Per le note protette tramite una frase chiave diversa, l'utente dovrà comunque autenticarsi. La sessione protetta viene chiusa quando:

- L'utente tocca il pulsante "Proteggi ora" in Note.
- Note viene messa in background per più di 3 minuti (8 minuti in macOS).
- Il dispositivo iOS o iPadOS si blocca.

Per modificare la frase chiave per una nota protetta, l'utente deve inserire la frase chiave attuale, perché Face ID e Touch ID non sono disponibili durante la modifica della frase chiave. Una volta scelta la nuova frase chiave, l'app Note cifra nuovamente, nello stesso account, le chiavi di tutte le note esistenti e codificate con la frase chiave precedente.

Se un utente scrive in modo errato per tre volte consecutive la frase chiave, Note mostra un suggerimento fornito dall'utente, se ne era stato fornito uno durante la configurazione. Se l'utente non ricorda comunque la frase chiave, può reimpostarla nelle impostazioni di Note. Questa funzionalità consente agli utenti di creare nuove note protette con una frase chiave nuova, ma non consente loro di visualizzare le note protette in precedenza. Tali note potranno essere visualizzate se verrà ricordata la frase chiave utilizzata per proteggerle. Per reimpostare la frase chiave è necessaria la frase chiave dell'account iCloud dell'utente.

Note condivise

Le note che non sono protette tramite codifica end-to-end con una frase chiave possono essere condivise con gli altri. Le note condivise utilizzano comunque il tipo di dati codificati di CloudKit per qualsiasi testo o allegato inserito dall'utente in una nota. Le risorse sono sempre codificate con una chiave che è crittografata in CKRecord. I metadati, come le date di creazione e modifica, non sono codificati. CloudKit gestisce il processo che consente agli utenti di codificare e decrittografare i dati altrui.

Funzionalità di protezione nell'app Comandi Rapidi

Nell'app Comandi Rapidi, i comandi vengono sincronizzati facoltativamente tra i dispositivi Apple tramite iCloud. I comandi possono anche essere condivisi con altri utenti tramite iCloud e sono archiviati localmente in un formato codificato.

I comandi personalizzati sono versatili, sono simili a script o programmi. Quando i comandi rapidi vengono scaricati da internet, l'utente viene avvisato del fatto che il comando non è stato verificato da Apple e gli viene data la possibilità di analizzarlo. Come misura di protezione contro i comandi rapidi nocivi, vengono scaricate le definizioni di malware aggiornate per identificare i comandi nocivi nel momento dell'esecuzione.

I comandi personalizzati possono eseguire anche codice JavaScript specificato dall'utente sui siti web in Safari, se avviato dal pannello di condivisione. Per garantire protezione da codice JavaScript dannoso che, ad esempio, potrebbe indurre l'utente a eseguire uno script su un sito di social media che raccoglierebbe i suoi dati, il codice JavaScript viene analizzato a fronte delle definizioni malware menzionate in precedenza. Quando l'utente esegue per la prima volta codice JavaScript su un dominio, gli viene richiesto di consentire ai comandi contenenti JavaScript di essere eseguiti sulla pagina web attuale del dominio.

Sicurezza dei servizi

Panoramica della sicurezza dei servizi

Apple ha creato un solido insieme di servizi per aiutare gli utenti a ottenere efficienza e produttività ancora maggiori dai propri dispositivi. Questi servizi forniscono potenti funzionalità per l'archiviazione sul cloud, la sincronizzazione, l'archiviazione delle password, l'autenticazione, i pagamenti, la messaggistica, le comunicazioni e altro ancora; il tutto proteggendo sempre la privacy degli utenti e la sicurezza dei loro dati.

Questo capitolo è dedicato alle tecnologie di sicurezza utilizzate in iCloud, "Accedi con Apple", Apple Pay, iMessage, Apple Messages for Business, FaceTime, Dov'è e Continuity.

Nota: non tutti i servizi e i contenuti Apple sono disponibili in tutti i paesi e in tutte le zone.

ID Apple e ID Apple gestito

Panoramica sulla sicurezza dell'ID Apple

L'ID Apple è l'account che utilizzi per accedere ai servizi Apple. È importante che gli utenti tengano al sicuro i propri ID Apple, così da aiutare ad evitare l'accesso non autorizzato ai loro account. Per contribuire in questo senso, gli ID Apple richiedono password sicure che:

- Devono avere una lunghezza minima di otto caratteri.
- Devono contenere sia lettere che numeri.
- Non devono contenere più di tre caratteri identici consecutivi.
- Non possono essere password utilizzate comunemente.

Gli utenti sono incoraggiati ad andare oltre queste linee guida, aggiungendo altri caratteri e segni di punteggiatura per rendere le password ancora più efficaci.

Inoltre, Apple invia e-mail e/o notifiche push agli utenti quando vengono effettuati cambiamenti importanti ai loro account, come la modifica di una password o delle informazioni di fatturazione oppure se l'ID Apple è stato utilizzato per accedere a un servizio su un nuovo dispositivo. Gli utenti sono invitati a cambiare immediatamente la password dell'ID Apple nel caso in cui non riconoscano l'azione eseguita.

Inoltre, Apple fa uso di una gamma di politiche e procedure volte a proteggere gli account utente. Tra queste, vi è la limitazione del numero di tentativi errati di accesso o di reimpostazione della password, il controllo attivo anti-frode, per aiutare nell'identificazione degli attacchi nel momento in cui si verificano, e revisioni periodiche delle proprie politiche, che consentono ad Apple di adattarsi a eventuali nuove informazioni riguardanti la sicurezza degli utenti.

Nota: la politica relativa alla password dell'ID Apple gestito viene impostata da un amministratore in Apple School Manager o Apple Business Manager.

Autenticazione a due fattori

Per aiutare gli utenti a proteggere ancora di più i propri account, Apple utilizza di default l'*autenticazione a due fattori*, un ulteriore livello di sicurezza per gli ID Apple. È pensata per garantire che l'accesso all'account possa avvenire unicamente da parte del proprietario dell'account, anche nel caso in cui qualcun altro sia a conoscenza della password. Con l'autenticazione a due fattori, l'accesso all'account di un utente può avvenire solo tramite dispositivi ritenuti attendibili, come l'iPhone, l'iPad o il Mac dell'utente, oppure su un altro dispositivo una volta completata una verifica tramite uno di questi dispositivi attendibili o tramite un numero di telefono autorizzato. Per effettuare l'accesso per la prima volta su un nuovo dispositivo, occorrono due dati: la password dell'ID Apple e un codice di verifica a sei cifre che viene visualizzato sui dispositivi autorizzati dell'utente oppure inviato a un numero di telefono autorizzato. Inserendo il codice, l'utente conferma di voler autorizzare il nuovo dispositivo e di considerare sicuro l'accesso. Poiché la sola password non è più sufficiente a garantire l'accesso a un account utente, l'autenticazione a due fattori rappresenta un miglioramento della sicurezza dell'ID Apple e di tutte le informazioni personali archiviate presso Apple. Questo tipo di autenticazione è integrato in iOS, iPadOS, macOS, tvOS, watchOS e nei sistemi di autenticazione utilizzati sui siti web di Apple.

Quando un utente accede a un sito web di Apple usando un browser web, viene inviata la richiesta di un secondo fattore a tutti i dispositivi attendibili associati all'account iCloud dell'utente, richiedendo l'approvazione per la sessione web. Se l'utente accede a un sito web di Apple da un browser su un dispositivo autorizzato, visualizza il codice di verifica sul dispositivo che sta usando. Quando l'utente inserisce il codice su tale dispositivo, la sessione web viene approvata.

Inizializzazione della password e recupero dell'account

Se la password di un account ID Apple viene dimenticata, l'utente può inizializzarla su un dispositivo autorizzato. Se non è disponibile un dispositivo autorizzato e si conosce la password, è possibile effettuare l'autenticazione con un numero di telefono autorizzato tramite la verifica via SMS. Inoltre, per effettuare il recupero immediato di un ID Apple, è possibile utilizzare un codice usato in precedenza, insieme a un SMS. Se queste opzioni non sono attuabili, sarà necessario seguire la procedura di recupero dell'account. Per ulteriori informazioni, consulta l'articolo del supporto Apple Come utilizzare la procedura di recupero dell'account quando non è possibile reimpostare la password dell'ID Apple.

Sicurezza dell'ID Apple gestito

Gli ID Apple gestiti funzionano in modo simile a un ID Apple, ma sono di proprietà di un'organizzazione aziendale o didattica che li controlla e che può reimpostare le password, limitare gli acquisti e l'uso di app per la comunicazione, come FaceTime e Messaggi, e configurare dei permessi, diversi in base al ruolo, per i dipendenti, per il personale, per i docenti e per gli studenti.

Per gli ID Apple gestiti, alcuni servizi sono disabilitati (per esempio, Apple Pay, HomeKit e Dov'è).

Gestione degli accessi per gli ID Apple gestiti

Le organizzazioni possono utilizzare la funzionalità di gestione degli accessi disponibile in Apple Business Manager, Apple School Manager e Apple Business Essentials per definire dove è possibile utilizzare gli ID Apple gestiti e per quali servizi.

La gestione degli accessi consente di determinare se gli utenti possono accedere con un ID Apple gestito su qualsiasi dispositivo, soltanto sui dispositivi gestiti o soltanto sui dispositivi gestiti e supervisionati. Inoltre, gli amministratori possono configurare l'impostazione che consente agli utenti di accedere ad iCloud dal web. In questo modo, le organizzazioni possono utilizzare lo stato di gestione del dispositivo come un fattore per decidere se concedere o meno l'accesso ai dati aziendali.

Inoltre, gli amministratori possono selezionare i servizi iCloud disponibili agli utenti. Tra questi sono inclusi la definizione dell'accesso agli Apple Developer Program o ad AppleSeed per il programma di test delle versioni beta del software e l'autorizzazione degli utenti ad accedere al portale Apple dedicato alla privacy all'indirizzo privacy.apple.com.

Gli ID Apple gestiti supportano anche la collaborazione sui documenti elaborati con Keynote, Numbers, Pages, su app come Promemoria e Note, oltre alla comunicazione con FaceTime e iMessage. In relazione a questi servizi, le organizzazioni sono in grado di definire se gli utenti possono collaborare con chiunque oppure soltanto con gli account creati all'interno della stessa organizzazione in Apple School Manager, Apple Business Manager o Apple Business Essential.

Se le regole per la gestione degli accessi cambiano, le modifiche si rifletteranno sui dispositivi ai quali l'utente ha effettuato l'accesso con il proprio ID Apple gestito. Se, invece, vengono modificati i requisiti per lo stato di gestione di un dispositivo, l'ID Apple gestito viene scollegato automaticamente dal dispositivo, se il suo stato non soddisfa i nuovi requisiti.

Controllo degli ID Apple gestiti

Gli ID Apple gestiti creati in Apple School Manager supportano, inoltre, la possibilità di essere *controllati*, consentendo così alle organizzazioni di soddisfare le norme legali e relative alla privacy. Un utente con il ruolo di amministratore, manager del sito, del personale o istruttore può esaminare determinati account corrispondenti all'ID Apple gestito.

Un utente può controllare esclusivamente account di livello inferiore nella gerarchia dell'organizzazione; vale a dire che i docenti possono controllare gli studenti, i manager possono controllare i docenti e gli studenti, gli amministratori possono controllare manager, docenti e studenti.

Quando, tramite Apple School Manager, vengono richieste delle credenziali per il controllo, viene creato un account speciale che ha accesso solo all'ID Apple gestito per cui è stato richiesto il controllo. Chi sta effettuando il controllo può leggere e modificare i contenuti dell'utente controllato archiviati su iCloud o in app compatibili con CloudKit. Tutte le richieste di accesso con privilegi di controllo vengono registrate in Apple School Manager. I log mostrano il nome di chi ha inoltrato la richiesta, l'ID Apple gestito per cui è stata effettuata la richiesta di controllo, l'ora della richiesta e se il controllo è stato effettivamente realizzato.

iCloud

Panoramica della sicurezza di iCloud

iCloud archivia contatti, calendari, foto, documenti e altri file dell'utente mantenendoli aggiornati su tutti i suoi dispositivi, automaticamente. Può essere utilizzato anche da app di terze parti per memorizzare e sincronizzare non solo documenti, ma anche i valori chiave per i dati delle app, come definito dallo sviluppatore. Gli utenti configurano iCloud accedendo con un ID Apple e scegliendo quali servizi desiderano utilizzare. Alcune funzionalità di iCloud, come iCloud Drive e backup di iCloud possono essere disabilitate da amministratori IT tramite i profili di configurazione utilizzando una soluzione di gestione dei dispositivi mobili (MDM).

iCloud utilizza metodi di sicurezza molto efficaci e applica criteri rigorosi per proteggere i dati degli utenti. La maggior parte dei dati iCloud viene crittografata sul dispositivo dell'utente utilizzando chiavi iCloud generate dal dispositivo, prima di essere caricata sui server iCloud. Per i dati non crittografati end-to-end, il dispositivo dell'utente carica in modo sicuro queste chiavi iCloud sui moduli di sicurezza hardware di iCloud nei data center Apple. Ciò consente ad Apple di aiutare l'utente nel recupero dei dati e di decrittografare i dati per conto dell'utente ogni volta che ne ha bisogno (ad esempio, quando accede a un nuovo dispositivo, ripristina i dati da un backup o accede ai dati iCloud sul web). I dati trasferiti dai dispositivi dell'utente e ai server iCloud e viceversa sono crittografati separatamente in transito con TLS e i server iCloud archiviano i dati dell'utente con un ulteriore livello di crittografia a riposo.

Le chiavi di crittografia, quando disponibili per Apple, sono protette nei data center Apple. Quando vengono elaborati i dati archiviati in data center di terze parti, solo il software Apple eseguito su server sicuri ha accesso a tali chiavi di crittografia e soltanto quando vengono effettuate le necessarie elaborazioni. Per offrire un livello maggiore di privacy e sicurezza, molti dei servizi Apple utilizzano la crittografia end-to-end, il che significa che i dati iCloud dell'utente sono accessibili unicamente all'utente stesso ed esclusivamente da dispositivi autorizzati su cui ha eseguito l'accesso con il proprio ID Apple.

Apple offre agli utenti due opzioni per crittografare e proteggere i dati archiviati su iCloud:

- **Protezione dei dati standard (impostazione di default):** i dati iCloud dell'utente sono crittografati, le chiavi di crittografia sono protette nei data center Apple e Apple può fornire assistenza per il recupero di dati e account. Solo alcuni dati iCloud, ossia 14 categorie di dati, tra cui i dati sanitari e le password salvate sul portachiavi iCloud, sono crittografati end-to-end.
- **Protezione avanzata dei dati per iCloud:** un'impostazione facoltativa che offre il livello più elevato di sicurezza per i dati sul cloud di Apple. Se un utente sceglie di attivare la protezione avanzata dei dati, i suoi dispositivi affidabili mantengono l'accesso esclusivo alle chiavi di crittografia per la maggior parte dei dati iCloud, proteggendoli con la crittografia end-to-end. Attivando la protezione avanzata dei dati, il numero di categorie di dati che utilizzano la crittografia end-to-end sale a 23 e include Backup, Foto e Note di iCloud e altro ancora.

Le categorie specifiche di dati iCloud protetti con la crittografia end-to-end sono elencate nell'articolo del supporto Apple Panoramica sulla sicurezza dei dati di iCloud.

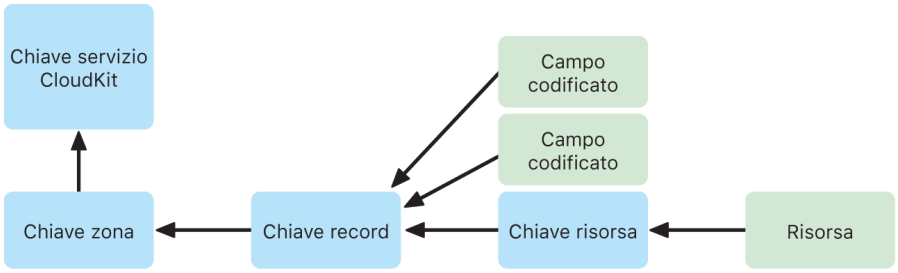
Crittografia iCloud

La crittografia dei dati in iCloud è strettamente legata al modello di archiviazione dei dati, a partire dai framework e dalle API di CloudKit che consentono alle app e al software di sistema di archiviare i dati in iCloud per conto dell'utente e di mantenere tutto aggiornato sui dispositivi e sul web.

Crittografia CloudKit

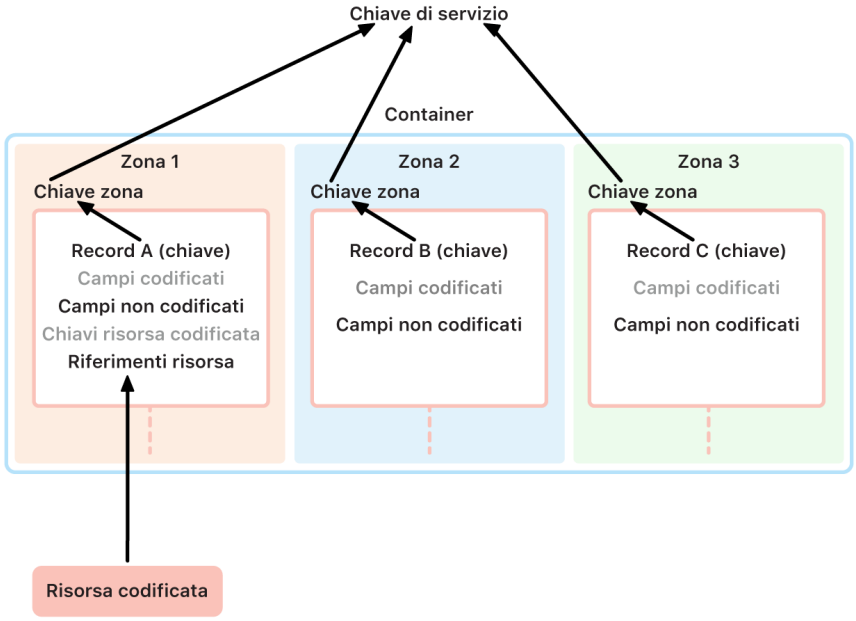
CloudKit è un framework che consente agli sviluppatori di app di archiviare dati chiave-valore, dati strutturati e risorse (dati di grandi dimensioni archiviati separatamente dal database, come immagini o video) in iCloud. CloudKit supporta database sia pubblici che privati, raggruppati in contenitori. I database pubblici sono condivisi a livello globale, vengono di norma utilizzati per attività generiche e non sono crittografati. I database privati contengono i dati iCloud di ciascun utente.

CloudKit utilizza una gerarchia di chiavi che corrisponde alla struttura dei dati. Il database privato di ogni contenitore è protetto da una gerarchia di chiavi, radicata in una chiave asimmetrica denominata *chiave di servizio CloudKit*. Queste chiavi sono uniche per ogni utente iCloud e vengono generate sul dispositivo sicuro di ciascun utente. Quando i dati vengono scritti su CloudKit, tutte le chiavi di registrazione vengono generate sul dispositivo sicuro dell'utente e inserite nella gerarchia di chiavi appropriata prima che i dati vengano caricati.



Molti servizi Apple, elencati nell'articolo del supporto Apple Panoramica sulla sicurezza dei dati iCloud, utilizzano la crittografia end-to-end con una chiave di servizio CloudKit protetta allo stesso modo della sincronizzazione del portachiavi iCloud. Per tali contenitori CloudKit, le chiavi di servizio sono disponibili solo per i dispositivi sicuri dell'utente e né Apple né altre terze parti possono accedervi. Queste chiavi sono sincronizzate sui vari dispositivi dell'utente anche se non viene utilizzato il portachiavi iCloud per la sincronizzazione di password, passkey e altri dati dell'utente. In caso di smarrimento del dispositivo, l'utente può recuperare i dati del portachiavi iCloud utilizzando il Recupero sicuro del portachiavi iCloud, i Contatti di recupero dell'account o una Chiave di recupero dell'account.

Gestione delle chiavi di crittografia



La sicurezza dei dati crittografati in CloudKit si basa sulla sicurezza delle chiavi di crittografia corrispondenti. Le chiavi di servizio CloudKit si dividono in due categorie: crittografate end-to-end e disponibili dopo l'autenticazione.

- **Chiavi di servizio crittografate end-to-end:** per i servizi iCloud crittografati end-to-end, le relative chiavi private del servizio CloudKit non vengono mai rese disponibili ai server Apple. Le coppie di chiavi di servizio, comprese le chiavi private, vengono create localmente sul dispositivo sicuro dell'utente e trasferite agli altri dispositivi dell'utente utilizzando la sicurezza del portachiavi iCloud. Sebbene i flussi di ripristino e sincronizzazione del portachiavi iCloud siano mediati dai server Apple, a questi server è impedito crittograficamente di accedere ai dati del portachiavi dell'utente. Nel caso in cui si perda l'accesso al portachiavi iCloud e a tutti i suoi meccanismi di recupero, i dati crittografati end-to-end in CloudKit andranno persi. Apple non può aiutare nel recupero di tali dati.
- **Chiavi di servizio disponibili dopo l'autenticazione:** per altri servizi, come Foto e iCloud Drive, le chiavi di servizio sono memorizzate nei moduli di sicurezza hardware di iCloud nei data center Apple e sono accessibili da alcuni servizi Apple. Quando un utente accede a iCloud su un nuovo dispositivo ed effettua l'autenticazione del proprio ID Apple, i server Apple possono accedere a queste chiavi senza ulteriori azioni o input da parte dell'utente. Ad esempio, dopo aver effettuato l'accesso a iCloud.com, l'utente può immediatamente visualizzare le proprie foto online. Queste chiavi di servizio sono *disponibili dopo l'autenticazione*.

Protezione avanzata dei dati per iCloud

La protezione avanzata dei dati per iCloud è un'impostazione facoltativa che offre il livello più elevato di sicurezza per i dati sul cloud di Apple. Quando un utente attiva la protezione avanzata dei dati, i suoi dispositivi affidabili mantengono l'accesso esclusivo alle chiavi di crittografia per la maggior parte dei dati iCloud, proteggendoli con la *crittografia end-to-end*. Per gli utenti che attivano la protezione avanzata dei dati, il numero totale di categorie di dati protetti con la crittografia end-to-end sale da 14 a 23 e include Backup, Foto e Note di iCloud e altro ancora.

Nota: questa funzionalità potrebbe non essere disponibile in tutti i paesi o in tutte le zone.

Il funzionamento della protezione avanzata dei dati è semplice: tutte le chiavi di servizio CloudKit generate sul dispositivo e successivamente caricate nei moduli di sicurezza hardware (HSM) iCloud *disponibili dopo l'autenticazione* nei data center Apple vengono eliminate da tali moduli HSM e vengono invece conservate interamente nel dominio di protezione del portachiavi iCloud dell'account. Vengono gestite come le chiavi di servizio *crittografate end-to-end* esistenti, il che significa che Apple non può più leggere tali chiavi né accedervi.

Inoltre, la protezione avanzata dei dati protegge automaticamente i campi CloudKit che gli sviluppatori di terze parti scelgono di contrassegnare come crittografati e tutte le risorse CloudKit.

Abilitare la protezione avanzata dei dati

Quando l'utente attiva la protezione avanzata dei dati, il dispositivo sicuro esegue due azioni: in primo luogo, comunica l'intenzione dell'utente di attivare la protezione avanzata dei dati agli altri dispositivi coinvolti nella crittografia end-to-end. Lo fa scrivendo un nuovo valore, firmato dalle chiavi dispositivo-locali, nei metadati del dispositivo del suo portachiavi iCloud. I server Apple non possono rimuovere o modificare questa attestazione mentre viene sincronizzata con gli altri dispositivi dell'utente.

In secondo luogo, il dispositivo avvia la rimozione delle chiavi di servizio *disponibili dopo l'autenticazione* dai data center Apple. Poiché queste chiavi sono protette dai moduli HSM di iCloud, l'eliminazione è immediata, permanente e irrevocabile. Dopo l'eliminazione delle chiavi, Apple non può più accedere ad *alcun* dato protetto dalle chiavi di servizio dell'utente. A questo punto, il dispositivo inizia un'operazione di rotazione asincrona delle chiavi, che crea una nuova chiave di servizio per ogni servizio la cui chiave era precedentemente disponibile ai server Apple. Se la rotazione delle chiavi non va a buon fine, a causa di un'interruzione della rete o di un altro errore, il dispositivo riprova la rotazione delle chiavi fino a quando questa non riesce.

Una volta che la rotazione delle chiavi di servizio è avvenuta correttamente, i nuovi dati scritti sul servizio non possono essere decrittografati con la chiave di servizio precedente. Sono protetti con la nuova chiave, che è controllata esclusivamente dai dispositivi sicuri dell'utente e non è mai stata utilizzabile o visibile per Apple.

Protezione avanzata dei dati e accesso web a iCloud.com

Quando un utente attiva per la prima volta la protezione avanzata dei dati, l'accesso web ai suoi dati su iCloud.com viene automaticamente disattivato. Ciò avviene perché i server web di iCloud non hanno più accesso alle chiavi necessarie per decifrare e visualizzare i dati dell'utente. L'utente può scegliere di attivare nuovamente l'accesso web e utilizzare la partecipazione del proprio dispositivo sicuro per accedere ai propri dati iCloud crittografati sul web.

Dopo aver attivato l'accesso web, l'utente deve autorizzare l'accesso web su uno dei suoi dispositivi sicuri ogni volta che visita iCloud.com. L'autorizzazione fornisce al dispositivo gli strumenti per l'accesso web. Per l'ora successiva, tale dispositivo accetta richieste da specifici server Apple per caricare chiavi di servizio singole, in particolare, unicamente quelle corrispondenti a un elenco di servizi normalmente accessibili su iCloud.com. In altri termini, anche dopo che l'utente ha autorizzato l'accesso web, una richiesta del server non è in grado di indurre il dispositivo dell'utente a caricare le chiavi di servizio per i dati che non sono destinati a essere visualizzati su iCloud.com (come i dati sanitari o le password salvate nel portachiavi iCloud). I server Apple richiedono solo le chiavi di servizio necessarie per decrittografare i dati specifici a cui l'utente chiede di accedere sul web. Ogni volta che viene caricata una chiave di servizio, questa viene crittografata utilizzando una chiave effimera legata alla sessione web autorizzata dall'utente e sul dispositivo dell'utente viene visualizzata una notifica che mostra il servizio iCloud i cui dati vengono temporaneamente resi disponibili ai server Apple.

Preservare le scelte dell'utente

Le impostazioni della protezione avanzata dei dati e di accesso web di iCloud.com possono essere modificate solo dall'utente. Questi valori vengono salvati nei metadati del dispositivo del portachiavi iCloud dell'utente e possono essere modificati solo da uno dei dispositivi sicuri dell'utente. I server Apple non possono modificare queste impostazioni per conto dell'utente, né possono ripristinarne una configurazione precedente.

Implicazioni per la sicurezza di condivisione e collaborazione

Nella maggior parte dei casi, quando gli utenti condividono contenuti per collaborare tra loro, ad esempio con Note condivise, Promemoria condivisi, cartelle condivise in iCloud Drive o Libreria foto condivisa di iCloud, e tutti gli utenti hanno attivato la protezione avanzata dei dati, i server Apple vengono utilizzati solo per stabilire la condivisione ma non hanno accesso alle chiavi di crittografia dei dati condivisi. Il contenuto rimane crittografato end-to-end e accessibile solo sui dispositivi affidabili dei partecipanti. Per ogni operazione di condivisione, Apple può memorizzare un titolo e una miniatura dimostrativa con una protezione dei dati standard per mostrare un'anteprima agli utenti che li ricevono.

Selezionando l'opzione "chiunque in possesso di un link" quando si attiva la collaborazione, il contenuto sarà disponibile ai server Apple con protezione dei dati standard, poiché i server devono essere in grado di fornire l'accesso a chiunque apra l'URL.

La collaborazione con iWork e la funzionalità "Album condivisi" di Foto non supportano la protezione avanzata dei dati. Quando gli utenti collaborano a un documento iWork o aprono un documento iWork da una cartella condivisa in iCloud Drive, le chiavi di crittografia del documento vengono caricate in modo sicuro sui server iWork nei data center Apple. Ciò avviene perché la collaborazione in tempo reale in iWork richiede una mediazione dal lato del server per coordinare le modifiche al documento tra i partecipanti. Le foto aggiunte agli Album condivisi vengono archiviate con una protezione dei dati standard, poiché la funzione consente di condividere pubblicamente gli album sul web.

Disabilitare la protezione avanzata dei dati

L'utente può disattivare la protezione avanzata dei dati in qualsiasi momento. Se decide di farlo:

1. In primo luogo, il dispositivo dell'utente registra la sua nuova scelta nei metadati di partecipazione del portachiavi iCloud e tale impostazione viene sincronizzata in modo sicuro su tutti i dispositivi.

2. Il dispositivo dell'utente carica in modo sicuro le chiavi di servizio per tutti i servizi *disponibili dopo l'autenticazione* nei moduli HSM di iCloud nei data center Apple. Questa operazione non include mai le chiavi per i servizi crittografati end-to-end secondo la protezione dei dati standard, come portachiavi iCloud e Salute.

Il dispositivo carica sia le chiavi di servizio originali, generate prima dell'attivazione della protezione avanzata dei dati, sia le nuove chiavi di servizio generate in seguito all'attivazione di tale funzionalità da parte dell'utente. In questo modo tutti i dati contenuti in tali servizi sono accessibili dopo l'autenticazione e l'account torna a utilizzare la protezione dei dati standard, così Apple può nuovamente aiutare l'utente a recuperare la maggior parte dei suoi dati in caso di perdita dell'accesso all'account.

Dati iCloud non coperti dalla protezione avanzata dei dati

A causa della necessità di collaborare con i sistemi globali di gestione di email, contatti e calendari, Mail, Contatti e Calendario iCloud non sono crittografati end-to-end.

iCloud memorizza alcuni dati senza la protezione delle chiavi di servizio CloudKit specifiche per l'utente, anche quando la protezione avanzata dei dati è attiva. Per risultare protetti, i campi dei record CloudKit devono essere contrassegnati esplicitamente come "crittografati" nello schema del contenitore, e la lettura e la scrittura di campi crittografati richiedono l'uso di API specifiche. Le date e gli orari di modifica di un file o di un oggetto vengono utilizzati per ordinare le informazioni di un utente e i checksum dei dati di file e foto vengono utilizzati per aiutare Apple nella deduplicazione e nell'ottimizzazione dell'archiviazione su iCloud e sui dispositivi dell'utente, il tutto senza avere accesso a tali file e foto. I dettagli su come viene utilizzata la crittografia per specifiche categorie di dati sono disponibili nell'articolo del supporto Apple Panoramica sulla sicurezza di iCloud.

Decisioni come l'uso di checksum per la deduplicazione dei dati, una nota tecnica detta *crittografia convergente*, facevano parte del progetto originale dei servizi iCloud al momento del lancio. Questi metadati sono sempre crittografati, ma le chiavi di crittografia sono archiviate da Apple con una protezione dei dati standard. Per continuare a rafforzare le protezioni di sicurezza per tutti gli utenti, Apple si impegna a garantire che un maggior numero di dati, tra cui questo tipo di metadati, siano crittografati end-to-end quando viene attivata la protezione avanzata dei dati.

Requisiti per la protezione avanzata dei dati

I requisiti per attivare la protezione avanzata dei dati per iCloud includono quanto segue:

- L'account dell'utente deve supportare la crittografia end-to-end. La crittografia end-to-end richiede l'autenticazione a due fattori per l'ID Apple dell'utente e un codice o una password impostata sui suoi dispositivi sicuri. Per ulteriori informazioni, consulta l'articolo del supporto Apple Autenticazione a due fattori per l'ID Apple.
- I dispositivi in cui l'utente ha effettuato l'accesso con il proprio ID Apple devono essere aggiornati a iOS 16.2, iPadOS 16.2, macOS 13.1, tvOS 16.2, watchOS 9.2, e all'ultima versione di iCloud per Windows. Questo requisito impedisce a una versione precedente di iOS, iPadOS, macOS, tvOS o watchOS di gestire erroneamente le chiavi di servizio appena create, ricaricandole sui moduli HSM *disponibili dopo l'autenticazione* nel tentativo errato di ripristinare lo stato dell'account.
- L'utente deve impostare almeno un metodo di recupero alternativo, ovvero uno o più contatti di recupero o una chiave di recupero, da utilizzare per recuperare i propri dati iCloud nel caso in cui perda l'accesso al proprio account.

Se i metodi di recupero non funzionano, ad esempio se le informazioni dei contatti di recupero non sono aggiornate o se l'utente le dimentica, Apple non sarà in grado di contribuire a recuperare i dati iCloud crittografati end-to-end dell'utente.

La protezione avanzata dei dati per iCloud può essere attivata solo per gli ID Apple. Gli ID Apple gestiti e gli account child (a seconda del paese o della zona) non sono supportati.

Sicurezza del backup di iCloud

iCloud esegue il backup delle informazioni (tra cui le impostazioni del dispositivo, i dati delle app, le foto e i video nel rullino fotografico e le conversazioni nell'app Messaggi) giornalmente tramite Wi-Fi. Il backup su iCloud avviene solo quando il dispositivo è bloccato, connesso a una fonte di alimentazione e ha accesso a internet tramite Wi-Fi. Tenendo a mente la crittografia utilizzata in iOS e iPadOS, il backup di iCloud è progettato per mantenere i dati al sicuro pur consentendo backup incrementali e operazioni di ripristino senza interventi da parte dell'utente. Di default, la chiave di servizio Backup iCloud è sottoposta a backup sicuro nei moduli di sicurezza hardware (HSM) di iCloud nei data center Apple e fa parte della categoria di dati disponibili dopo l'autenticazione. Per gli utenti che attivano la protezione avanzata dei dati per iCloud, la chiave di servizio Backup iCloud è protetta con crittografia end-to-end ed è disponibile solo per gli utenti sui loro dispositivi sicuri.

Quando i file vengono creati in classi di protezione dei dati non accessibili a dispositivo bloccato, le loro chiavi per file sono crittografate utilizzando le chiavi di classe provenienti dalla keybag Backup iCloud e archiviando i file su iCloud nel loro stato originale crittografato. Tutti i file sono crittografati durante il trasporto e, una volta archiviati, vengono crittografati con le chiavi basate sull'account, come descritto nella crittografia CloudKit.

La keybag Backup iCloud contiene chiavi asimmetriche (Curve25519) per le classi di protezione dati che non sono accessibili quando il dispositivo è bloccato. Il set di backup è archiviato nell'account iCloud dell'utente ed è formato da una copia dei file dell'utente e dalla keybag Backup iCloud. La keybag Backup iCloud è protetta da una chiave casuale, anch'essa archiviata insieme al set di backup. La password di iCloud dell'utente non viene utilizzata per la crittografia, così da non invalidare i backup presenti qualora venisse modificata.

La procedura di ripristino recupera i file copiati nel backup, la keybag Backup iCloud e la chiave della keybag dall'account iCloud dell'utente. La keybag Backup iCloud viene decrittografata utilizzando la relativa chiave, quindi si utilizzano le chiavi per file nella keybag per decrittografare i file nel set di backup, che vengono scritti come nuovi file nel file system e quindi nuovamente crittografati in base alla loro classe di protezione dei dati.

Tramite il backup di iCloud, viene effettuato il backup dei seguenti contenuti:

- Dati di musica, film, programmi TV, app e libri acquistati. Il backup di iCloud di un utente include le informazioni relative ai contenuti acquistati presenti sul dispositivo dell'utente, ma non i contenuti stessi. Quando l'utente effettua il ripristino da un backup di iCloud, i contenuti che aveva acquistato vengono scaricati automaticamente da iTunes Store, App Store, dall'app Apple TV o da Apple Books. Alcuni tipi di contenuto non vengono scaricati automaticamente in tutti i paesi o in tutte le zone e gli acquisti effettuati in precedenza potrebbero non essere disponibili se sono stati rimborsati o non sono più disponibili nel rispettivo store. La cronologia completa degli acquisti è associata all'ID Apple dell'utente.
- Foto e video sul dispositivo di un utente. Se un utente attiva "Foto di iCloud" in iOS 8.1, iPadOS 13.1, OS X 10.10.3 o versioni successive, le sue foto e i suoi video sono già archiviati su iCloud, quindi non saranno inclusi nel backup di iCloud di quell'utente.
- Contatti, eventi del calendario, promemoria e note.
- Impostazioni del dispositivo.
- Dati delle app.
- Schermata Home e organizzazione delle app.

- Configurazione di HomeKit.
- Dati della cartella clinica.
- Password dei memo vocali (se necessario, richiede la scheda SIM fisica che era in uso durante il backup).
- Messaggi, Apple Messages for Business, messaggi di testo (SMS) e MMS (se necessario, richiede la scheda SIM fisica che era in uso durante il backup).

Backup di iCloud viene utilizzato anche per eseguire il backup del portachiavi del dispositivo locale, crittografato con una chiave derivata dalla chiave crittografica root UID Secure Enclave del dispositivo. Questa chiave è unica per il dispositivo e sconosciuta a Apple. In questo modo il database può essere ripristinato solo sullo stesso dispositivo su cui è stato generato; questo significa che nessun altro, nemmeno Apple, potrà leggerlo. Per ulteriori informazioni, consulta Secure Enclave.

Messaggi su iCloud

Messaggi su iCloud mantiene l'intera cronologia dei messaggi dell'utente aggiornata e disponibile su tutti i dispositivi.

Con la protezione dei dati standard, Messaggi in iCloud è crittografato end-to-end quando il backup di iCloud è disattivato. Quando è attivo, il backup di iCloud include una copia della chiave di crittografia di Messaggi in iCloud, in modo che Apple possa aiutare l'utente a recuperare i suoi messaggi anche se ha perso l'accesso al portachiavi iCloud e ai suoi dispositivi affidabili. Se l'utente disattiva il backup di iCloud, sul suo dispositivo viene generata una nuova chiave per proteggere Messaggi in iCloud in futuro. La nuova chiave viene memorizzata solo nel portachiavi iCloud, accessibile solo all'utente sui propri dispositivi sicuri, e i nuovi dati scritti nel contenitore non possono essere decifrati con la vecchia chiave del contenitore.

Con la protezione avanzata dei dati, Messaggi in iCloud è sempre crittografato end-to-end. Quando viene attivato il backup di iCloud, tutto ciò che contiene è crittografato end-to-end, inclusa la chiave di crittografia di Messaggi in iCloud. La chiave di servizio Backup iCloud e la chiave del contenitore Messaggi in iCloud vengono entrambe rinnovate quando l'utente attiva la protezione avanzata dei dati. Per ulteriori informazioni, consulta l'articolo del supporto Apple Panoramica sulla sicurezza dei dati iCloud.

Sicurezza del relay privato iCloud

Il relay privato iCloud consente di proteggere l'utente principalmente quando naviga sul web con Safari, ma include anche tutte le richieste di risoluzione del nome DNS. Ciò consente di garantire che nessuno, nemmeno Apple, possa risalire all'attività di navigazione dell'utente dall'indirizzo IP. Questo risultato viene ottenuto grazie all'utilizzo di vari proxy: uno in ingresso, gestito da Apple, e uno in uscita, gestito da un provider di contenuti. Il relay privato iCloud è disponibile con iOS 15, iPadOS 15 o macOS 12.0.1 o versioni successive. Dopo che l'utente avrà effettuato l'accesso al proprio account iCloud+ con l'ID Apple, potrà attivare il relay privato iCloud in Impostazioni > iCloud o Impostazioni di Sistema > iCloud.

Per ulteriori informazioni, consulta la panoramica sul relay privato iCloud.

Sicurezza dei contatti per il recupero dell’account

È possibile aggiungere fino a cinque persone che, in caso di necessità, potrebbero aiutare l’utente a recuperare l’account iCloud e tutti i dati in esso archiviati, inclusi tutti i dati protetti da crittografia end-to-end, indipendentemente dal fatto che sia attiva o meno la protezione avanzata dei dati. Né Apple, né il contatto di recupero individualmente sono in possesso delle informazioni necessarie per decrittografare i dati iCloud dell’utente protetti con crittografia end-to-end.

Il contatto di recupero è concepito per tutelare la privacy degli utenti. I contatti di recupero scelti dall’utente non sono noti ad Apple. I server Apple vengono a conoscenza delle informazioni relative a un contatto di recupero solo in un momento successivo al tentativo di recupero, dopo che l’utente ha chiesto aiuto al contatto e che quest’ultimo ha iniziato a contribuire al recupero. Tali informazioni non vengono mantenute dopo il completamento del recupero.

Procedura di sicurezza per i contatti di recupero

Quando un utente configura un contatto di recupero per un account, viene generata una chiave associata a tale contatto. Questa chiave protegge l’accesso ai dati di iCloud dell’utente (compresi i dati protetti con crittografia end-to-end di CloudKit). Successivamente, viene generata una chiave AES a 256 bit casuale, utilizzata per crittografare la chiave del contatto di recupero e creare un pacchetto del contatto di recupero. Il pacchetto crittografato viene inviato al contatto di recupero perché venga conservato e la chiave AES casuale viene archiviata presso Apple. Né la chiave AES né il pacchetto sono in grado di fornire informazioni sulla chiave sottostante. Al momento del recupero, una volta che il dispositivo dell’utente avrà ottenuto correttamente sia il pacchetto dal contatto di recupero sia la chiave AES da Apple, i due elementi potranno essere combinarli per ricevere la chiave originale e accedere ai dati di iCloud dell’utente.

Per creare un contatto di recupero dell’account, il dispositivo dell’utente comunica con i server Apple per caricare la porzione di informazioni sulla chiave che saranno in possesso di Apple (la chiave AES menzionata sopra). Quindi stabilisce un contenitore CloudKit protetto con crittografia end-to-end con il contatto di recupero per condividere la parte di cui il contatto di recupero ha bisogno (il pacchetto del contatto di recupero crittografato utilizzando la chiave AES). Con il contatto di recupero viene condiviso anche un segreto utilizzato per l’autorizzazione, creato da Apple. Questo verrà usato per recuperare l’account e aiutare a inizializzarne la password. La comunicazione per invitare e accettare i contatti di recupero avviene attraverso un canale IDS reciprocamente autenticato. Il contatto di recupero memorizza automaticamente le informazioni ricevute nel proprio portachiavi iCloud. Apple non può accedere né al contenuto del contenitore CloudKit, né al portachiavi iCloud che memorizza queste informazioni. Quando viene eseguita la condivisione, i server Apple visualizzano solo un ID anonimo del contatto di recupero.

Successivamente, quando l’utente avrà la necessità di recuperare l’account e i dati iCloud, potrà chiedere aiuto al contatto di recupero selezionato. In quel caso, un codice di recupero verrà generato dal dispositivo del contatto di recupero, che lo fornirà all’utente tramite un accesso fuori banda, ossia di persona o tramite una chiamata telefonica. L’utente quindi inserirà il codice di recupero sul proprio dispositivo per stabilire una connessione sicura tra i dispositivi che utilizzano il protocollo SPAKE2+, i cui contenuti non sono accessibili da parte di Apple. Sebbene l’iterazione descritta sopra sia gestita dai server Apple, Apple non è in grado di avviare la procedura di recupero.

Una volta che la connessione sicura è stata stabilita e tutte le necessarie verifiche di sicurezza sono state completate, il dispositivo del contatto di recupero restituisce la propria parte di informazioni e l'autorizzazione segreta stabilita in precedenza all'utente che ha richiesto il recupero. L'utente presenta l'autorizzazione segreta a un server Apple, che gli consente di accedere alle informazioni sulla chiave di cui Apple dispone. Fornire l'autorizzazione segreta autorizza anche l'inizializzazione della password dell'account per ripristinare l'accesso.

Infine, il dispositivo dell'utente combina nuovamente le informazioni sulla chiave ricevute da Apple e dal contatto di recupero dell'account e le utilizza per decrittografare e recuperare i dati di iCloud.

Per evitare che un contatto di recupero avvii il ripristino senza il consenso dell'utente, sono state adottate delle misure di salvaguardia, tra cui un controllo dell'attività dell'account dell'utente. Se l'account è in uso, il recupero tramite un contatto di recupero richiede anche la conoscenza di un codice di accesso recente del dispositivo o del Codice di sicurezza iCloud.

Sicurezza del contatto erede

Se l'utente desidera che i propri dati siano accessibili ad alcuni beneficiari designati dopo la sua scomparsa, può configurare un contatto erede sul proprio account. Un contatto erede viene stabilito in modo simile a un contatto di recupero, tranne per il fatto che la chiave usata dal beneficiario non comprende le informazioni necessarie a decrittografare il portachiavi iCloud della persona deceduta. La struttura delle chiavi è la stessa di un contatto di recupero dell'account, ma in questo caso Apple archivia il pacchetto crittografato e il beneficiario conserva la chiave AES. In questo modo, la porzione ricevuta dal beneficiario è più breve e dunque più facile da stampare, se necessario; tuttavia, nessuna delle due parti da sola fornisce informazioni sulla chiave sottostante.

La chiave ricevuta dal beneficiario viene chiamata chiave di accesso nella documentazione disponibile agli utenti. La chiave di accesso viene salvata automaticamente sui dispositivi supportati, ma può essere anche stampata e conservata offline per essere usata all'occorrenza. Per ulteriori informazioni, consulta l'articolo del supporto Apple: Come aggiungere un contatto erede all'ID Apple.

Dopo la scomparsa dell'utente, i contatti erede accedono al sito di Apple per iniziare la procedura di accesso ai suoi dati. La procedura richiede un certificato di morte ed è parzialmente autorizzata tramite l'autorizzazione segreta menzionata nella sezione precedente. Dopo che tutti i controlli di sicurezza sono stati completati, Apple genera un nome utente e una password per il nuovo account e fornisce al contatto erede le informazioni sulla chiave necessarie.

Per inserire la chiave di accesso più facilmente quando viene richiesta, la chiave viene presentata sotto forma di codice alfanumerico al quale è associato un codice QR. Dopo l'inserimento della chiave, l'accesso ai dati iCloud dell'utente deceduto viene ripristinato. L'operazione può essere eseguita da un dispositivo oppure online. Per ulteriori informazioni, consulta l'articolo del supporto Apple Richiedere l'accesso a un account Apple in qualità di contatto erede.

Gestione di password e codici

Panoramica sulla sicurezza delle password

iOS, iPadOS e macOS semplificano l'autenticazione ad app di terze parti e siti web che utilizzano le password. Il modo migliore per gestire le password è non doverle utilizzare. La funzionalità "Accedi con Apple" consente agli utenti di accedere ad app e siti web di terze parti senza dover creare né gestire account o password aggiuntive. Inoltre l'accesso viene protetto dall'autenticazione a due fattori dell'ID Apple. Sui siti che non supportano "Accedi con Apple", la funzionalità per la creazione di password sicure automatiche consente ai dispositivi di un utente di creare, sincronizzare e inserire automaticamente password sicure uniche per siti e app. In iOS e iPadOS, le password vengono salvate in uno speciale portachiavi per l'inserimento automatico, controllato dall'utente e gestibile da Impostazioni > Password.

In macOS, le password salvate possono essere gestite nelle preferenze Password di Safari. Questo sistema di sincronizzazione può anche essere utilizzato per sincronizzare le password create manualmente dall'utente.

Sicurezza di "Accedi con Apple"

"Accedi con Apple" è un'alternativa rispettosa della privacy ad altri sistemi SSO. Fornisce la comodità e l'efficienza dell'accesso in un tocco offrendo al tempo stesso all'utente trasparenza e controllo maggiori sulle proprie informazioni personali.

"Accedi con Apple" consente agli utenti di configurare un account e di accedere alle app e ai siti web usando l'ID Apple di cui già dispongono, offrendo loro un maggior controllo sulle proprie informazioni personali. Durante la configurazione di un account, le app possono chiedere solo il nome e l'indirizzo email dell'utente, che avrà sempre la possibilità di scegliere: condividere l'indirizzo email personale con un'app oppure decidere di mantenerlo privato e utilizzare invece il nuovo servizio di relay di email di Apple. Questo servizio condivide un indirizzo email univoco e anonimo che inoltra i messaggi all'indirizzo personale dell'utente, in modo che l'utente possa comunque ricevere le comunicazioni utili dallo sviluppatore pur mantenendo un livello di privacy e controllo sulle proprie informazioni personali.

"Accedi con Apple" è una funzionalità ideata per la sicurezza. Tutti gli utenti di "Accedi con Apple" devono obbligatoriamente avere l'autenticazione a due fattori abilitata per il proprio ID Apple. L'autenticazione a due fattori contribuisce a garantire la tutela sia dell'ID Apple dell'utente che degli account creati nelle app. Inoltre, Apple ha sviluppato e integrato un segnale anti-frode rispettoso della privacy all'interno di "Accedi con Apple". Tale segnale garantisce agli sviluppatori che i nuovi utenti che acquisiscono sono persone reali e non bot o account gestiti da script.

Password sicure automatiche

Quando il portachiavi iCloud è abilitato, iOS, iPadOS e macOS creano password uniche, casuali e sicure quando gli utenti si iscrivono a un sito web in Safari o ne modificano la password. In iOS e iPadOS, la generazione di password sicure automatiche è disponibile anche per le app. Per non utilizzare le password sicure, gli utenti devono disattivare la relativa opzione. Le password generate vengono salvate nel portachiavi e mantenute aggiornate tra i dispositivi tramite il portachiavi iCloud, se abilitato.

Di default, le password generate da iOS e iPadOS contengono 20 caratteri: una cifra, un carattere maiuscolo, due trattini e 16 caratteri minuscoli. Si tratta di password sicure, contenenti 71 bit di entropia.

Le password vengono generate in base a dati euristici che determinano se il contesto è adatto alla creazione di una password. Se la determinazione euristica non riesce a identificare il contesto adatto alla creazione di una password, gli sviluppatori delle app possono impostare `UITextContentType.newPassword` sul campo di testo e gli sviluppatori web possono impostare `autocomplete= "new-password"` sugli elementi <input>.

Per aiutare a garantire che le password generate siano compatibili con i servizi pertinenti, le app e i siti web possono fornire delle regole. Gli sviluppatori forniscono tali regole tramite l'attributo `UITextInputPasswordRules` o `passwordrules` sugli elementi di input. I dispositivi generano quindi la password più sicura possibile che soddisfi tali requisiti.

Sicurezza dell'inserimento automatico delle password

La funzionalità di inserimento automatico delle password si occupa di digitare automaticamente dove necessario le credenziali archiviate nel portachiavi. Il portachiavi iCloud e l'inserimento automatico delle password forniscono le seguenti funzionalità:

- Inserimento credenziali in app e siti web.
- Generazione di password sicure.
- Salvataggio di password in app e siti web su Safari.
- Condivisione sicura delle password verso i contatti dell'utente.
- Invio di password a un'Apple TV vicina che richiede delle credenziali.

La creazione e il salvataggio delle password all'interno delle app, nonché l'invio delle password ad Apple TV sono funzionalità disponibili solo su iOS e iPadOS.

Inserimento automatico delle password nelle app

iOS e iPadOS consentono agli utenti di inserire i nomi utente e le password salvati negli appositi campi delle app, in modo simile al funzionamento dell'inserimento automatico delle password in Safari. In iOS e iPadOS, per avvalersi di tale funzionalità gli utenti devono toccare un'icona a forma di chiave visualizzata nella barra QuickType della tastiera. In macOS, per le app create con Mac Catalyst sotto i campi per le credenziali viene mostrato il menu a comparsa Password.

Quando un'app è fortemente associata a un sito web che usa lo stesso meccanismo di associazione app-sito web reso possibile dallo stesso file AASA (Apple-App-Site-Association), la barra QuickType di iOS e iPadOS e il menu a comparsa di macOS suggeriscono direttamente le credenziali dell'app, se salvate nel portachiavi per l'inserimento automatico delle password. Questo consente agli utenti di rivelare alle app le credenziali salvate tramite Safari, con le stesse proprietà di sicurezza, ma senza che le app debbano adottare un'API.

L'inserimento automatico delle password non rivela nessuna informazione sulle credenziali a un'app finché l'utente non ne consente il rilascio. Gli elenchi delle credenziali vengono creati o presentati al di fuori del processo dell'app.

Quando un'app e un sito web hanno una relazione attendibile e un utente invia le credenziali in un'app, iOS e iPadOS potrebbero chiedere all'utente di salvarle nel portachiavi per l'inserimento automatico delle password per un uso successivo.

Accesso delle app alle password salvate

Le app di iOS, iPadOS e macOS possono chiedere l'aiuto del portachiavi per l'inserimento automatico delle password per consentire l'accesso di un utente tramite `ASAuthorizationPasswordProvider` e `SecAddSharedWebCredential`. La funzionalità che fornisce le password e la relativa richiesta possono essere utilizzate insieme ad "Accedi con Apple", in modo che la stessa API venga chiamata per aiutare gli utenti ad accedere a un'app, a prescindere dal fatto che l'account dell'utente sia protetto da password o sia stato creato tramite "Accedi con Apple".

L'accesso alle password è concesso solo se lo sviluppatore dell'app e l'amministratore del sito web hanno dato la loro approvazione e se l'utente ha espresso il proprio consenso. Gli sviluppatori di app esprimono la loro intenzione di accedere alle password salvate in Safari includendo un'autorizzazione nell'app. L'autorizzazione elenca i nomi di dominio completi dei siti web associati e i siti web devono posizionare un file sul proprio server che elenchi gli identificatori unici delle app approvate da Apple.

Quando viene installata un'app con autorizzazione per i domini associati a com.apple.developer.associated-domains, iOS e iPadOS rivolgono una richiesta TLS a ogni sito web elencato, chiedendo uno dei seguenti file:

- apple-app-site-association
- .well-known/apple-app-site-association

Se l'elenco contenuto nel file comprende l'identificatore dell'app che viene installata, iOS e iPadOS contrassegnano come affidabile la relazione tra il sito web e l'app. Solo nelle relazioni di fiducia, le chiamate a queste due API si trasformano in una richiesta rivolta all'utente, che dovrà esprimere il proprio consenso prima che qualsiasi password venga rilasciata all'app, venga aggiornata o eliminata.

Consigli sulla sicurezza delle password

L'elenco di password per l'inserimento automatico in iOS, iPadOS e macOS indica quali, tra le password salvate dell'utente, saranno *riutilizzate* in altri siti web, sono considerate *deboli* e quali sono state compromesse da una fuga *di dati*.

Panoramica

L'uso della stessa password per più di un servizio potrebbe rendere i relativi account vulnerabili a un attacco teso alla sottrazione di credenziali. Se viene violato un servizio e le password vengono rese note, i fautori dell'attacco potrebbero provare le stesse credenziali su altri servizi al fine di compromettere altri account.

- Una password viene contrassegnata come *riutilizzata* se viene rilevato che è stata utilizzata più di una volta tra le password salvate su diversi domini.
- Le password sono contrassegnate come *deboli* se esiste la possibilità che vengano indovinate facilmente da un hacker. iOS, iPadOS e macOS rilevano dei pattern comuni utilizzati per creare delle password facili da ricordare, come parole trovate in un dizionario, sostituzione di caratteri con altri simili (come ad esempio "p4ssw0rd" invece di "password"), caratteri vicini su una tastiera (come "q12we34r" su una tastiera QWERTY) o sequenze ripetute (come "123123"). Tali pattern vengono spesso utilizzati per creare delle password che soddisfino i requisiti minimi per i servizi, ma sono anche comunemente utilizzati da hacker che cercano di scoprire una password tramite un attacco di forza bruta.

  Poiché molti servizi richiedono espressamente un codice PIN a quattro o sei cifre, i codici brevi sono valutati in base a regole diverse. I codici PIN sono considerati deboli se sono costituiti da codici PIN molto comuni, da sequenze numeriche crescenti o decrescenti come "1234" o "8765" oppure se seguono un pattern ripetuto, come ad esempio "123123" o "123321".
- Una password viene contrassegnata come *esposta* se la funzionalità di monitoraggio riesce a rilevare che è stata coinvolta in una fuga di dati. Per ulteriori informazioni, consulta Monitoraggio delle password.

Le password deboli, riutilizzate o coinvolte in fughe di dati vengono contrassegnate nell'elenco delle password (macOS) o vengono mostrate nell'interfaccia dedicata "Suggerimenti di sicurezza" (iOS e iPadOS). Se l'utente accede a un sito web in Safari usando una password salvata in precedenza che è molto debole o che è stata coinvolta in una fuga di dati, gli verrà mostrato un avviso con la raccomandazione di aggiornarla a una password sicura automatica.

Migliorare la sicurezza della procedura di autenticazione dell'account in iOS e iPadOS

Le app che implementano l'estensione per la modifica dell'autenticazione per gli account (nel framework dei servizi di autenticazione) possono fornire un rapido aggiornamento per gli account basati su password. In particolare, consentono il passaggio ad "Accedi con Apple" o l'uso di una password sicura automatica. Questo punto di estensione è disponibile in iOS e iPadOS.

Se un'app ha implementato il punto di estensione ed è installata sul dispositivo, agli utenti verranno mostrate delle opzioni di aggiornamento quando visualizzano i suggerimenti di sicurezza per le credenziali associate all'app nel gestore delle password del portachiavi iCloud in Impostazioni. Gli aggiornamenti vengono offerti anche quando gli utenti accedono all'app con credenziali a rischio. Le app hanno la capacità di impedire al sistema di mostrare agli utenti le opzioni di aggiornamento dopo avere effettuato l'accesso. Utilizzando la nuova API AuthenticationServices, le app possono anche richiamare le proprie estensioni ed eseguire gli aggiornamenti in modo autonomo, idealmente da una schermata per le impostazioni o per la gestione dell'account nell'app.

Le app possono scegliere di supportare l'aggiornamento alle password sicure, "Accedi con Apple" o entrambi. In un aggiornamento a una password sicura, il sistema ne genera una automaticamente per l'utente. Se necessario, l'app può fornire regole personalizzate da seguire per la generazione della nuova password. Quando un utente passa da un account con password all'uso di "Accedi con Apple", il sistema fornisce all'estensione delle nuove apposite credenziali da associare all'account. L'email associata all'ID Apple dell'utente non viene fornita insieme alle credenziali. Una volta effettuato correttamente l'aggiornamento ad "Accedi con Apple", il sistema elimina le credenziali della password precedentemente utilizzata dal portachiavi dell'utente, se vi erano state salvate.

Le estensioni per la modifica dell'autenticazione per gli account hanno la capacità di eseguire un'autenticazione utente aggiuntiva prima di eseguire un aggiornamento. Per gli aggiornamenti avviati all'interno del gestore delle password o dopo aver effettuato l'accesso a un'app, l'estensione fornisce il nome utente e la password per l'account da aggiornare. Per gli aggiornamenti in-app, viene fornito solo il nome utente. Se l'estensione necessita di un'ulteriore autenticazione utente, può richiedere di mostrare un'interfaccia personalizzata prima di procedere con l'aggiornamento. La possibilità di mostrare tale interfaccia è pensata per consentire all'utente di inserire un secondo fattore di autenticazione per autorizzare l'aggiornamento.

Monitoraggio delle password

La funzionalità di monitoraggio delle password confronta le password archiviate nel portachiavi per l'inserimento automatico dell'utente con un elenco costantemente aggiornato e curato di password che sono state segnalate come coinvolte in fughe di dati da diverse organizzazioni online. Se la funzionalità è attivata, il protocollo di monitoraggio confronta in modo continuo le password archiviate per l'inserimento automatico dell'utente con la lista curata.

Funzionamento del monitoraggio

Il dispositivo dell'utente esegue continuamente verifiche cicliche delle password, effettuando query a intervalli che non dipendono dalle password stesse o dagli schemi di utilizzo del gestore delle password. Ciò aiuta a garantire che gli stati delle verifiche rimangano aggiornati con la lista curata delle password coinvolte in fughe di dati attuale. Per aiutare a evitare di rivelare informazioni sul numero di password uniche di cui un utente dispone, le richieste vengono eseguite in gruppo e in parallelo. In ciascun controllo viene verificato in parallelo un numero fisso di password e se un utente dispone di meno password rispetto a questo numero, verranno generate e aggiunte delle password casuali per colmare la differenza.

Procedura di controllo delle password

La procedura di controllo delle password è composta da due fasi. Le password più comunemente coinvolte in fughe di dati sono incluse in un elenco locale sul dispositivo. Se la password compare in tale elenco, l'utente viene avvisato immediatamente senza alcuna interazione con l'esterno. Questo meccanismo è progettato per garantire che non vengano esposte informazioni sulle password dell'utente che sono a maggiore rischio a causa di una fuga di dati.

Se la password non compare nell'elenco di quelle più frequenti, viene confrontata con l'elenco delle password coinvolte meno frequentemente in fughe di dati.

Confronto delle password degli utenti con un elenco curato

La verifica di una password non presente nell'elenco locale prevede un'interazione con i server Apple. Per aiutare a garantire che le password non a rischio non vengano inviate ad Apple, viene messa in atto una forma di *intersezione crittografica di set privati* che confronta le password dell'utente con un grande insieme di password coinvolte in fughe di dati. Questo meccanismo è progettato per garantire che per le password meno a rischio di coinvolgimento in fughe di dati venga condivisa con Apple una quantità minima di informazioni. Per la password di un utente, tali informazioni sono limitate a un prefisso di 15 bit di un hash crittografico. La rimozione delle password più frequentemente a rischio da questo processo interattivo, utilizzando l'elenco locale delle password più comunemente esposte, riduce il delta della frequenza relativa delle password nei bucket del servizio web, rendendo difficile risalire alle password tramite operazioni di ricerca.

Il protocollo sottostante suddivide l'elenco curato delle password (che al momento della stesura di questo documento conteneva circa 1,5 miliardi di password) in 2^{15} diversi bucket. Il bucket a cui una password appartiene è determinato dai primi 15 bit del valore dell'hash SHA256 della password stessa. Inoltre, ogni password esposta, pw, viene associata a un punto della curva ellittica NIST P256: $P_{pw} = \alpha \cdot H_{SWU}(pw)$, dove α è una chiave casuale segreta conosciuta solo da Apple e H_{SWU} è una funzione oracolo casuale che associa le password a punti sulla curva in base al metodo Shallue-van de Woestijne-Ulas. Questa trasformazione è concepita per nascondere in maniera computazionale i valori delle password e per aiutare a evitare di rivelare nuove password esposte tramite la funzionalità di monitoraggio.

Per calcolare l'intersezione tra set privati, il dispositivo dell'utente determina il bucket a cui appartiene la password utilizzando λ, il prefisso di 15 bit di SHA256(upw), dove upw è una delle password dell'utente. Il dispositivo genera la propria costante casuale β e invia il punto $P_c = \beta \cdot H_{SWU}(upw)$ al server, insieme alla richiesta del bucket corrispondente a λ. In questo modo, β nasconde le informazioni sulla password dell'utente e limita a λ le informazioni esposta dalla password ad Apple. Infine, il server prende il punto inviato dal dispositivo dell'utente, calcola $\alpha P_c = \alpha\beta \cdot H_{SWU}(upw)$ e lo restituisce, insieme al corretto bucket di punti $B\lambda = \{ P_{pw} \mid \text{SHA256}(pw) \text{ inizia con il prefisso } \lambda\}$ al dispositivo.

Le informazioni restituite consentono al dispositivo di calcolare $B'_\lambda = \{\beta \cdot P_{pw} \mid P_{pw} \in B_\lambda\}$ e verificare che la password è stata esposta se $\alpha P_c \in B'_\lambda$.

Invio delle password ad altri utenti o dispositivi Apple

Apple invia le password in modo sicuro ad altri utenti di dispositivi Apple tramite AirDrop e su Apple TV.

Salvare le credenziali su un altro dispositivo tramite AirDrop

Quando iCloud è abilitato, gli utenti possono utilizzare AirDrop per inviare le credenziali salvate a un altro dispositivo. Le credenziali includono il nome utente e la password e il sito web per il quale sono stati salvati. L'invio delle credenziali con AirDrop funziona sempre in modalità "Solo contatti", a prescindere dalle impostazioni dell'utente. Sul dispositivo ricevente, dopo il consenso dell'utente, le credenziali vengono archiviate nel portachiavi per l'inserimento automatico delle password.

Inserimento credenziali nelle app su Apple TV

L'inserimento automatico delle password è disponibile per inserire le credenziali nelle app su Apple TV. Quando l'utente seleziona un campo di testo per nome utente o password in tvOS, Apple TV inizia a trasmettere una richiesta per l'inserimento automatico della password tramite BLE (Bluetooth Low Energy).

Qualsiasi iPhone o iPad nelle vicinanze mostrerà una richiesta che invita l'utente a condividere le credenziali con Apple TV. Ecco come viene stabilito il metodo di codifica:

- Se il dispositivo e Apple TV usano lo stesso account iCloud, la codifica tra i dispositivi avviene automaticamente.
- Se il dispositivo è collegato a un account iCloud diverso da quello usato da Apple TV, all'utente viene chiesto di stabilire una connessione codificata tramite l'uso di un codice PIN. Per ricevere questa richiesta, iPhone deve essere sbloccato e vicino al telecomando Siri Remote abbinato a Apple TV.

Una volta effettuata la connessione codificata tramite BLE, le credenziali vengono inviate a Apple TV e vengono automaticamente inserite nei campi di testo appropriati nell'app.

Estensioni per la fornitura di credenziali

In iOS, iPadOS e macOS, gli utenti possono indicare un'app di terze parti compatibile come fornitrice di credenziali per l'inserimento automatico delle password nelle impostazioni Password (iOS e iPadOS) o nelle impostazioni Estensioni in Impostazioni di Sistema (macOS 13 o versioni successive) o Preferenze di Sistema (macOS 12 o versioni precedenti). Questo meccanismo si basa sulle estensioni delle app. L'estensione fornitrice di credenziali *deve* prevedere una schermata per scegliere le credenziali. L'estensione *può facoltativamente* fornire dei metadati sulle credenziali salvate, in modo che possano essere offerte direttamente nella barra QuickType (iOS e iPadOS) o nei suggerimenti del completamento automatico (macOS). I metadati includono il sito web delle credenziali e il nome utente associato, ma non la password. iOS, iPadOS e macOS comunicano con l'estensione per ottenere la password quando l'utente sceglie di inserire una credenziale in un'app o in un sito con Safari. I metadati delle credenziali sono archiviati nel contenitore dell'app del fornitore di credenziali e vengono rimossi automaticamente quando un'app viene disinstallata.

Portachiavi iCloud

Panoramica sulla sicurezza del portachiavi iCloud

Il portachiavi iCloud consente agli utenti di sincronizzare in maniera sicura le proprie password e passkey tra iPhone, iPad e il Mac senza rivelare tali informazioni ad Apple. Oltre a un forte accento sulla privacy e la sicurezza, gli altri obiettivi relativi a design e architettura del portachiavi iCloud sono stati la semplicità d'uso e la possibilità di recuperare i portachiavi. Il portachiavi iCloud è composto da due servizi: sincronizzazione del portachiavi e recupero del portachiavi.

Il portachiavi iCloud e il suo meccanismo di recupero sono progettati in moto tale che le password e le passkey dell'utente rimangano protette anche nei seguenti casi:

- Se l'account iCloud dell'utente viene compromesso.
- Se iCloud viene compromesso da un attacco esterno o da un dipendente.
- Se una terza parte accede agli account utente.

Integrazione del gestore di password con il portachiavi iCloud

iOS, iPadOS e macOS possono generare automaticamente stringhe casuali crittograficamente sicure da utilizzare come password di account in Safari. iOS e iPadOS possono generare anche password sicure per le app. Le password generate vengono archiviate nel portachiavi e vengono sincronizzate sugli altri dispositivi. Gli elementi del portachiavi vengono trasferiti da un dispositivo all'altro attraverso i server Apple, ma sono codificati in modo che né Apple né altri dispositivi possano leggerne i contenuti.

Sincronizzazione sicura del portachiavi

Quando l'utente attiva per la prima volta il portachiavi iCloud su un account con autenticazione a due fattori, il dispositivo stabilisce una propria identità di sincronizzazione L'identità di sincronizzazione è composta da chiavi ellittiche asimmetriche (con la curva P-384), archiviate nel portachiavi del dispositivo. Ciascun dispositivo conserva un proprio elenco di identità di sincronizzazione degli altri dispositivi dell'utente e lo firma utilizzando una delle chiavi dell'identità. Questi elenchi vengono archiviati su CloudKit, consentendo ai dispositivi dell'utente di raggiungere un consenso su come sincronizzare in modo sicuro i dati del portachiavi tra di loro.

Per offrire compatibilità con dispositivi iCloud meno recenti, viene creata una cerchia di attendibilità simile e viene formata un'altra identità di sincronizzazione. La chiave pubblica dell'identità di sincronizzazione viene inserita nella cerchia, che viene firmata due volte: prima dalla chiave privata dell'identità, poi nuovamente con una chiave ellittica asimmetrica (con la curva P-256) derivata dalla password dell'account iCloud dell'utente. Nella cerchia vengono memorizzati anche i parametri (random salt e iterazioni) utilizzati per creare una chiave basata sulla password iCloud dell'utente.

Archiviazione su iCloud della cerchia di sincronizzazione

Per gli account protetti dall'autenticazione a due fattori, l'elenco di dispositivi attendibili di ciascun dispositivo viene archiviato su CloudKit. Non è possibile leggerli senza conoscere la password iCloud dell'utente né modificarli senza le chiavi private del dispositivo posseduto.

In modo analogo, la cerchia di sincronizzazione firmata viene salvata nell'area di archiviazione chiave-valore di iCloud dell'utente. Non è possibile leggerla senza conoscere la password iCloud dell'utente né modificarla in maniera valida senza la chiave privata dell'identità di sincronizzazione del membro della cerchia.

Modalità di aggiunta degli altri dispositivi dell'utente alla cerchia di sincronizzazione

Durante l'accesso ad iCloud, i nuovi dispositivi possono unirsi alla cerchia di sincronizzazione del portachiavi iCloud in uno dei due modi seguenti: abbinandosi a uno dei dispositivi esistenti nel portachiavi iCloud, dal quale verranno sponsorizzati, oppure utilizzando il recupero del portachiavi iCloud.

Durante il flusso di abbinamento, il dispositivo richiedente crea nuove identità di sincronizzazione, sia per la cerchia che per gli elenchi (per gli account con l'autenticazione a due fattori) di sincronizzazione e le presenta al dispositivo principale. Questo aggiunge la chiave pubblica del nuovo membro alla cerchia di sincronizzazione e la firma nuovamente utilizzando sia la sua identità di sincronizzazione che la chiave derivata dalla password iCloud dell'utente. La nuova cerchia di sincronizzazione viene inserita in iCloud e firmata in maniera simile dal nuovo membro. Negli account con l'autenticazione a due fattori, il dispositivo principale fornisce al dispositivo richiedente anche un *voucher* firmato con le proprie chiavi dell'identità, che mostrano che il dispositivo richiedente può essere ritenuto attendibile. Quindi aggiorna il proprio elenco individuale di identità di sincronizzazione attendibili in modo da includere il dispositivo richiedente.

Ora nella cerchia di sincronizzazione ci sono due membri e ciascuno dispone della chiave pubblica dell'altro. A questo punto iniziano a scambiarsi singoli elementi del portachiavi attraverso CloudKit o attraverso l'archivio chiave-valore di iCloud a seconda dei casi. Se entrambi i membri della cerchia devono aggiornare lo stesso elemento, è possibile scegliere sia l'uno che l'altro, ottenendo sempre un risultato coerente. Ogni elemento sincronizzato viene crittografato in maniera tale che possa essere decrittografato solo da un dispositivo che faccia parte della cerchia di attendibilità dell'utente; non può essere decrittografato da nessun altro dispositivo né da Apple.

Ogni volta che un nuovo dispositivo si aggiunge alla cerchia di sincronizzazione, il processo descritto sopra si ripete. Ad esempio, se si dovesse aggiungere un terzo dispositivo potrebbe essere abbinato con uno qualsiasi dei dispositivi esistenti. Man mano che vengono aggiunti nuovi membri, ognuno di essi si sincronizza con quello nuovo. Questo meccanismo è progettato per garantire che tutti i membri abbiano gli stessi elementi nel portachiavi.

Solo determinati elementi vengono sincronizzati

Alcuni elementi del portachiavi sono specifici di ciascun dispositivo, come le chiavi di iMessage, pertanto devono rimanere sul dispositivo. Per impedire trasferimenti di dati inattesi, ciascun elemento che verrà sincronizzato deve essere contrassegnato esplicitamente con l'attributo `kSecAttrSynchronizable`.

Apple imposta questo attributo per i dati utente di Safari (inclusi nomi utente, password e numeri di carte di credito) oltre che per le password Wi-Fi, le chiavi di crittografia di HomeKit e per gli altri elementi del portachiavi che supportano la crittografia end-to-end di iCloud.

Inoltre, di default, non vengono sincronizzati gli elementi del portachiavi aggiunti da app di terze parti. Quando aggiungono elementi al portachiavi, gli sviluppatori devono impostare l'attributo `kSecAttrSynchronizable`.

Recupero sicuro del portachiavi iCloud

Il portachiavi iCloud deposita i dati del portachiavi dell'utente presso Apple senza che Apple possa leggere le password e gli altri dati al suo interno Anche per chi ha un solo dispositivo, la funzionalità di recupero del portachiavi funge da rete di sicurezza in caso di perdita dei dati. Si tratta di un aspetto particolarmente importante quando si utilizza Safari per generare password o passkey sicure e casuali per gli account web, poiché tali password risiedono esclusivamente nel portachiavi.

Fattori fondamentali nel recupero del portachiavi sono l'autenticazione secondaria e un servizio di deposito sicuro, creato da Apple specificamente per questa funzionalità. Il portachiavi dell'utente viene codificato con una password sicura, inoltre il servizio di deposito ne fornisce una copia solo nel caso in cui sia rispettata una serie di condizioni molto precise.

Utilizzo dell'autenticazione secondaria

Esistono diversi modi di stabilire un codice forte:

- Se sull'account dell'utente è abilitata l'autenticazione a due fattori, viene utilizzato il codice del dispositivo per recuperare un portachiavi depositato.
- Se l'autenticazione a due fattori non è configurata, all'utente viene richiesto di creare un codice di sicurezza di iCloud a sei cifre. In alternativa, senza l'autenticazione a due fattori, l'utente può specificare un codice più lungo oppure lasciare al dispositivo il compito di creare un codice crittograficamente casuale da annotare e conservare in un luogo sicuro.

Processo di escrow del portachiavi

Una volta stabilito il codice, il portachiavi viene depositato presso Apple. Per prima cosa, il dispositivo iOS, iPadOS o macOS esporta una copia del portachiavi dell'utente, quindi lo codifica utilizzando le chiavi in una keybag asimmetrica e lo colloca nell'archivio chiave-valore dell'utente su iCloud. La keybag viene cifrata con il codice di sicurezza iCloud dell'utente e con la chiave pubblica del cluster HSM che archivia il record di deposito. Questo diventerà il *record di deposito iCloud* dell'utente. Per gli account con l'autenticazione a due fattori, il portachiavi viene archiviato anche in CloudKit e viene crittografato con chiavi intermedie che sono recuperabili solo con i contenuti del record di deposito iCloud, fornendo quindi lo stesso livello di protezione.

I contenuti del record di deposito consentono anche di recuperare il dispositivo affinché possa unirsi nuovamente al portachiavi iCloud, dimostrando a tutti i dispositivi esistenti che il processo di deposito è stato eseguito correttamente dal dispositivo che veniva recuperato, che può quindi essere autorizzato dal proprietario dell'account.

Nota: oltre a stabilire un codice di sicurezza, gli utenti devono anche registrare un numero di telefono per il proprio account iCloud. Ciò fornisce un secondo livello di autenticazione durante il recupero del portachiavi. L'utente riceve un messaggio SMS a cui è necessario rispondere per poter procedere con il recupero.

Sicurezza del servizio di deposito per il portachiavi iCloud

iCloud fornisce un'infrastruttura sicura per il deposito del portachiavi che aiuta a garantire che solo gli utenti e i dispositivi autorizzati possano effettuare un recupero. Dietro iCloud, vi sono i cluster HSM (moduli di sicurezza hardware) che proteggono i record depositati. Come descritto in precedenza, ciascuno dispone di una chiave utilizzata per codificare i record di propria competenza.

Per recuperare un portachiavi, l'utente deve autenticarsi con l'account e la password di iCloud e rispondere al messaggio SMS inviato al numero di telefono registrato. Fatto questo, l'utente deve inserire il proprio codice di sicurezza iCloud. Il cluster HSM verifica che l'utente conosca il proprio codice di sicurezza iCloud utilizzando il protocollo Secure Remote Password (SRP); il codice non viene inviato ad Apple. Ogni membro del cluster verifica in modo indipendente che l'utente non abbia superato il numero massimo di tentativi consentiti per recuperare il proprio record, come spiegato in seguito. Se la maggioranza concorda, il cluster decifra il record depositato e lo invia al dispositivo dell'utente.

A questo punto il dispositivo utilizza i dati depositati per decifrare le chiavi casuali usate per codificare il portachiavi dell'utente. Con queste chiavi, il portachiavi, recuperato da CloudKit e dall'archivio chiave-valore dell'utente su iCloud, viene decrittografato e ripristinato sul dispositivo. Il servizio di deposito consente soltanto 10 tentativi di autenticazione per recuperare il record depositato. Dopo una serie di tentativi non riusciti, il record viene bloccato e l'utente deve contattare il Supporto Apple per poter effettuare ulteriori tentativi. Dopo il decimo tentativo non riuscito, il cluster HSM distrugge il record depositato e il portachiavi è perduto per sempre. Si tratta di una protezione contro gli attacchi di forza bruta volti a recuperare il record: in questo modo, i dati sono tutelati anche a costo di sacrificare il portachiavi.

Queste politiche sono codificate nel firmware HSM. Le schede di accesso amministrativo che permettono di modificare il firmware sono state distrutte. Qualsiasi tentativo di alterare il firmware o di accedere alla chiave privata causa l'eliminazione della chiave privata da parte del cluster HSM. Se ciò dovesse verificarsi, il proprietario di ciascun portachiavi custodito dal cluster riceve un messaggio che lo informa che il record depositato è andato perduto; potrà quindi scegliere di registrarsi nuovamente.

Apple Pay

Panoramica sulla sicurezza di Apple Pay

Grazie ad Apple Pay, gli utenti possono utilizzare gli iPhone, iPad, Mac e Apple Watch supportati per effettuare i pagamenti in modo facile, sicuro e privato nei negozi, nelle app e sul web in Safari. Gli utenti possono anche aggiungere le carte dei mezzi pubblici, le tessere identificative studente e i pass di accesso compatibili con Apple Pay ad Apple Wallet. È un metodo intuitivo e facile da usare ed è sviluppato con un sistema di sicurezza integrato a livello di hardware e di software.

Apple Pay è inoltre progettato per proteggere le informazioni personali dell'utente. Apple Pay non raccoglie alcuna informazione sulle transazioni che possa essere ricollegata all'utente. Le transazioni di pagamento vengono effettuate tra l'utente, l'esercente e l'emittente della carta.

Sicurezza dei componenti di Apple Pay

Apple Pay utilizza diverse funzionalità hardware e software per consentire acquisti sicuri e affidabili.

Secure Element

Secure Element è un processore certificato e realizzato secondo i massimi standard del settore. Su di esso è in esecuzione Java Card, una piattaforma che soddisfa i requisiti dell'industria finanziaria per i pagamenti elettronici. Il circuito integrato Secure Element e la piattaforma Java Card sono certificati secondo il processo di verifica della sicurezza EMVCo. Quando tale verifica è completata correttamente, l'EMVCo rilascia certificati di circuito integrato e di piattaforma e unici.

Il circuito integrato Secure Element è stato certificato in base agli standard Common Criteria.

Controller NFC

Il controller NFC gestisce i protocolli Near Field Communication e instrada la comunicazione tra il processore per le applicazioni e Secure Element e tra Secure Element e il terminale POS.

Apple Wallet

L'app Apple Wallet è utilizzata per aggiungere e gestire le carte di credito, di debito e le carte dei negozi e per eseguire pagamenti con Apple Pay. In Apple Wallet gli utenti possono visualizzare le carte e informazioni aggiuntive fornite dall'emittente, come la politica sulla privacy dell'emittente, le transazioni recenti e molto altro ancora. Gli utenti possono anche aggiungere le carte a Apple Pay in:

- Impostazione Assistita e Impostazioni per iOS e iPadOS
- L'app Watch per Apple Watch
- "Wallet e Apple Pay" in Impostazioni di Sistema (macOS 13 o versioni successive) o in Preferenze di Sistema (macOS 12 o versioni precedenti) per i Mac con Touch ID

Inoltre Apple Wallet consente agli utenti di aggiungere e gestire carte dei mezzi pubblici, carte fedeltà, carte d'imbarco, biglietti, carte regalo, tessere identificative studente, pass di accesso e altro ancora.

Secure Enclave

Su iPhone, iPad, Apple Watch, sui Mac con Touch ID e sui Mac con il chip Apple che utilizzano la Magic Keyboard con Touch ID, Secure Enclave gestisce il processo di autenticazione e garantisce l'avanzamento delle transazioni di pagamento.

Su Apple Watch, il dispositivo deve essere sbloccato e l'utente deve premere due volte il tasto laterale. Il doppio clic viene rilevato e inoltrato direttamente a Secure Element o Secure Enclave, dove disponibile, senza passare dal processore per le applicazioni.

Server Apple Pay

I server Apple Pay gestiscono la configurazione e il provisioning delle carte di credito, carte di debito, carte dei mezzi pubblici, delle tessere identificative studente e dei pass di accesso in Apple Wallet. I server gestiscono anche i numeri di account del dispositivo archiviati in Secure Element. Comunicano sia con il dispositivo sia con i server delle rete di pagamento o con i server degli emittenti delle carte. I server Apple Pay sono inoltre responsabili di codificare nuovamente le credenziali di pagamento per le transazioni all'interno delle app o sul web.

In che modo Apple Pay protegge gli acquisti degli utenti

Secure Element

All'interno di Secure Element è presente un'apposita applet per la gestione di Apple Pay, che include anche applet certificate dalle reti di pagamento o dagli emittenti delle carte. I dati relativi alla carta di debito, di credito o prepagata vengono inviati codificati dalla rete di pagamento o dall'emittente della carta a queste applet utilizzando chiavi conosciute solo dalla rete di pagamento o dagli emittenti delle carte e dal dominio di sicurezza delle applet. Questi dati sono archiviati all'interno delle applet e protetti utilizzando le funzionalità di sicurezza di Secure Element. Durante una transazione, il terminale comunica direttamente con Secure Element attraverso il controller NFC (Near Field Communication) mediante un bus hardware dedicato.

Controller NFC

Come gateway di Secure Element, il controller NFC aiuta a garantire che tutti i pagamenti contactless siano eseguiti utilizzando un terminale POS che si trovi in prossimità del dispositivo. Solo le richieste di pagamento provenienti da un terminale entro il raggio di azione sono contrassegnate dal controller NFC come transazioni contactless.

Quando il proprietario della carta autorizza il pagamento della carta di credito, di debito o prepagata (comprese le carte dei negozi) usando Face ID, Touch ID o un codice, oppure premendo due volte il tasto laterale su Apple Watch dopo averlo sbloccato, le risposte contactless preparate dalle applet di pagamento all'interno di Secure Element sono dirette dal controller al campo NFC. Di conseguenza i dettagli dell'autorizzazione al pagamento per le transazioni contactless sono contenuti nel campo NFC locale e non sono mai esposti al processore per le applicazioni. I dettagli dell'autorizzazione per i pagamenti all'interno delle app o sul web vengono invece diretti al processore per le applicazioni, ma solo dopo la codifica eseguita da Secure Element sul server Apple Pay.

Carte di credito, di debito e prepagate

Panoramica sulla sicurezza dell'aggiunta delle carte

Quando un utente aggiunge ad Apple Wallet una carta di credito, di debito o prepagata (comprese le carte dei negozi), Apple invia i dati della carta, insieme a quelli relativi al dispositivo e all'account dell'utente, all'ente di emissione della carta o al fornitore di servizi autorizzato dall'ente di emissione della carta (normalmente la rete di pagamento), il tutto in modalità sicura. Attraverso queste informazioni, l'emittente (o il suo fornitore di servizi) decide se approvare o meno l'aggiunta della carta ad Apple Wallet. Nell'ambito del processo di provisioning della carta, Apple Pay utilizza tre chiamate lato server per inviare e ricevere comunicazioni con l'emittente o la rete di pagamento:

- Campi richiesti
- Verifica della carta
- Collega e inserisci

L'emittente o la rete di pagamento utilizzano queste chiamate per consentire all'emittente di verificare, approvare e aggiungere carte a Apple Wallet. Queste sessioni client-server utilizzano il protocollo TLS 1.2 per trasferire i dati.

I numeri completi delle carte non sono archiviati sul dispositivo o sui server Apple Pay. In Secure Element, viene invece creato, codificato e poi archiviato un numero identificativo del dispositivo unico Questo numero unico è codificato in modo che neanche Apple possa accedervi. Il numero identificativo del dispositivo è unico e diverso dai numeri della maggior parte delle carte di credito o di debito; l'emittente o la rete di pagamento possono impedirne l'utilizzo su una carta a banda magnetica, per telefono o sui siti web. Il numero identificativo del dispositivo in Secure Element non viene mai archiviato sui server di Apple Pay, non ne viene effettuato il backup su iCloud ed è isolato dai dispositivi iOS, iPadOS, watchOS e dai Mac dotati di chip Apple che utilizzano la Magic Keyboard con Touch ID.

Il provisioning in Apple Pay delle carte da utilizzare con Apple Watch avviene con l'app Watch su iPhone o tramite l'app per iPhone dell'emittente. Per poter inserire una carta per Apple Watch è necessario che l'orologio si trovi entro il raggio d'azione del Bluetooth. Le carte sono registrate specificamente per l'uso con Apple Watch e ciascuna ha un proprio numero identificativo del dispositivo, memorizzato nel Secure Element su Apple Watch.

In seguito all'aggiunta, le carte di credito, di debito o prepagate (comprese le carte dei negozi) vengono visualizzate in un elenco durante Impostazione Assistita sui dispositivi in cui è stato effettuato l'accesso allo stesso account iCloud. Tali carte restano nell'elenco finché risultano attive su almeno un dispositivo. Le carte vengono rimosse dall'elenco dopo che sono state rimosse da tutti i dispositivi da sette giorni. Per questa funzionalità è necessario che sia abilitata l'autenticazione a due fattori sull'account iCloud in questione.

Aggiungere carte di credito o di debito ad Apple Pay

Le carte di credito possono essere aggiunte manualmente ad Apple Pay nei dispositivi Apple.

Aggiungere manualmente carte di debito o di credito

Per facilitare il processo di provisioning, per l'aggiunta manuale delle carte, vengono utilizzati il nome, il numero della carta, la data di scadenza e il CVV. Da Impostazioni, Apple Wallet o dall'app Watch, gli utenti possono inserire manualmente le informazioni acquisendole con la fotocamera sul dispositivo. Quando la fotocamera acquisisce le informazioni della carta, Apple prova a inserire i dati nei campi del nome, numero della carta e data di scadenza. La foto non è mai salvata sul dispositivo né archiviata nella libreria fotografica. Una volta compilati tutti i campi, il processo di verifica della carta controlla tutti i campi tranne quello relativo al CVV. Questi dati vengono quindi codificati e inviati al server di Apple Pay.

Se il processo "Verifica carta" dà come risultato un ID di termini e condizioni, Apple scarica e mostra all'utente i termini e le condizioni dell'emittente della carta. Se l'utente accetta i termini e le condizioni dell'emittente, Apple invia al processo "Collega e inserisci" l'ID dei termini che sono stati accettati, insieme al CVV. Inoltre, nell'ambito del processo "Collega e inserisci", Apple condivide informazioni dal dispositivo con l'istituto o il circuito emittente. Queste includono dati su (a) l'attività dell'account iTunes e App Store (ad esempio, se l'utente ha una lunga cronologia di transazioni su iTunes), (b) informazioni sul dispositivo (ad esempio numero di telefono, nome e modello, nonché ogni eventuale dispositivo Apple abbinato necessario per configurare Apple Pay) e (c) la posizione approssimativa nel momento in cui è stata aggiunta la carta (se la localizzazione è attiva). Attraverso queste informazioni, l'emittente decide se approvare o meno l'aggiunta della carta ad Apple Pay.

Come risultato del processo "Collega e inserisci" si verificano due condizioni:

- Il dispositivo inizia a scaricare il biglietto di Apple Wallet che rappresenta la carta di debito o di credito.
- Il dispositivo inizia a vincolare la carta a Secure Element.

Il file del biglietto contiene gli URL per scaricare l'immagine della carta, i metadati della carta come ad esempio le informazioni di contatto, la relativa app dell'emittente e le funzionalità supportate. Contiene anche lo stato del biglietto, che indica ad esempio se la personalizzazione di Secure Element è stata completata, se la carta è attualmente sospesa dall'istituto emittente o se sono necessarie ulteriori informazioni prima che la carta possa essere utilizzata per effettuare pagamenti con Apple Pay.

Aggiungere carte di credito o di debito da un account iTunes Store

L'utente potrebbe dover inserire di nuovo la password del proprio ID Apple per utilizzare una carta di credito o di debito registrata in iTunes. Il numero della carta viene recuperato da iTunes, quindi ha inizio il processo di verifica. Se la carta è idonea per Apple Pay, il dispositivo scarica e visualizza i termini e le condizioni dell'emittente della carta, quindi invia il relativo ID e il codice di sicurezza della carta al processo "Collega e inserisci". Potrebbero essere effettuate ulteriori verifiche per le carte registrate con gli account iTunes.

Aggiungere carte di credito o di debito dall'app dell'emittente

Quando un'app è registrata per l'utilizzo con Apple Pay, vengono stabilite delle chiavi per l'app e per il server dell'emittente. Tali chiavi sono utilizzate per codificare le informazioni della carta che vengono inviate all'emittente. Questo meccanismo è progettato per impedire che le informazioni vengano lette dal dispositivo Apple. Il processo di provisioning è simile a quello utilizzato per aggiungere manualmente le carte, descritto precedentemente, con l'unica eccezione che al posto del CVV vengono impiegate delle password utilizzabili una sola volta.

Aggiungere carte di credito o di debito dal sito web dell'emittente

Alcuni istituti che emettono carte di credito offrono la possibilità di avviare la procedura per l'emissione di una carta per Apple Wallet direttamente dal loro sito web. In questo caso, l'utente avvia la procedura selezionando la carta che desidera ricevere sul sito web dell'emittente. Da qui l'utente viene reindirizzato a un'esperienza di accesso Apple (contenuta all'interno del dominio Apple), dove viene richiesto di accedere con il proprio ID Apple. Dopo aver effettuato l'accesso, l'utente sceglie uno o più dispositivi sui quali desidera utilizzare la carta. Questo passaggio è richiesto per confermare il risultato dell'emissione della carta su ciascun dispositivo di destinazione.

Aggiungere verifiche aggiuntive

L'emittente può decidere se una carta di credito o di debito richiede ulteriori verifiche. In base a quanto predisposto dall'emittente della carta, l'utente potrebbe avere la possibilità di scegliere fra varie opzioni di verifica aggiuntive, per esempio un messaggio di testo, un'email, una telefonata al servizio clienti o un'azione da eseguire in un'app di terze parti per completare la procedura. Per i messaggi di testo e le e-mail, l'utente avrà l'opzione di selezionare le informazioni di contatto fra i dati già in possesso dell'emittente. Riceverà quindi un codice che dovrà essere inserito nell'app Apple Wallet, in Impostazioni o nell'app Watch. Per il servizio clienti o per la verifica tramite app, l'emittente adotta il proprio processo di comunicazione.

Autorizzazione dei pagamenti con Apple Pay

Per i dispositivi che dispongono di Secure Enclave, i pagamenti saranno consentiti solo dopo che Secure Enclave li avrà autorizzati. Su iPhone, su iPad o su un Mac con Touch ID (o abbinato a una tastiera Magic Keyboard con Touch ID), ciò richiede la conferma che l'utente abbia eseguito l'autenticazione tramite biometria o con il codice o la password del dispositivo. L'autenticazione biometrica, se disponibile, è il metodo di default, ma il codice o la password possono essere usati in qualsiasi momento e vengono automaticamente offerti dopo tre tentativi non riusciti di riconoscimento dell'impronta digitale o (su iPhone e iPad) dopo due tentativi non riusciti di riconoscimento del volto. Dopo cinque tentativi non riusciti, viene richiesto il codice o la password. Il codice o la password sono richiesti anche quando l'autenticazione biometrica non è configurata oppure è attivata per Apple Pay. Per effettuare un pagamento su Apple Watch, il dispositivo dev'essere sbloccato con il codice e l'utente deve premere due volte il tasto laterale.

Utilizzare una chiave di abbinamento condivisa

Secure Enclave e Secure Element comunicano tramite un'interfaccia seriale, utilizzando una crittografia e un'autenticazione basate su AES e valori anti-replay crittografici per evitare attacchi di tipo replay. Sebbene i due componenti non siano collegati direttamente, comunicano in modo sicuro tramite una chiave di abbinamento condivisa fornita durante la produzione. Durante tale processo, Secure Enclave genera la chiave di abbinamento dalla propria chiave UID e dall'ID unico di Secure Element. Quindi trasferisce la chiave di abbinamento in modo sicuro su un modulo di sicurezza hardware (HSM) nella fabbrica. Questo modulo di sicurezza hardware infine inserisce la chiave di abbinamento in Secure Element.

Autorizzare una transazione sicura

Quando l'utente autorizza una transazione, che include un gesto fisico comunicato direttamente a Secure Enclave, quest'ultimo invia i dati firmati relativi al tipo di autenticazione e i dettagli sul tipo di transazione (contactless o all'interno di app) a Secure Element, legandoli a un valore Authorization Random (AR). Il valore AR è generato in Secure Enclave quando l'utente fornisce per la prima volta una carta di credito e resta in vigore finché la funzionalità Apple Pay è attiva, protetto dalla codifica e dal meccanismo anti-rollback di Secure Enclave. Viene trasmesso in maniera protetta a Secure Element facendo uso della chiave di abbinamento. Alla ricezione di un nuovo valore AR, Secure Element contrassegna ogni carta aggiunta in precedenza come annullata.

Utilizzare un crittogramma di pagamento per una sicurezza dinamica

Le transazioni di pagamento originate dalle applet di pagamento includono un crittogramma di pagamento e un numero identificativo del dispositivo. Tale crittogramma, un codice utilizzabile una sola volta, viene calcolato tramite un contatore di transazioni e una chiave. Il contatore di transazioni viene incrementato per ogni nuova transazione. La chiave viene fornita nell'applet di pagamento durante la personalizzazione ed è conosciuta dalla rete di pagamento e/o dall'emittente della carta. A seconda dello schema di pagamento, per il calcolo possono essere utilizzati anche altri dati, tra cui:

- Un numero non prevedibile per il terminale, per le transazioni NFC.
- Un valore anti-replay del server di Apple Pay, per le transazioni all'interno delle app.
- I risultati della verifica dell'utente, ad esempio le informazioni ottenute dal metodo di verifica del titolare della carta (CVM).

I codici di sicurezza vengono forniti al circuito di pagamento e all'emittente in modo da consentire a quest'ultimo la verifica di ogni transazione. La lunghezza dei codici può variare in base al tipo di transazione.

Pagare con le carte tramite Apple Pay

Apple Pay può essere usato per pagare gli acquisti nei negozi, all'interno delle app e sui siti web.

Pagare con le carte nei negozi

Se iPhone o Apple Watch sono accesi e rilevano un campo NFC, presentano all'utente la carta richiesta (se è attivata la selezione automatica per la carta) oppure la carta di default, che viene gestita in Impostazioni. L'utente può anche aprire Apple Wallet e scegliere una carta oppure, quando il dispositivo è bloccato:

- Può premere due volte il tasto laterale sui dispositivi con Face ID.
- Può premere due volte il tasto Home sui dispositivi con Touch ID.
- Può utilizzare le funzionalità di accessibilità che consentono di utilizzare Apple Pay dalla schermata di blocco.

Quindi, prima che le informazioni di pagamento vengano trasmesse, l'utente dovrà autenticarsi utilizzando Face ID, Touch ID o il proprio codice. Quando Apple Watch è sbloccato, premendo due volte il tasto laterale si attiva la carta di default per il pagamento. Senza l'autenticazione da parte dell'utente non viene inviata alcuna informazione di pagamento.

Una volta completata l'autenticazione, per elaborare il pagamento vengono utilizzati il numero identificativo del dispositivo e un codice di sicurezza dinamico specifico per la transazione. Né Apple né il dispositivo invieranno all'esercente i numeri completi della carta di credito o di debito. Apple potrebbe ricevere informazioni anonime, per esempio ora e posizione approssimative della transazione, che serviranno a migliorare Apple Pay e altri prodotti e servizi Apple.

Pagare con le carte all'interno delle app

Apple Pay può essere utilizzato anche per effettuare pagamenti nelle app per iOS iPadOS, macOS e watchOS. Quando gli utenti effettuano un pagamento all'interno delle app usando Apple Pay, Apple riceve le informazioni codificate sulla transazione, per instradarle allo sviluppatore o all'esercente. Prima che tali informazioni siano inviate allo sviluppatore o all'esercente, Apple codifica nuovamente la transazione con una chiave specifica dello sviluppatore. Apple Pay conserva informazioni anonime sulla transazione, come l'importo approssimativo. Tali informazioni non permettono di risalire all'utente e non includono mai l'oggetto dell'acquisto.

Quando un'app avvia una transazione di pagamento Apple Pay, i server di Apple Pay ricevono la transazione codificata dal dispositivo prima che questa arrivi all'esercente. I server di Apple Pay codificano nuovamente la transazione con una chiave specifica per l'esercente prima di trasmettergliela.

Quando un'app richiede un pagamento, richiama un'API per determinare se il dispositivo supporta Apple Pay e se l'utente ha carte di credito o di debito che possono essere utilizzate su un circuito di pagamento accettato dall'esercente. L'app richiede le informazioni necessarie per elaborare e completare la transazione, come ad esempio l'indirizzo di fatturazione e spedizione e i dati di contatto. Quindi l'app chiede a iOS, iPadOS, macOS o watchOS di mostrare la schermata di Apple Pay, che richiede informazioni per l'app e altre informazioni necessarie, come ad esempio la carta da utilizzare.

A questo punto vengono fornite all'app le informazioni relative a città, stato e CAP per calcolare le spese di spedizione finali. Il set completo di informazioni viene trasmesso all'app solo quando l'utente autorizza il pagamento con Face ID, Touch ID o con il codice del dispositivo. Una volta autorizzato il pagamento, le informazioni incluse nella schermata di Apple Pay vengono trasferite all'esercente.

Pagare con le carte nelle app clip

Un'app clip è la versione ridotta di un'app che consente agli utenti di svolgere attività rapidamente (come noleggiare una bicicletta o pagare il parcheggio) senza dover scaricare l'intera app. Se un'app clip supporta i pagamento, l'utente può utilizzare "Accedi con Apple", quindi effettuare un pagamento con Apple Pay. Quando il pagamento viene effettuato dall'interno dell'app clip, le misure a tutela della sicurezza e della privacy sono le stesse che vengono applicate al pagamento effettuato all'interno dell'app completa.

In che modo i pagamenti nelle app vengono autorizzati dagli utenti e verificati dagli esercenti

Gli utenti e gli esercenti garantiscono la sicurezza dei pagamenti nelle app trasferendo informazioni ai server Apple, a Secure Element, al dispositivo e all'API delle app stesse. Per iniziare, quando l'utente autorizza un pagamento in un'app, questa ottiene un valore anti-replay crittografico contattando i server di Apple Pay. I server inviano questo valore e altri dati sulla transazione a Secure Element per calcolare delle credenziali di pagamento, che vengono crittografate con una chiave di Apple. Quindi Secure Element restituisce le credenziali di pagamento ai server di Apple Pay, in modo tale che possano decrittografarlo, verificare il valore anti-replay confrontandolo con quello inviato originariamente dai server di Apple Pay e crittografarlo nuovamente con la chiave dell'esercente associata dell'ID esercente. I server Apple, dunque, restituiscono i dati del pagamento al dispositivo, che li consegna all'API dell'app, che infine li passa al sistema dell'esercente perché possano essere elaborati. L'esercente esegue la decrittografia delle credenziali di pagamento per verificare di essere il destinatario corretto della transazione.

Le API richiedono un'autorizzazione che specifichi gli ID esercente supportati. Un'app può inoltre includere dati aggiuntivi (come il numero di ordine o l'identità del cliente) da inviare a Secure Element per la firma, garantendo che la transazione non possa essere assegnata a un altro cliente. Questo aspetto è gestito dallo sviluppatore dell'app, che può specificare i dati della stringa applicationData per l'oggetto PKPaymentRequest. Un hash di questi dati viene incluso nelle informazioni codificate del pagamento. L'esercente sarà quindi responsabile di verificare che il proprio hash applicationData corrisponda a quanto contenuto nei dati del pagamento.

Pagare con le carte sui siti web

Apple Pay può essere utilizzato per effettuare pagamenti sui siti web su iPhone, iPad, Apple Watch e computer Mac con Touch ID. È anche possibile iniziare una transazione di Apple Pay sul Mac e completarla su un iPhone o Apple Watch che utilizza lo stesso account iCloud ed è abilitato a effettuare acquisti con Apple Pay.

Apple Pay sul web richiede a tutti i siti web che partecipano di registrarsi con Apple. Una volta che il dominio è registrato, la convalida del nome del dominio viene eseguita solo dopo che Apple ha emesso un certificato client TLS. Per potere essere compatibili con Apple Pay, i siti web devono offrire i propri contenuti via HTTPS. Per ogni transazione di pagamento, i siti web devono ottenere una sessione di vendita sicura e unica con un server di Apple tramite il certificato client TLS rilasciato da Apple. I dati della sessione di vendita sono firmati da Apple. Dopo che è stata verificata la firma di una sessione di vendita, il sito web potrebbe inviare una richiesta per sapere se l'utente ha un dispositivo compatibile con Apple Pay e se dispone di una carta di credito, debito o prepagata attivata su tale dispositivo. Non viene condiviso nessun altro dato. Se l'utente non desidera condividere queste informazioni, può disabilitare le richieste di Apple Pay nelle impostazioni relative alla privacy di Safari su iPhone, iPad e Mac.

Una volta convalidata la sessione di vendita, le misure di privacy e sicurezza sono le stesse che vengono adottate quando un utente effettua un pagamento dall'interno di un'app.

Se l'utente sta trasmettendo informazioni relative a un pagamento da un Mac a un iPhone o Apple Watch, Apple Pay utilizza il protocollo di Apple Identity Service (IDS) con codifica end-to-end per trasmettere le informazioni relative al pagamento dal Mac dell'utente al dispositivo. Il client IDS sul Mac utilizza le chiavi del dispositivo dell'utente per la crittografia, in modo che nessun altro dispositivo sia in grado di decrittografare tali informazioni e che le chiavi non siano disponibili per Apple. Il rilevamento del dispositivo per il passaggio da un Mac a un dispositivo iOS durante una transazione di Apple Pay contiene il tipo e l'identificatore unico delle carte di credito dell'utente, oltre alcuni metadati. Il numero di conto associato alla carta dell'utente specifico del dispositivo non viene condiviso e rimane archiviato in modo sicuro sull'iPhone o l'Apple Watch dell'utente. Apple trasferisce in modo sicuro tramite il portachiavi iCloud anche gli indirizzi di contatto, fatturazione e spedizione dell'utente usati di recente.

Una volta che l'utente ha autorizzato il pagamento tramite Face ID, Touch ID, un codice oppure premendo due volte il tasto laterale di Apple Watch, viene generato un token di pagamento codificato in modo univoco per ogni certificato di vendita del sito web, che viene trasmesso in modo sicuro da iPhone o Apple Watch al Mac dell'utente e viene quindi consegnato al sito web dell'esercente.

Il pagamento può essere richiesto e completato unicamente da dispositivi tra loro vicini. La vicinanza è determinata mediante segnali Bluetooth Low Energy (BLE).

Pagamenti automatici e token esercente

In iOS 16 o versioni successive, le app e i siti web che supportano Apple Pay possono sfruttare i token esercente di Apple Pay, che consentono di effettuare pagamenti sicuri su tutti i dispositivi dell'utente. La schermata di pagamento aggiornata di Apple Pay su iOS 16 offre anche un'esperienza ottimizzata per i pagamenti preautorizzati. I nuovi tipi di transazioni disponibili nell'API di Apple Pay consentono agli sviluppatori di app e siti web di perfezionare l'esperienza della pagina di pagamento per abbonamenti, bollette ricorrenti, rate e caricamento automatico del saldo delle carte.

I token esercente non sono vincolati a dispositivi specifici, permettendo così la continuità dei pagamenti ricorrenti, nel caso in cui l'utente rimuova una carta di pagamento dal dispositivo.

Pagamenti verso più esercenti

In iOS 16 o versioni successive, Apple Pay offre la possibilità di specificare importi di pagamento per più esercenti in un'unica schermata di pagamento su Apple Pay. In questo modo i clienti avranno la possibilità di effettuare più pagamenti contemporaneamente, ad esempio, se acquistano un pacchetto di viaggio che include un volo, un'auto a noleggio e un hotel e potranno inviare diversi pagamenti ai singoli esercenti.

Biglietti contactless in Apple Pay

Per trasmettere i dati di biglietti supportati ai terminali NFC compatibili, Apple utilizza il protocollo VAS (Value Added Services) di Apple. Il protocollo VAS può essere implementato sui terminali contactless o sulle app per iPhone e utilizza NFC per comunicare con i dispositivi Apple supportati. Funziona entro una breve distanza e può essere utilizzato per presentare biglietti contactless in modo indipendente o come parte di una transazione di Apple Pay.

Quando il dispositivo viene avvicinato al terminale NFC, quest'ultimo avvia la ricezione delle informazioni del biglietto inviando una richiesta di biglietto. Se un utente dispone di un biglietto con l'identificatore del fornitore del biglietto, gli viene richiesto di autorizzarne l'utilizzo tramite Face ID, Touch ID o il codice. Le informazioni del biglietto, la data e l'ora e una chiave casuale ECDH P-256 utilizzabile una sola volta vengono usate insieme alla chiave pubblica del fornitore del biglietto per generare una chiave di codifica per i dati del biglietto, che vengono poi inviati al terminale.

Nelle versioni da iOS 12.0.1 a iOS 13 compreso, gli utenti possono selezionare manualmente il biglietto prima di presentarlo al terminale NFC dell'esercente. In iOS 13.1 o versioni successive, i fornitori dei biglietti possono configurare manualmente i biglietti selezionati perché richiedano o meno l'autenticazione da parte dell'utente per poter essere utilizzati.

Disabilitare l’uso delle carte con Apple Pay

Le carte di credito, di debito e prepagate aggiunte a Secure Element possono essere utilizzate solo se Secure Element riceve un’autorizzazione che contiene la stessa chiave di abbinamento e lo stesso valore AR indicati in fase di aggiunta della carta. Alla ricezione di un nuovo valore AR, Secure Element contrassegna ogni carta aggiunta in precedenza come annullata. In questo modo il sistema operativo può comunicare a Secure Enclave di rendere le carte inutilizzabili contrassegnandone la copia del valore AR come non valida quando si verificano le seguenti condizioni:

Condizione	Dispositivo
Il codice è disattivato.	iPhone, iPad, Apple Watch
La password è disattivata.	Mac
L’utente esce da iCloud.	iPhone, iPad, Mac, Apple Watch
L’utente seleziona “Inizializza contenuto e impostazioni”.	iPhone, iPad, Mac, Apple Watch
Il dispositivo viene ripristinato dalla modalità di recupero.	iPhone, iPad, Mac, Apple Watch
Quando viene annullato l’abbinamento al dispositivo	Apple Watch

Sospendere, rimuovere e cancellare le carte

Gli utenti possono interrompere l’uso di Apple Pay su iPhone, iPad e Apple Watch attivando la modalità smarrito sul dispositivo con Dov’è. Inoltre, hanno la possibilità di rimuovere e cancellare le proprie carte da Apple Pay utilizzando Dov’è, iCloud.com o direttamente tramite Apple Wallet sui dispositivi. Su Apple Watch è possibile rimuovere le carte utilizzando le impostazioni di iCloud o l’app Watch su iPhone, oppure direttamente l’orologio. L’emittente o il relativo circuito sospenderà o rimuoverà l’abilitazione ai pagamenti con carte da Apple Pay anche se il dispositivo non è in linea e non è connesso a una rete Wi-Fi o cellulare. Gli utenti possono inoltre chiamare il proprio emittente per chiedere la sospensione o la rimozione delle carte da Apple Pay.

Quando un utente inizializza l’intero dispositivo (usando “Inizializza contenuto e impostazioni”, tramite Dov’è o ripristinandolo) iPhone, iPad, Apple Watch e il Mac faranno sì che Secure Element contrassegni tutte le carte come annullate. Le carte risulteranno così inutilizzabili con effetto immediato fino a quando non sarà possibile contattare i server di Apple Pay per cancellarle completamente da Secure Element. In modo indipendente, Secure Enclave contrassegna il valore AR come non valido al fine di impedire ulteriori autorizzazioni di pagamento per le carte precedentemente registrate. Quando è in linea, il dispositivo tenta di contattare i server Apple Pay per aiutare a garantire che tutte le carte in Secure Element vengano cancellate.

Sicurezza di Apple Card

Sui modelli supportati di iPhone e Mac, gli utenti possono richiedere un'Apple Card in totale sicurezza.

Richiedere Apple Card

In iOS 12.4 o versione successiva, macOS 10.14.6 o versione successiva e watchOS 5.3 o versione successiva, è possibile utilizzare Apple Card con Apple Pay per effettuare acquisti nei negozi, nelle app e sul web.

Per richiedere Apple Card, l'utente deve aver effettuato l'accesso al proprio account iCloud su un dispositivo iPhone o iPad compatibile con Apple Pay e deve aver configurato l'autenticazione a due fattori sull'account iCloud; in alternativa, può richiederla su apply.applecard.apple dopo aver effettuato l'accesso con il proprio ID Apple Quando la richiesta dell'utente viene approvata, Apple Card diventa disponibile in Apple Wallet o da Impostazioni > Wallet e Apple Pay su qualsiasi dispositivo idoneo su cui l'utente abbia effettuato l'accesso con il proprio ID Apple.

Quando l'utente richiede Apple Card, i dati relativi alla sua identità vengono verificati in modo sicuro dai provider di identità partner di Apple e vengono quindi condivisi con Goldman Sachs Bank USA al fine di valutare le informazioni relative a identità e credito dell'utente.

Le informazioni quali il numero di sicurezza sociale statunitense (Social Security Number) o l'immagine del documento identificativo fornite durante il processo di richiesta vengono trasmesse, codificate con la relativa chiave, ai provider di identità partner di Apple e/o a Goldman Sachs Bank USA. Apple non può decrittografare tali dati.

Le informazioni sul reddito fornite durante la richiesta e i dati del conto bancario utilizzati per i pagamenti delle bollette vengono trasmessi in modo sicuro a Goldman Sachs Bank USA, codificate con la relativa chiave. Le informazioni relative al conto bancario vengono salvate nel portachiavi. Apple non può decrittografare tali dati.

Quando aggiungi Apple Card ad Apple Wallet, le stesse informazioni utilizzate quando aggiungi una carta di credito o di debito potrebbero essere condivise con il partner di Apple, Goldman Sachs Bank USA, e con Apple Payments Inc. Tali informazioni vengono utilizzate unicamente per la risoluzione dei problemi, la protezione dalle frodi e a scopo normativo.

In iOS 14.6 o versioni successive, iPadOS 14.6 o versioni successive e watchOS 7.5 o versioni successive, la persona responsabile di una famiglia iCloud che possiede un'Apple Card può condividere la propria carta con i membri della famiglia su iCloud di età superiore ai 13 anni. Per accettare l'invito è richiesta l'autenticazione da parte degli utenti. Apple Wallet utilizza una chiave in Secure Enclave per elaborare una firma che collega la persona che possiede la carta e quella che ha ricevuto l'invito. La firma viene convalidata sui server di Apple.

La persona responsabile della famiglia ha la facoltà di imporre dei limiti alle transazioni degli altri partecipanti. Inoltre, le carte dei partecipanti possono anche essere bloccate per interrompere il loro utilizzo in qualsiasi momento tramite Apple Wallet. Quando un co-titolare o un partecipante di età superiore ai 18 anni accetta l'invito e richiede la carta, dovrà effettuare la procedura definita nella sezione relativa alla richiesta di Apple Card in Apple Wallet.

Utilizzo di Apple Card

È possibile ordinare una carta fisica da Apple Card in Apple Wallet. Una volta che l'utente ha ricevuto la carta fisica, questa viene attivata usando il tag NFC presente nella doppia busta della carta. Il tag è unico per ogni carta e non può essere utilizzato per attivare la carta di un altro utente. In alternativa, la carta può essere attivata manualmente nelle impostazioni di Apple Wallet. L'utente può inoltre scegliere di bloccare o sbloccare la carta fisica in qualsiasi momento da Apple Wallet.

Pagamenti con Apple Card e dettagli dei biglietti di Apple Wallet

I pagamenti addebitati sull'account Apple Card possono essere effettuati da un browser web o da Apple Wallet su iOS con Apple Cash e un conto bancario. Con Apple Cash e un conto bancario, i pagamenti delle bollette possono essere programmati come ricorrenti o come pagamenti unici per una data specifica. Quando un utente effettua un pagamento, viene eseguita una chiamata ai server di Apple Pay per ottenere un valore anti-replay crittografico, come per Apple Cash. Il valore anti-replay viene trasmesso a Secure Element insieme ai dettagli sulla configurazione del pagamento, così da elaborare una firma per il pagamento. La firma viene poi inviata ai server di Apple Pay. L'autenticazione, l'integrità e la correttezza del pagamento vengono verificate mediante la firma e il valore anti-replay dai server di Apple Pay e l'ordine viene trasmesso a Goldman Sachs Bank USA per l'elaborazione.

Il numero di Apple Card può essere recuperato utilizzando un certificato su Apple Wallet. Il server di Apple Pay convalida il certificato per confermare che la chiave è stata generata in Secure Enclave. Quindi utilizza la chiave per crittografare il numero dell'Apple Card prima di restituirlo ad Apple Wallet, in modo che soltanto l'iPhone da cui è stata richiesto il numero dell'Apple Card possa decrittografarlo. Dopo che la decrittografia è stata eseguita, il numero dell'Apple Card viene salvato nel portachiavi iCloud.

Per mostrare i dettagli del numero di Apple Card nel biglietto usando l'app Apple Wallet è necessario autenticarsi con Face ID, Touch ID o il codice. Tali dettagli possono essere sostituiti dall'utente nella sezione relativa alle informazioni sulla carta, disabilitando quelli precedenti.

Protezione avanzata dalle frodi

In iOS 15 o versioni successive e in iPadOS 15 o versioni successive, l'utente di Apple Card può abilitare la protezione avanzata dalle frodi in Apple Wallet. Quando questa funzionalità è abilitata, il codice di sicurezza della carta viene aggiornato una volta ogni determinato numero di giorni.

Sicurezza di Apple Cash

In iOS 11.2 o versione successiva, iPadOS 13.1 o versione successiva e watchOS 4.2 o versione successiva, Apple Cash può essere utilizzato su iPhone, iPad o Apple Watch per inviare, ricevere e richiedere denaro da altri utenti. Il denaro ricevuto da un utente viene aggiunto a un conto Apple Cash accessibile tramite Apple Wallet o da Impostazioni > Wallet e Apple Pay su qualsiasi dispositivo idoneo su cui l'utente abbia effettuato l'accesso con il proprio ID Apple.

In iOS 14, iPadOS 14 e watchOS 7, l'organizzatore di una famiglia su iCloud che ha effettuato la verifica della propria identità con Apple Cash può abilitare Apple Cash per i membri della famiglia di età inferiore ai 18 anni. Facoltativamente, l'organizzatore può limitare le capacità di invio di denaro di tali utenti ai soli membri della famiglia o solo ai contatti. Se un membro della famiglia di età inferiore ai 18 anni effettua un recupero dell'account dell'ID Apple, l'organizzatore della famiglia deve riattivare manualmente la carta Apple Cash per tale utente. Se il membro di età inferiore ai 18 anni non fa più parte della famiglia su iCloud, il suo saldo di Apple Cash viene trasferito automaticamente all'account dell'organizzatore.

Quando l'utente configura Apple Cash, è possibile che vengano condivise le stesse informazioni necessarie all'aggiunta di carte di credito o di debito con il nostro partner bancario Green Dot Bank e con Apple Payments Inc., una società sussidiaria interamente partecipata creata per proteggere la privacy archiviando ed elaborando le informazioni separatamente dal resto di Apple e senza che vengano divulgate al resto di Apple. Tali informazioni vengono utilizzate solo per la risoluzione di problemi, per proteggere dai tentativi di frode e a scopo normativo.

Utilizzo di Apple Cash in iMessage

Per utilizzare i pagamenti da persona a persona e Apple Cash, l'utente deve aver effettuato l'accesso al proprio account iCloud su un dispositivo compatibile con il servizio e deve aver configurato l'autenticazione a due fattori sull'account iCloud. Le richieste e i trasferimenti tra gli utenti vengono avviati all'interno dell'app Messaggi o chiedendo a Siri. Quando un utente tenta di inviare denaro, iMessage mostra la finestra di Apple Pay. Il saldo presente in Apple Cash viene sempre utilizzato per primo. Se necessario, i fondi aggiuntivi vengono prelevati da una seconda carta di credito o di debito che l'utente ha aggiunto ad Apple Wallet.

Utilizzare Apple Cash nei negozi, nelle app e sul web

La carta Apple Cash in Apple Wallet può essere utilizzata con Apple Pay per effettuare pagamenti nei negozi, nelle app e sul web. Il denaro presente sul conto di Apple Cash può anche essere trasferito su un conto bancario. Oltre a ricevere denaro da un altro utente, è anche possibile aggiungere denaro al conto di Apple Cash da una carta di debito o prepagata in Apple Wallet.

Una volta completata una transazione, Apple Payments Inc. ne archivia i dati, che può utilizzare per la risoluzione dei problemi, per proteggere dai tentativi di frode e a scopo normativo. Il resto di Apple non è a conoscenza del destinatario o del mittente del denaro né è a conoscenza dei luoghi in cui l'utente ha effettuato acquisti tramite la carta Apple Cash.

Quando l'utente invia denaro con Apple Pay, aggiunge denaro a un conto di Apple Cash o trasferisce denaro su un conto bancario, viene effettuata una chiamata ai server di Apple Pay per ottenere un valore anti-replay crittografico, simile al valore restituito per Apple Pay all'interno delle app. Il valore anti-replay viene trasmesso a Secure Element insieme ad altri dati sulla transazione, così da elaborare una firma per il pagamento. La firma viene poi inviata ai server di Apple Pay. L'autenticazione, l'integrità e la correttezza della transazione sono verificate dai server di Apple Pay tramite la firma del pagamento e il valore anti-replay. Quindi, viene avviato il trasferimento di denaro e l'utente riceve una notifica di transazione completata.

Se la transazione coinvolge:

- Una carta di debito per aggiungere denaro su Apple Cash
- La fornitura di denaro aggiuntivo se il saldo di Apple Cash è insufficiente

Viene prodotta e inviata ai server di Apple Pay anche una credenziale di pagamento codificata, simile a quella usata per Apple Pay all'interno delle app e sui siti web.

Se il saldo del conto di Apple Cash supera una certa cifra o se viene rilevata un'attività insolita, all'utente viene richiesto di verificare la propria identità. Le informazioni fornite per verificare l'identità dell'utente, come il codice fiscale o le risposte a determinate domande (ad esempio, confermare il nome della via in cui ha vissuto in precedenza) vengono trasmesse in maniera sicura al partner di Apple e codificate tramite la rispettiva chiave. Apple non può decrittografare tali dati. Prima di ottenere di nuovo l'accesso al saldo di Apple Cash, all'utente verrà chiesto di riverificare la propria identità se esegue un recupero dell'account ID Apple.

Sicurezza di Tap to Pay on iPhone

"Tap to Pay on iPhone", disponibile in iOS 15.4 o versioni successive, consente agli esercenti di accettare Apple Pay e altri pagamenti contactless utilizzando iPhone e un'app partner abilitata per iOS. Grazie a questo servizio, gli utenti in possesso di un iPhone abilitato possono accettare in tutta sicurezza pagamenti contactless e pass Apple Pay abilitati NFC. Con "Tap to Pay on iPhone", gli esercenti non hanno bisogno di hardware aggiuntivo per accettare i pagamenti contactless.

"Tap to Pay on iPhone" è inoltre progettato per proteggere le informazioni personali dell'utente che esegue il pagamento. Il servizio non raccoglie alcuna informazione sulle transazioni che possa essere ricollegata all'utente che effettua il pagamento. Le informazioni relative alla carta di pagamento, come il numero della carta di credito o di debito (PAN), non sono visibili dal dispositivo dell'esercente e sono protette da Secure Element. Tali informazioni sono note soltanto al fornitore di servizi di pagamento dell'esercente, all'utente che effettua il pagamento e all'emittente della carta. Inoltre, il servizio "Tap to Pay on iPhone" non memorizza il nome del pagante, il suo indirizzo o i suoi numeri di telefono.

"Tap to Pay on iPhone" è stato verificato esternamente da un laboratorio di sicurezza accreditato e il suo uso è stato approvato per tutte le reti di pagamento accettate nei territori in cui è disponibile.

Sicurezza dei componenti dei pagamenti contactless

- *Secure Element:* Secure Element ospita i kernel di pagamento che leggono e garantiscono la sicurezza dei dati della carta di pagamento contactless.
- *Controller NFC:* il controller NFC gestisce i protocolli Near Field Communication e instrada la comunicazione tra il processore per le applicazioni e Secure Element e tra Secure Element e la carta di pagamento contactless.
- *Server di "Tap to Pay on iPhone":* i server di "Tap to Pay on iPhone" gestiscono la configurazione e la fornitura dei kernel di pagamento nel dispositivo. Inoltre, monitorano la sicurezza dei dispositivi abilitati per "Tap to Pay on iPhone", compatibilmente allo standard Contactless Payments on COTS (CPoC) del Payment Card Industry Security Standards Council (PCI SSC), conformi anche allo standard DSS del PCI.

In che modo le carte di credito, di debito e prepagate vengono lette dal servizio "Tap to Pay on iPhone"

Come viene fornita la sicurezza di "Tap to Pay"

In seguito al primo utilizzo di "Tap to Pay on iPhone" tramite un'app con i necessari privilegi, il server di "Tap to Pay on iPhone" determina se il dispositivo soddisfa i criteri di idoneità previsti come il modello, la versione di iOS e la presenza di un codice di accesso. Al termine di questa verifica, l'applet per l'accettazione del pagamento viene scaricata dal server di "Tap to Pay on iPhone" e installata su Secure Element, insieme alla configurazione del relativo kernel di pagamento. L'operazione viene eseguita in modo sicuro tra i server di "Tap to Pay on iPhone" e Secure Element. Secure Element convalida l'integrità e l'autenticità di questi dati prima dell'installazione.

In che modo “Tap to Pay” legge le carte in sicurezza

Quando un’app utilizzata per “Tap to Pay on iPhone” richiede la lettura di una carta dal framework ProximityReader, viene visualizzato un pannello, controllato da iOS, che invita l’utente a presentare la carta di pagamento. Nessuna app è in grado di leggere i sensori che potrebbero rivelare, anche in modo parziale, i dati della carta sensibili, nell’arco di tempo in cui la schermata per presentare la carta è attiva. iOS avvia il lettore delle carte di pagamento, quindi richiede i kernel di pagamento in Secure Element per avviare la lettura della carta.

A questo punto, Secure Element assume il controllo del controller NFC in modalità di lettura, grazie alla quale i dati della carta vengono scambiati tra la carta di pagamento e Secure Element tramite il controller NFC. In questa modalità, le carte di pagamento possono essere di sola lettura.

Dopo che l’applet di completamento del pagamento ha terminato la lettura della carta su Secure Element, i dati della carta vengono crittografati e firmati. I dati della carta di pagamento rimangono crittografati e autenticati fino a quando raggiungono il fornitore dei servizi di pagamento. Il fornitore dei servizi di pagamento utilizzato dall’app per richiedere la lettura della carta è l’unico che può decrittografare i dati della carta. Lo può fare richiedendo la chiave di decrittografia dei dati della carta di pagamento dal server di “Tap to Pay on iPhone”. Dopo aver verificato l’integrità e l’autenticità dei dati e dopo aver appurato che la lettura della carta è stata eseguita entro 60 secondi dalla richiesta della chiave di decrittografia per i dati della carta di pagamento, il server di “Tap to Pay on iPhone” fornisce le chiavi di decrittografia al fornitore dei servizi di pagamento.

Grazie a questa procedura, i dati della carta possono essere decrittografati soltanto dal fornitore dei servizi di pagamento che elabora la transazione per conto dell’esercente.

Utilizzare l’inserimento del PIN per autorizzare le transazioni

L’inserimento del PIN, disponibile in iOS 16.0 o versioni successive, consente alla persona che paga di inserire il proprio PIN sul dispositivo dell’esercente per autorizzare la transazione. La visualizzazione della schermata di inserimento del PIN può essere attivata immediatamente dopo l’avvicinamento del dispositivo, in base alle informazioni scambiate con la carta di pagamento. In alternativa, il provider di servizi di pagamento può attivare la visualizzazione della schermata del PIN fornendo un token firmato, valido per una sola transazione.

Il meccanismo di inserimento del PIN è stato verificato esternamente da un laboratorio di sicurezza accreditato e il suo uso è stato approvato per tutte le reti di pagamento accettate nei territori in cui è disponibile. Mentre la schermata di inserimento del PIN è attiva, non è possibile acquisire screenshot o duplicare lo schermo e nessuna app può leggere informazioni da alcun sensore che potrebbe rivelare una qualsiasi parte del PIN.

Le cifre del PIN inserite vengono registrate in modo sicuro da Secure Element. Utilizzando tali cifre, Secure Element crea un blocco del PIN crittografato che soddisfa gli standard del settore dei pagamenti. Apple trasmette in modo sicuro il blocco del PIN crittografato dal proprio back-end, che soddisfa lo standard PCI per i PIN, al fornitore dei servizi di pagamento per l’elaborazione successiva.

Il valore del PIN:

- Non è mai reso disponibile all’esercente sul suo dispositivo.
- Non viene mai decrittografato da Apple in nessun momento.
- Non viene mai archiviato da Apple.

Utilizzo di Apple Wallet

Accesso tramite Apple Wallet

In Apple Wallet sugli iPhone e gli Apple Watch che supportano la funzionalità, gli utenti possono salvare vari tipi di chiavi. Quando l'utente arriva davanti a una porta, la chiave corretta può persino venire presentata automaticamente (se l'opzione "Modalità rapida" è supportata per quella chiave e se è attiva), consentendogli di accedere con un semplice tap, grazie alla tecnologia NFC (Near Field Communication).

Facilità di utilizzo per l'utente

Modalità rapida

Quando una chiave viene aggiunta ad Apple Wallet, la modalità rapida viene attivata di default. Le chiavi in modalità rapida interagiscono con i terminali compatibili senza richiedere l'autenticazione tramite Face ID, Touch ID o codice o senza dover premere due volte il tasto laterale di Apple Watch. Per disattivare questa funzionalità, gli utenti possono disattivare la modalità rapida, toccando il pulsante Altro sul lato anteriore della carta che rappresenta la chiave in Apple Wallet. Per attivare nuovamente la modalità rapida, gli utenti devono autenticarsi tramite Face ID o Touch ID o inserendo un codice.

Condivisione delle chiavi

In iOS 16 o versioni successive, è possibile condividere alcuni tipi di chiave.

Gli utenti avranno così la possibilità di condividere l'accesso a una chiave, ad esempio della propria casa o dell'auto; le funzionalità a protezione della sicurezza e della privacy verranno applicate dall'iPhone della persona che possiede la chiave all'iPhone della persona che riceve la condivisione della chiave. È possibile condividere le chiavi toccando l'icona di condivisione della chiave in Apple Wallet, tramite i metodi mostrati nel pannello di condivisione. Le persone proprietarie delle chiavi possono anche scegliere il livello di accesso e un periodo di tempo di validità per ogni chiave condivisa; hanno inoltre la possibilità di vedere tutte le chiavi che hanno condiviso e di revocarne l'accesso, anche nel caso in cui una chiave venga condivisa con un altro utente dalla persona con cui era stata condivisa inizialmente.

L'invito alla condivisione delle chiavi viene archiviato in forma anonima e protetto da un server dedicato all'interno di una casella di posta, crittografata con chiave di crittografia AES 128 o 256. La chiave di crittografia non viene mai condivisa con il server né con persone diverse da quella con cui si intende condividerla. Soltanto il destinatario della chiave può decrittografare l'invito. In seguito alla creazione della casella postale, l'iPhone del proprietario genera un claim del dispositivo legato esclusivamente a quella casella postale dal server. Quando l'iPhone del destinatario della chiave accede per la prima volta alla casella postale, presenta il claim del dispositivo corrispondente al destinatario della chiave. Solo gli iPhone del proprietario e del destinatario della chiave che presentano un claim del dispositivo valido possono accedere alla casella postale. A ciascun claim di iPhone corrisponde in valore UUID univoco, in conformità alle specifiche RFC4122.

Come misura di sicurezza aggiuntiva, il proprietario della chiave può configurare un codice di attivazione a 6 cifre generato casualmente, che verrà richiesto sull'iPhone del destinatario. Il numero di tentativi di inserimento del codice viene implementato e convalidato dal proprietario della chiave o dal server partner. Il codice di attivazione deve essere comunicato dal proprietario della chiave al destinatario, che lo inserirà quando il proprietario della chiave o il server partner gliene richiederanno la convalida.

Dopo che l'invito sarà stato sbloccato dal destinatario, l'iPhone ricevente lo cancellerà immediatamente dal server. Anche la casella di posta che contiene l'invito alla condivisione della chiavi ha una durata limitata, che viene impostata durante la sua creazione e implementata dal server. Tutti gli inviti scaduti vengono eliminati automaticamente dal server.

A seconda del produttore originale, le chiavi possono essere condivise anche con dispositivi non Apple, tuttavia il metodo di protezione della condivisione delle chiavi potrebbe essere diverso da quello di Apple.

Privacy e sicurezza

Le chiavi di accesso in Apple Wallet sfruttano a pieno le funzionalità a tutela della privacy e della sicurezza integrate in iPhone e Apple Watch. L'orario o il luogo in cui una persona utilizza le proprie chiavi in Apple Wallet non vengono mai condivisi con Apple né archiviati sui server Apple e le credenziali sono salvate in modo sicuro all'interno di Secure Element nei dispositivi supportati. Secure Element ospita applet progettate appositamente per gestire e archiviare in modo sicuro le chiavi, garantendo che non possano essere estratte o sottratte in alcun modo.

Prima di fornire le chiavi, è necessario che l'utente abbia effettuato l'accesso all'account iCloud da un iPhone compatibile e abbia attivato l'autenticazione a due fattori per quell'account. L'unica eccezione è la tessera identificativa studente che non richiede che l'autenticazione a due fattori sia attivata.

Quando la procedura di provisioning viene avviata dall'utente, vengono effettuati dei passaggi simili a quelli del provisioning delle carte di credito e di debito, come illustrato nella sezione dedicata al collegamento e al provisioning Durante una transazione, il lettore comunica con Secure Element attraverso il controller NFC (Near Field Communication) mediante il canale sicuro che è stato stabilito.

Il numero di dispositivi, inclusi iPhone e Apple Watch, per i quali viene fornita una chiave è definito e controllato da ciascun partner e può variare da un partner all'altro. In questo modo, ciascun partner ha pieno controllo sul numero di chiavi di emesse per ciascun dispositivo per soddisfare al meglio le proprie esigenze specifiche. A questo scopo, Apple fornisce ai partner identificativi per tipo di dispositivo e dispositivo anonimizzati. Per ragioni di privacy e sicurezza, gli identificativi sono diversi per ciascun partner.

I partner ricevono, inoltre, identificativi utente, anonimizzati e univoci per ciascuno, che consentono loro di collegare in modo sicuro la chiave all'account iCloud dell'utente durante il provisioning iniziale. In questo modo, le chiavi sono protette e non possono essere fornite a un utente diverso, nel caso in cui un account creato con il partner venisse compromesso, ad esempio, nel contesto di un attacco all'account.

Le chiavi possono essere disabilitate o rimosse:

- Inizializzando il dispositivo da remoto con Dov'è.
- Abilitando la modalità smarrito con Dov'è.
- Ricevendo un comando di cancellazione dei dati in remoto tramite una soluzione MDM.
- Rimuovendo tutte le carte dalla pagina dell'account ID Apple.
- Rimuovendo tutte le carte da iCloud.com.
- Rimuovendo tutte le carte da Apple Wallet.
- Rimuovendo la carta dall'app dell'emittente.

In iOS 15.4 o versioni successive, quando un utente preme due volte il tasto laterale su un iPhone con Face ID o preme due volte il tasto Home su un iPhone con Touch ID, i dettagli dei pass e delle chiavi di accesso non vengono mostrati fino a quando non viene eseguita l'autenticazione sul dispositivo. Prima che informazioni specifiche relative ai pass, come ad esempio i dettagli di una prenotazione in un albergo, salvate in Apple Wallet vengano visualizzate, è richiesta l'autenticazione tramite Face ID, Touch ID o il codice.

Tipi di chiavi di accesso

Apple Wallet offre diversi tipi di accesso, ad esempio, a strutture di ospitalità, alle aziende tramite i badge, oppure tramite le tessere identificative studente, le chiavi di casa e dell'auto.

Strutture di ospitalità

Salvare le chiavi delle stanze di albergo in Apple Wallet consente di offrire dell'utente un'esperienza contactless semplificata dal check-in al check-out, garantendo, al contempo, ulteriori vantaggi di sicurezza e privacy per gli ospiti, rispetto alle tradizionali tessere di plastica fornite dagli hotel. Nelle strutture che supportano la funzionalità, gli ospiti possono aprire la porta della propria stanza d'albergo con un semplice tap grazie alle chiavi salvate in Apple Wallet sugli iPhone e gli Apple Watch (Series 4 o modelli successivi) compatibili.

Le funzionalità supportate in Apple Wallet sono concepite specificamente per semplificare l'esperienza del cliente e ridurre eventuali disagi:

- Provisioning prima dell'arrivo direttamente dall'app dell'hotel, per consentire al cliente di aggiungere un pass ad Apple Wallet prima del soggiorno.
- Riquadri per i pass dell'albergo, per avviare le procedure di check-in e di assegnazione delle camera da Apple Wallet.
- Aggiornamento delle chiavi dopo il provisioning, per supportare eventuali prolungamenti o modifiche dei soggiorni in corso.
- Supporto di chiavi per più stanze corrispondenti a un unico pass in Apple Wallet.
- Archiviazione automatica delle chiavi scadute in Apple Wallet.

Pass Disney MagicMobile

È possibile aggiungere un pass Disney MagicMobile ad Apple Wallet su iPhone o Apple Watch per entrare nei parchi a tema Disney. I pass MagicMobile possono essere utilizzati come biglietto di accesso ai parchi ma anche presso tutti gli altri lettori che li supportano all'interno dei parchi.

Per poter aggiungere un pass Disney MagicMobile, è necessario aver abilitato l'autenticazione a due fattori sul proprio account iCloud e aver acquistato biglietti o prenotato presso uno dei parchi a tema aderenti con un account My Disney Experience valido. Dall'app My Disney Experience su iPhone, l'utente può selezionare uno o più pass da aggiungere ad Apple Wallet. Se l'utente ha abbinato un Apple Watch, i pass selezionati saranno aggiunti automaticamente sia all'iPhone che all'Apple Watch abbinato. La modalità rapida viene attivata automaticamente per i pass aggiunti sia su iPhone che su Apple Watch. Per facilità d'uso, quando la modalità rapida è attiva, viene attivata per tutti i pass MagicMobile salvati sul dispositivo.

È possibile aggiungere più pass a un unico dispositivo in modo che gli utenti possano gestire i pass di tutte le persone che partecipano alla visita. In alternativa, gli utenti possono utilizzare anche l'app My Disney Experience per condividere i pass con altri utenti, che potranno aggiungere i pass condivisi in Apple Wallet nei propri dispositivi.

Badge aziendali

In Apple Wallet su iPhone e Apple Watch è possibile aggiungere i badge aziendali presso i partner che supportano la funzionalità, per consentire ai dipendenti di tutto il mondo di accedere al luogo di lavoro in modalità contactless. Per aggiungere un badge, è necessario che i dipendenti abbiano abilitato l'autenticazione a più fattori per l'account utilizzato per accedere all'app fornita dal datore di lavoro.

L'aggiunta del badge aziendale sfrutta a pieno le funzionalità di accesso offerte da Apple, consentendo agli utenti di:

- Aggiungere automaticamente il badge di un dipendente all'Apple Watch abbinato mediante il provisioning push che non richiede l'installazione di un'app partner.
- Accedere facilmente ai servizi dell'ufficio utilizzando la modalità rapida.
- Accedere al posto di lavoro anche quando la batteria di iPhone è scarica.

Tessere identificative studente

In iOS 12 o versioni successive, gli studenti, i docenti e il personale degli istituti d'istruzione partecipanti possono aggiungere la propria tessera identificativa ad Apple Wallet sui modelli di iPhone e Apple Watch supportati per accedere alle strutture e pagare presso le attività che accettano tale tessera.

Gli utenti aggiungono la tessera identificativa studente all'app Apple Wallet attraverso un'app fornita dall'emittente della stessa o dall'istituto partecipante. Il procedimento tecnico impiegato è lo stesso descritto precedentemente in Aggiungere carte di credito o di debito dall'app dell'emittente. Inoltre, le app dell'emittente devono supportare l'autenticazione a due fattori sugli account che controllano l'accesso alle tessere identificative studente. È possibile configurare una carta simultaneamente su iPhone e su un Apple Watch abbinato.

Abitazioni con più famiglie

Coloro che vivono e lavorano presso strutture partner che supportano questa funzionalità, possono utilizzare le proprie chiavi di casa in Apple Wallet per accedere all'edificio, all'appartamento e alle aree comuni. Le chiavi di casa possono essere fornite dall'app del partner. Per i partner che supportano la fornitura semplificata delle chiavi, la società di gestione della proprietà può inviare agli inquilini un link per avviare la procedura di emissione delle chiavi tramite il servizio di messaggistica che preferiscono (ad esempio, email o SMS). In questo modo, gli inquilini dovranno solo fare clic sul link che hanno ricevuto per ottenere le chiavi. Anche le app clip offrono un'esperienza sicura e semplificata, consentendo agli inquilini di ottenere le chiavi senza dover installare l'app dei partner. Per ulteriori informazioni, consulta l'articolo del supporto Apple Utilizzare le app clip su iPhone.

La chiave di casa per più famiglie può essere utilizzata anche in modalità rapida ed essere condivisa in modo sicuro con persone amiche e familiari. Per ulteriori informazioni, consulta Condivisione delle chiavi.

Chiavi di casa

È possibile utilizzare le chiavi di casa da Apple Wallet con le serrature delle porte abilitate NFC, semplicemente avvicinando iPhone o Apple Watch. Per ulteriori informazioni su come configurare e utilizzare le chiavi di casa, consulta l'articolo del supporto Apple: Sbloccare la porta con una chiave di casa su iPhone.

Quando un utente configura le chiavi di casa, tutti coloro che vivono nella stessa abitazione le ricevono automaticamente. Per gestire gli inviti e i membri, il proprietario può utilizzare l'app Casa, ad esempio, per condividere le chiavi con altre persone o rimuovere uno dei membri da un'abitazione condivisa. Quando un utente accetta l'invito a unirsi a un'abitazione provvista di chiavi di casa, viene avviata la procedura di provisioning delle chiavi in Apple Wallet sul suo dispositivo. Se un utente sceglie di abbandonare un'abitazione o se il proprietario revoca il suo accesso, di conseguenza anche le sue chiavi di casa verranno rimosse da Apple Wallet.

Chiavi dell'automobile

In Apple Wallet, le chiavi dell'automobile sono disponibili in maniera nativa sugli iPhone compatibili e sugli Apple Watch abbinati. Vengono presentate come biglietti (creati da Apple per conto del produttore del veicolo) in Apple Wallet e supportano il ciclo di vita completo delle carte di Apple Pay (modalità smarrito di iCloud, cancellazione remota, eliminazione locale e cancellazione di tutti i contenuti e di tutte le impostazioni). Così come per le carte di Apple Pay standard, le chiavi delle automobili condivise possono essere eliminate dall'iPhone e dall'Apple Watch del proprietario e dall'interfaccia del veicolo.

Le chiavi possono essere utilizzate, ad esempio, per sbloccare e bloccare il veicolo, aprire o chiudere il bagagliaio, attivare o disattivare l'allarme, avviare il motore oppure per attivare la modalità di guida. La transazione standard offre autenticazione reciproca ed è obbligatoria per l'avvio del motore. Le transazioni di sblocco e blocco possono utilizzare la transazione rapida, quando richiesta per motivi di prestazioni.

Le chiavi vengono create tramite la connessione (o abbinamento) di iPhone con un veicolo supportato di proprietà dell'utente. Tutte le chiavi sono create all'interno di Secure Element tramite una generazione basata su curva ellittica (NIST P-256) che avviene sul dispositivo (ECC-OBKG) e le chiavi private non lasciano mai Secure Element. La comunicazione tra i dispositivi e il veicolo utilizza la funzionalità NFC o una combinazione di Bluetooth® LE e banda ultralarga. La gestione delle chiavi utilizza un'API di comunicazione tra Apple e il server del produttore del veicolo con autenticazione reciproca tramite TLS. Dopo che una chiave è stata abbinata a un iPhone, anche qualsiasi Apple Watch abbinato a tale iPhone potrà riceverla. Quando una chiave viene eliminata dal veicolo o dal dispositivo, non può essere ripristinata. Le chiavi su dispositivi smarriti o rubati possono essere sospese e riattivate, ma l'attivazione su un nuovo dispositivo richiede un nuovo abbinamento o una nuova condivisione.

Le chiavi dell'auto possono essere utilizzate anche in modalità rapida ed essere condivise in modo sicuro con persone amiche e familiari. Per ulteriori informazioni, consulta Condivisione delle chiavi. Per ulteriori informazioni sulla sicurezza e sulla privacy delle chiavi dell'automobile digitali, consultaSicurezza delle chiavi dell'automobile in iOS.

Chiavi del monopattino

In iOS 17 o versioni successive e in alcuni paesi o zone in cui operano partner supportati, gli utenti possono ottenere una chiave del monopattino dall'app del partner direttamente su Apple Wallet su un iPhone e un Apple Watch supportati, per svolgere le seguenti operazioni:

- Toccare per bloccare o sbloccare il monopattino.
- Toccare per bloccare o sbloccare il bauletto del monopattino (se disponibile).

In Secure Element, un'applet dedicata gestisce le credenziali crittografiche associate alle chiavi del monopattino e consente di eseguire transazioni sicure con il monopattino.

Sul retro della tessera sono disponibili informazioni aggiuntive sul monopattino, come le ultime quattro cifre del numero identificativo del veicolo e il numero di targa. Alcuni dati potrebbero essere considerati confidenziali e potrebbero essere visibili solo dopo aver effettuato l'accesso tramite autenticazione biometrica o inserimento del codice del dispositivo.

Le chiavi del monopattino possono essere utilizzate anche in modalità rapida ed essere condivise in modo sicuro con persone amiche e familiari. Per ulteriori informazioni, consulta Condivisione delle chiavi.

Sicurezza delle chiavi dell'automobile in iOS

Gli sviluppatori sono in grado di supportare l'accesso sicuro senza chiavi fisiche a un veicolo tramite un iPhone compatibile e l'Apple Watch abbinato.

Abbinamento da parte del proprietario

Il proprietario deve dare prova del possesso del veicolo (il metodo varia a seconda del produttore) e può avviare il processo di abbinamento nell'app del produttore, tramite un link ricevuto via email dal produttore o dall'interfaccia del veicolo. In tutti i casi, il proprietario deve presentare ad iPhone una password di abbinamento unica e confidenziale, che viene usata per generare un canale di abbinamento sicuro tramite il protocollo SPAKE2+ con la curva NIST P-256. Quando si utilizza l'app o il link via email, la password viene trasferita automaticamente ad iPhone, mentre deve essere inserita manualmente quando l'abbinamento viene avviato dal veicolo.

Condivisione delle chiavi

L'iPhone abbinato del proprietario può condividere le chiavi con gli iPhone (e con gli Apple Watch abbinati) di amici e familiari idonei inviando un invito specifico per ciascun dispositivo tramite iMessage e il servizio IDS. Tutti i comandi di condivisione vengono scambiati utilizzando la funzionalità IDS con codifica end-to-end. L'iPhone abbinato del proprietario impedisce che il canale IDS cambi durante il processo di condivisione, al fine di evitare che l'invito venga inoltrato.

Una volta accettato l'invito, l'iPhone dell'altra persona crea una chiave digitale e invia la catena di certificati per la creazione della chiave all'iPhone abbinato del proprietario, per verificare che sia stata creata da un dispositivo Apple autentico. L'iPhone abbinato del proprietario firma la chiave pubblica ECC dell'iPhone dell'altra persona e invia la firma a tale dispositivo. La firma nel dispositivo del proprietario richiede l'autenticazione da parte dell'utente (Face ID, Touch ID o inserimento del codice) e l'intenzione dell'utente, come descritto in Utilizzi di Face ID e Touch ID. L'autorizzazione viene richiesta durante l'invio dell'invito ed è archiviata in Secure Element, pronta per essere usata quando il dispositivo dell'altra persona invia la richiesta di firma. I permessi per le chiavi vengono forniti al veicolo online tramite il server OEM del veicolo oppure durante il primo utilizzo delle chiavi condivise.

Eliminazione delle chiavi

Una chiave può essere eliminata dal dispositivo di chi l'ha ricevuta utilizzando il dispositivo del proprietario o l'interfaccia del veicolo. L'eliminazione dall'iPhone di chi l'ha ricevuta ha effetto immediato, anche se la chiave è in uso. Quindi, prima dell'eliminazione viene mostrato un avviso. Potrebbe essere possibile eliminare le chiavi dal veicolo in qualsiasi momento oppure soltanto quando è online.

In entrambi i casi, l'eliminazione viene comunicata a un server del produttore, che conserva un inventario delle chiavi emesse per ogni veicolo a scopi assicurativi.

Il proprietario può richiedere un'eliminazione della propria chiave. La richiesta viene prima inviata al produttore, per la rimozione dal veicolo. Le condizioni per la rimozione della chiave dal veicolo sono definite dal produttore. Solo quando la chiave è rimossa dal veicolo, il server del produttore invierà una richiesta di annullamento remota al dispositivo di chi ha ricevuto la chiave.

Quando una chiave è annullata su un dispositivo, l'applet che gestisce le chiavi digitali crea un attestato di annullamento con firma crittografica, che viene usato dal produttore come prova dell'eliminazione e per rimuovere la chiave dal proprio inventario.

Transazioni standard NFC

Per i veicoli che utilizzano una chiave NFC, viene aperto un canale sicuro tra il lettore e iPhone, generando coppie di chiavi effimere sul lato lettore e sul lato iPhone. Utilizzando un metodo di accordo tra le chiavi, è possibile derivare un segreto condiviso su entrambi i lati, da utilizzare per generare una chiave simmetrica condivisa, tramite il protocollo Diffie-Hellman, una funzione di derivazione delle chiavi e firme dalla chiave a lungo termine stabilita durante l'abbinamento.

La chiave pubblica effimera generata sul lato veicolo è firmata con la chiave privata a lungo termine del lettore, il che risulta nell'autenticazione del lettore da parte di iPhone. Dal punto di vista di iPhone, questo protocollo è progettato per impedire a un malintenzionato che intercetti la comunicazione di ricevere dati privati.

Infine, iPhone utilizza il canale sicuro stabilito per codificare l'identificativo della propria chiave pubblica, insieme alla firma calcolata dalla richiesta derivata dai dati del lettore e alcuni altri dati specifici per l'app. Questo controllo della firma di iPhone da parte del lettore consente a quest'ultimo di autenticare il dispositivo.

Transazioni rapide

iPhone genera un crittogramma basato su un segreto precedentemente condiviso durante una transazione standard. Il crittogramma consente al veicolo di eseguire rapidamente l'autenticazione del dispositivo in situazioni in cui sono necessarie alte prestazioni. Facoltativamente, viene stabilito un canale sicuro tra il veicolo e il dispositivo, derivando chiavi di sessione da un segreto condiviso in precedenza durante una transazione standard e una nuova coppia di chiavi effimere. L'abilità del veicolo di stabilire il canale sicuro autentica il veicolo su iPhone.

Transazioni standard BLE/UWB

Per i veicoli che utilizzano una chiave UWB, viene stabilita una sessione Bluetooth LE tra il veicolo e iPhone. In modo analogo a quanto avviene per una transazione NFC, viene derivato da entrambi i lati un segreto condiviso che viene poi utilizzato per stabilire una sessione sicura. Successivamente, la sessione viene utilizzata per ottenere e firmare una UWB Ranging Secret Key (URSK). La chiave URSK viene fornita alle radio UWB nel dispositivo dell'utente e sul veicolo per abilitare la localizzazione accurata del dispositivo in una posizione specifica nelle vicinanze o all'interno del veicolo. Il veicolo utilizzerà quindi la posizione del dispositivo per decidere se consentire o meno lo sblocco dell'auto o l'accensione del motore. Le chiavi URSK presentano un TTL predefinito. Per evitare l'interruzione delle operazioni di ranging quando un TTL scade, è possibile prederivare le chiavi URSK in SE del dispositivo e HSM/SE del veicolo, mentre il ranging protetto non è attivo ma BLE è connesso. In questo modo, durante una transazione standard non è più necessario derivare una nuova URSK in situazioni in cui la rapidità è cruciale. La chiave URSK prederivata può essere trasferita molto rapidamente alle radio UWB dell'auto e del dispositivo per evitare l'interruzione del ranging UWB.

Privacy

Il server del produttore che conserva l'inventario delle chiavi non archivia l'ID del dispositivo, il SEID o l'ID Apple. Esso archivia solamente un identificativo mutabile, l'identificativo dell'autorità di certificazione. Tale identificativo non è legato a nessun dato privato sul dispositivo o sul server e viene eliminato quando l'utente inizializza il dispositivo (tramite l'opzione "Inizializza contenuto e impostazioni").

Aggiungere carte trasporti e per i pagamenti elettronici ad Apple Wallet

In molti mercati globali, gli utenti possono aggiungere le carte per i trasporti e per i pagamenti elettronici compatibili in Apple Wallet sui modelli supportati di iPhone e Apple Watch. In base all'azienda, possono farlo trasferendo il valore o il titolo di viaggio o entrambi da una carta fisica alla corrispondente rappresentazione digitale in Apple Wallet oppure richiedendo una nuova carta per i trasporti da Apple Wallet o dall'app dell'emittente della carta. Una volta che le carte sono state aggiunte ad Apple Wallet, gli utenti possono utilizzare i mezzi pubblici semplicemente avvicinando iPhone o Apple Watch all'apposito lettore. Alcune carte trasporti possono essere utilizzate anche per effettuare pagamenti.

Funzionamento delle carte trasporti e per i pagamenti elettronici

Le carte per i trasporti e i pagamenti elettronici aggiunte sono associate all'account iCloud dell'utente. Se l'utente aggiunge più di una carta ad Apple Wallet, Apple o l'azienda di trasporti potrebbero essere in grado di collegare le informazioni personali dell'utente e le relative informazioni dell'account tra le varie carte. Le carte per i trasporti e i pagamenti elettronici e le relative transazioni sono protette da un insieme di chiavi di codifica gerarchiche.

Durante il processo di trasferimento del saldo da una carta fisica ad Apple Wallet, agli utenti viene richiesto di inserire i dati specifici della carta. Agli utenti potrebbe anche essere richiesto di fornire informazioni personali per dimostrare di essere i possessori della carta. Durante il trasferimento dei biglietti da iPhone ad Apple Watch, entrambi i dispositivi devono essere in linea.

Il saldo può essere ricaricato con fondi provenienti da carte di credito, debito o prepagate tramite Apple Wallet o dall'app dell'emittente della carta per i trasporti o i pagamenti elettronici. Per informazioni sulla sicurezza della ricarica del saldo quando si utilizza Apple Pay, consulta Pagare con le carte all'interno delle app. Per informazioni sulla fornitura delle carte dall'app dell'emittente, consulta Aggiungere carte di credito o di debito dall'app dell'emittente.

Se è supportata l'aggiunta di una carta fisica, l'emittente della carta per i trasporti o per i pagamenti elettronici dispone delle chiavi di crittografia necessarie all'autenticazione della carta fisica e alla verifica dei dati inseriti dall'utente. Una volta verificati i dati, il sistema può creare un numero identificativo del dispositivo per Secure Element e attivare il biglietto appena aggiunto in Apple Wallet con il saldo trasferito. Per alcune carte, una volta completato l'inserimento della carta fisica, questa viene disabilitata.

Alla fine di entrambi i processi di inserimento, se il saldo della carta viene archiviato sul dispositivo, viene crittografato e archiviato in un'apposita applet in Secure Element. L'operatore dispone delle chiavi per eseguire le operazioni di crittografia sui dati della carta per le transizioni che riguardano il saldo.

Di default, gli utenti delle carte trasporti possono sfruttare l'opzione di pagamento rapido, che consente loro di pagare ed effettuare corse senza che venga richiesto l'uso di Face ID, Touch ID o del codice. Informazioni come le stazioni visitate di recente, la cronologia delle transazioni e i biglietti aggiuntivi sono accessibili da parte di qualsiasi lettore di carte contactless vicino che abbia l'opzione "Modalità rapida" abilitata. Gli utenti possono attivare la richiesta di autorizzazione tramite Face ID, Touch ID o codice nelle impostazioni "Wallet e Apple Pay", disabilitando l'opzione "Carta rapida trasporti". La modalità rapida non è supportata per le carte per i pagamenti elettronici.

Come per le altre carte di Apple Pay, per sospendere o rimuovere le carte per i trasporti o i pagamenti elettronici, gli utenti possono:

- Inizializzare il dispositivo da remoto con Dov'è.
- Abilitare la modalità smarrito con Dov'è.
- Inserire un comando di cancellazione del dispositivo da remoto tramite una soluzione MDM.
- Rimuovere tutte le carte dalla pagina dell'account ID Apple.
- Rimuovere tutte le carte da iCloud.com.
- Rimuovere tutte le carte da Apple Wallet.
- Rimuovendo la carta dall'app dell'emittente.

I server di Apple Pay invieranno una richiesta all'operatore per sospendere o disabilitare tali carte. Se un utente rimuove la propria carta per i trasporti o per i pagamenti elettronici da un dispositivo online, il saldo può essere recuperato aggiungendola di nuovo a un dispositivo a cui è stato effettuato l'accesso con lo stesso ID Apple. Se il dispositivo non è in linea, è spento o inutilizzabile, il recupero potrebbe non essere possibile.

Aggiungere carte trasporti e per i pagamenti elettronici all'Apple Watch di uno dei membri della famiglia

In iOS 15 o versioni successive e watchOS 8 o versioni successive, l'organizzatore di una famiglia su iCloud ha la possibilità di aggiungere le carte per i trasporti e i pagamenti elettronici agli Apple Watch dei membri della famiglia, utilizzando l'app Watch su iPhone. Quando viene fornito l'accesso a una di queste carte dall'Apple Watch di uno dei membri della famiglia, è necessario che Apple Watch si trovi nelle vicinanze e che sia connesso all'iPhone dell'organizzatore mediante la rete Wi-Fi o il Bluetooth. I membri della famiglia devono aver abilitato l'autenticazione a due fattori per il proprio ID Apple.

I membri della famiglia possono inviare una richiesta per aggiungere denaro a una carta per i trasporti o per i pagamenti elettronici dal loro Apple Watch tramite iMessage. Il contenuto del messaggio è protetto tramite crittografia end-to-end, come descritto in Panoramica sulla sicurezza di iMessage. È possibile aggiungere denaro a una carta dall'Apple Watch di un membro della famiglia anche in remoto tramite una connessione Wi-Fi o i dati cellulare. Non è necessaria la prossimità.

Nota: questa funzionalità potrebbe non essere disponibile in tutti i paesi o in tutte le zone.

Carte di credito e di debito

In alcune città, i lettori dei mezzi pubblici accettano le carte (smart) EMV per il pagamento delle corse. Quando un utente avvicina una carta di credito o di debito EMV a tali lettori, viene richiesta l'autorizzazione dell'utente esattamente come nel caso del pagamento con carta di credito o di debito nei negozi.

In iOS 12.3 o versioni successive, è possibile abilitare alcune delle carte di credito o di debito EMV che sono già presenti in Apple Wallet come carte rapide per i trasporti. In questo modo, gli utenti potranno pagare una corsa con un operatore di trasporto che supporta la funzionalità, senza doversi autenticare tramite Face ID, Touch ID o un codice. Quando un utente aggiunge una carta di credito o debito EMV, la prima carta fornita ad Apple Wallet viene abilitata come carta rapida trasporti. L'utente può toccare il pulsante Altro sulla parte anteriore della carta in Apple Wallet e disabilitare la carta rapida trasporti per quella carta impostando l'opzione "Impostazioni carte rapide trasporti" su Nessuna. In Apple Wallet, inoltre, l'utente può selezionare una carta di credito o debito diversa come carta rapida trasporti. Per abilitare nuovamente la modalità rapida oppure per selezionare un'altra carta come carta trasporti, è richiesta l'autenticazione tramite Face ID, Touch ID o il codice.

Apple Card e Apple Cash sono compatibili con le carte rapide trasporti.

Documenti d'identità in Apple Wallet

Documenti d'identità in Apple Wallet

In iPhone 8 o modelli successivi con iOS 15.4 o versioni successive e in Apple Watch Series 4 o modelli successivi con watchOS 8.4 o versioni successive, gli utenti possono aggiungere il proprio documento d'identità o la patente ad Apple Wallet e toccare iPhone o Apple Watch per presentarli in modo semplice e sicuro, nei casi in cui la funzionalità è supportata.

Nota: disponibile soltanto in alcuni stati degli Stati Uniti.

I documenti d'identità in Apple Wallet utilizzano le funzionalità di sicurezza integrate nell'hardware e nel software dei dispositivi degli utenti, allo scopo di proteggere la loro identità e tenere al sicuro le loro informazioni personali.

Aggiungere la patente o un documento d'identità ad Apple Wallet

Su iPhone, basta premere il pulsante Aggiungi (+) nella parte superiore della schermata di Apple Wallet per iniziare ad aggiungere la patente o un documento d'identità. Se al momento della configurazione, gli utenti hanno un Apple Watch abbinato, viene richiesto loro di aggiungere la patente o il documento d'identità anche ad Apple Wallet su Apple Watch.

Prima di tutto agli utenti viene richiesto di utilizzare iPhone per scansionare la parte anteriore e posteriore della patente o del documento d'identità fisici. Quindi iPhone valuta la qualità e il tipo di immagini acquisito per garantire che possano essere accettate dalle autorità dello stato che emette i documenti. Queste immagini vengono crittografate sul dispositivo utilizzando la chiave messa a disposizione dalle autorità dello stato che emette i documenti e inviate poi alle autorità stesse.

Poi all'utente viene richiesto di completare la registrazione di una serie di movimenti del volto e della testa. Questi vengono valutati dal dispositivo dell'utente e da Apple per ridurre il rischio che venga utilizzata una fotografia, un video o una maschera per cercare di aggiungere ad Apple Wallet un documento d'identità di terzi e non il proprio. I risultati dell'analisi di questi movimenti vengono poi inviati all'autorità di emissione ma il video dei movimenti non viene inviato direttamente.

Per garantire che la persona che sta aggiungendo il documento d'identità ad Apple Wallet coincida con il titolare del documento d'identità, agli utenti viene richiesto di scattare un selfie. Prima che la foto dell'utente venga inviata all'autorità emittente, i server di Apple e il dispositivo dell'utente confrontano la foto con l'aspetto della persona che ha registrato i movimenti del volto e della testa, in modo da garantire che la foto che sta per essere inviata sia di una persona realmente esistente molto somigliante a quella sulla foto presente nel documento. Al termine del confronto, la foto viene crittografata sul dispositivo e inviata all'autorità emittente per essere confrontata ulteriormente con la foto archiviata con il documento d'identità.

Infine, agli utenti viene richiesto di autenticarsi tramite Face ID o Touch ID. Il dispositivo dell'utente collega i dati biometrici corrispondenti in modo univoco a Face ID o Touch ID al documento d'identità, per garantire che soltanto la persona che ha effettivamente aggiunto il documento d'identità ad iPhone sia autorizzata a presentarlo. Dati biometrici registrati in altri modi non possono essere utilizzati per autorizzare la presentazione del documento d'identità. Questa procedura avviene esclusivamente in locale sul dispositivo e non viene condivisa con l'autorità che emette il documento.

Tuttavia, quest'ultima riceverà le informazioni necessarie per configurare il documento d'identità digitale. Queste includono le immagini della parte anteriore e posteriore del documento d'identità dell'utente, i dati acquisiti dal codice a barre PDF417 e il selfie scattato come parte della procedura di verifica. L'autorità emittente riceve anche un codice di una cifra, che serve a prevenire le frodi, basato sulle abitudini di utilizzo del dispositivo dell'utente, sui dati relativi alle impostazioni e sulle informazioni relative all'ID Apple personale. Al termine della procedura, sarà l'autorità emittente a decidere se approvare o respingere la richiesta di aggiunta del documento di identità ad Apple Wallet.

Dopo che l'autorità emittente avrà autorizzato l'aggiunta del documento d'identità o della patente ad Apple Wallet, viene generata una coppia di chiavi in Secure Element su iPhone che vincola il documento a quel dispositivo specifico. Nel caso in cui il documento venga aggiunto ad Apple Watch, la coppia di chiavi viene generata in Secure Element su Apple Watch.

Una volta che il documento d'identità è stato aggiunto su iPhone, le informazioni in esso contenute vengono salvate in Apple Wallet in formato crittografato e protette tramite Secure Enclave.

Utilizzare la patente o un documento d’identità in Apple Wallet con un lettore di documenti

Per utilizzare un documento in Apple Wallet, gli utenti devono autenticarsi tramite Face ID o Touch ID sul dispositivo associato al documento d’identità in Apple Wallet, prima che iPhone possa presentare le informazioni all’apposito lettore.

Per utilizzare un documento in Apple Wallet su Apple Watch, gli utenti devono sbloccare il proprio iPhone utilizzando l’aspetto di Face ID o l’impronta digitale di Touch ID associati ogni volta che indossano Apple Watch. Quindi potranno utilizzare il proprio documento d’identità su Apple Wallet senza doversi autenticare nuovamente fino a quando non si tolgono Apple Watch. Questa funzionalità si basa sullo sblocco automatico di base descritto nella sezione dedicata alla sicurezza di sistema per watchOS.

Quando gli utenti avvicinano iPhone o Apple Watch a un lettore di documenti o quando condividono il proprio documento d’identità tramite un’app, vedranno un messaggio sul dispositivo che mostra le informazioni specifiche che vengono richieste, da chi e se verranno memorizzate. Dopo aver autorizzato l’operazione con Face ID o Touch ID associati, le informazioni relative all’identità richieste vengono autorizzate dal dispositivo.

Importante: per presentare il documento d’identità, non sarà necessario sbloccare, mostrare o passare il dispositivo ad altre persone.

Nel caso in cui venga utilizzata una funzionalità di accessibilità come “Controllo vocale”, “Controllo interruttori” o AssistiveTouch al posto di Face ID o Touch ID, gli utenti possono utilizzare il codice di accesso per presentare le informazioni richieste.

La trasmissione dei dati relativi all’identità al lettore dei documenti è conforme allo standard ISO/IEC 18013-5, che prevede la presenza di vari meccanismi di sicurezza in grado di individuare, bloccare e attenuare i rischi per la sicurezza. Questi includono l’integrità dei dati relativi all’identità e misure anti-falsificazione, l’associazione a un unico dispositivo, il consenso informato e tutela della riservatezza dei dati dell’utente tramite link radio.

Utilizzare la patente o un documento d’identità in Apple Wallet con le app di iOS

Gli utenti possono condividere le informazioni della propria patente o del proprio documento d’identità in Apple Wallet anche con le app di iOS. Quando un utente condivide il proprio documento d’identità con un’app, Wallet recupera e convalida un certificato di crittografia registrato con lo sviluppatore dell’app.

Tale certificato verrà usato per crittografare le informazioni di cui l’utente ha autorizzato la condivisione. Le informazioni vengono crittografate da Wallet tramite HPKE e non vengono mai rese disponibili ad Apple. Wallet contatta periodicamente i server Apple per verificare che il documento sia ancora valido. Se recentemente non è stata effettuata alcuna verifica, è possibile che ne venga eseguita una quando l’utente condivide il documento d’identità con un’app.

La sicurezza dei documenti d’identità in Apple Wallet

Le funzionalità descritte di seguito consentono di migliorare la sicurezza durante l’utilizzo dei documenti d’identità in Apple Wallet.

Misure anti-falsificazione e per garantire l'integrità dei dati

I documenti d'identità in Apple Wallet utilizzano una firma da parte dell'autorità emittente per consentire a un lettore conforme allo standard ISO/IEC 18013-5 di verificare il documento dell'utente salvato in Apple Wallet. Inoltre, tutti gli elementi dati presenti nel documento salvato in Wallet sono protetti singolarmente dalla falsificazione. Questo consente al lettore di richiedere un sottogruppo specifico di elementi dati presenti sul documento in Apple Wallet e al documento in Apple Wallet di rispondere mettendo a disposizione esattamente il sottogruppo richiesto, condividendo soltanto i dati richiesti e ottimizzando la protezione della privacy dell'utente.

Associazione a un dispositivo

L'autenticazione dei documenti d'identità in Apple Wallet utilizza la firma del dispositivo per impedire che i documenti vengano clonati e riutilizzati in modo improprio. Apple Wallet archivia la chiave privata per l'autenticazione del documento in Secure Element su iPhone, in modo che il documento sia collegato allo stesso dispositivo per cui l'autorità emittente ha creato il documento d'identità digitale.

Consenso informato

I documenti d'identità in Apple Wallet potrebbero venire autenticati sul lettore utilizzando il protocollo definito dallo standard ISO/IEC 18013-5. Durante la presentazione del documento, se il lettore ha il proprio certificato e questo è ritenuto attendibile da Apple Wallet, viene mostrata un'icona per confermare all'utente che sta interagendo con l'entità prevista.

Protezione della riservatezza dei dati dell'utente tramite i link radio

La crittografia delle sessioni garantisce che tutti i dati che consentono di risalire all'identità dell'utente scambiati tra il documento d'identità in Apple Wallet e il lettore di documenti vengano crittografati. La crittografia viene eseguita a livello dell'applicazione. La sicurezza della crittografia della sessione non si basa dunque sul livello della trasmissione, ad esempio NFC, Bluetooth e Wi-Fi.

Con i documenti d'identità in Apple Wallet le informazioni dell'utente rimangono riservate

I documenti d'identità in Apple Wallet aderiscono alle procedure di "recupero dei dispositivi" illustrate nello standard ISO/IEC 18013-5. Queste consentono di ovviare alla necessità di effettuare chiamate ai server durante la presentazione dei documenti d'identità, evitando che l'identità degli utenti venga tracciata da Apple o dall'autorità emittente.

Sicurezza della verifica dell'identità

In iOS 17 o versioni successive, le aziende e le organizzazioni statunitensi possono utilizzare iPhone per leggere in modo sicuro e agevole i documenti d'identità conformi allo standard ISO 18013-5 in presenza, senza dover utilizzare hardware esterno. La funzionalità di verifica dell'identità può essere utilizzata in due modi, in base al caso d'uso:

- *Verifica dell'identità finalizzata solo alla visualizzazione di informazioni:* con questa opzione è possibile utilizzare un'interfaccia utente di iOS per visualizzare dati quali nome, età, foto del documento ed età per i casi d'uso in cui è necessario ottenere soltanto una conferma visiva. Il servizio non raccoglie alcuna *informazione personale* che possa essere ricollegata all'utente che effettua il pagamento.

- *Trasferimento dati durante la verifica dell'identità:* questa funzionalità consente alle app di richiedere ulteriori dati, come la data di nascita e l'indirizzo, per soddisfare i requisiti di verifica previsti per legge. L'accesso all'API del trasferimento dei dati durante la verifica dell'identità è controllato attraverso autorizzazioni e le app devono essere conformi alle restrizioni che riguardano l'uso dei dati. Ad esempio, le app devono dimostrare che sussiste un requisito legale per richiedere dati relativi all'identità. Inoltre, le app sono tenute a rispettare un'informativa sulla privacy che disciplini nel dettaglio le modalità di elaborazione, archiviazione e altro utilizzo dei dati relativi all'identità richiesti.

Leggere un documento d'identità su dispositivo mobile

La funzionalità di verifica dell'identità segue il protocollo definito in base allo standard ISO/IEC 18013-5. Quando un'app che utilizza l'API di verifica dell'identità richiede di leggere un documento d'identità su dispositivo mobile, viene mostrato un pannello, controllato da iOS, che invita la persona a cui è intestato il documento ad avvicinare il dispositivo al lettore. Il primo contatto NFC (a quanto definito dallo standard ISO/IEC 18013-5, è possibile utilizzare un codice QR per avviare una procedura di trasferimento tramite Bluetooth in luogo della tecnologia NFC) stabilisce una connessione sicura Bluetooth® Low Energy (BLE) tra i due dispositivi. A questo punto, la persona titolare del documento d'identità può verificare sul proprio dispositivo le informazioni che vengono richieste. Una volta concessa l'autorizzazione avrà concesso l'autorizzazione, i dati richiesti vengono trasferiti al lettore. Le app che utilizzano l'API per il trasferimento dati di verifica dell'identità ricevono i dati di risposta per l'elaborazione, mentre le app che utilizzando l'API di sola visualizzazione di verifica dell'identità vedono direttamente i dati mostrati da iOS.

In base allo standard ISO/IEC 18013-5 sono previsti vari meccanismi di sicurezza per rilevare, bloccare e mitigare i rischi di sicurezza. A questo proposito, la funzionalità di verifica dell'identità controlla sia la firma dell'emittente che quella del dispositivo. Inoltre, supporta l'autenticazione del lettore tramite il protocollo definito in base allo standard ISO/IEC 18013-5. Le app possono visualizzare un'icona e il nome per confermare che la persona titolare del documento sta interagendo con la parte interessata tramite il certificato del lettore.

Convalida di emittente e dispositivo

Come misura di protezione contro la contraffazione, la funzionalità di verifica dell'identità convalida la firma dell'oggetto di sicurezza mobile dell'emittente attendibile dell'identità mobile. Inoltre, il trasferimento di dati della verifica dell'identità offre un'API che consente alle app di eseguire la convalida delle firme al posto di iOS, se necessario. Per dare conferma all'azienda o all'organizzazione che il documento digitale non è stato copiato da un dispositivo all'altro, la verifica dell'identità convalida la firma tramite i dati della sessione.

Autenticazione del lettore

Quando il documento viene presentato, la richiesta del lettore di verifica dell'identità viene firmata tramite la chiave privata associata al certificato di autenticazione del lettore che si collega all'autorità di certificazione root di Apple, contenente le estensioni personalizzate x509 rilevanti per indicare alla persona titolare del documento se l'azienda intende archiviare i suoi dati. Se si desidera che un'applicazione mostri il nome e l'icona alla persona titolare del documento, l'amministratore dell'app deve effettuare la registrazione tramite Apple Business Register e fornire informazioni accurate sul marchio. In seguito alla verifica delle informazioni inviate, quando viene eseguita la transazione, il certificato di autenticazione del lettore fornisce alla persona titolare del documento le informazioni relative all'entità provenienti da Apple Register, tramite il certificato stesso.

iMessage

Panoramica sulla sicurezza di iMessage

Apple iMessage è un servizio di messaggistica per iPhone e iPad, Apple Watch e Mac che supporta testo e allegati come foto, contatti, posizioni, link e allegati direttamente in un messaggio, come ad esempio l'icona del pollice rivolto verso l'alto. I messaggi compaiono su tutti i dispositivi registrati dell'utente, in modo da poter continuare la conversazione su qualsiasi dispositivo. iMessage fa un uso estensivo del servizio di notifiche push di Apple (APN). Apple non tiene traccia di messaggi o allegati e i loro contenuti sono protetti da una codifica end-to-end in modo che solo il mittente e il destinatario possano accedervi. Apple non può decrittografare i dati.

Quando un utente attiva iMessage su un dispositivo, questo genera coppie di chiavi di firma e codifica da utilizzare con il servizio. Per la codifica, il dispositivo fa uso di una chiave RSA a 1280 bit e di una chiave EC a 256 bit sulla curva NIST P-256. Per le firme, vengono usate chiavi di firma da 256 bit basate su ECDSA (Elliptic Curve Digital Signature Algorithm). Le chiavi private vengono salvate nel portachiavi del dispositivo e sono disponibili solo dopo il primo sblocco. Le chiavi pubbliche vengono inviate al servizio Apple Identity Service (IDS), dove sono associate al numero di telefono o all'indirizzo e-mail dell'utente, insieme all'indirizzo APN del dispositivo.

Man mano che gli utenti abilitano altri dispositivi per l'utilizzo di iMessage, le loro chiavi pubbliche per la codifica e la firma, gli indirizzi APN e i numeri di telefono associati vengono aggiunti al servizio di directory. Gli utenti possono anche aggiungere altri indirizzi e-mail, che vengono verificati con l'invio di un link di conferma. I numeri di telefono vengono verificati dalla rete e dalla SIM del gestore. Con alcune reti, tale operazione richiede l'utilizzo del servizio SMS (all'utente viene mostrata una finestra di conferma se il messaggio SMS non è gratuito). La verifica del numero di telefono può essere richiesta per vari servizi di sistema oltre a iMessage, come FaceTime e iCloud. Tutti i dispositivi registrati dell'utente mostrano un messaggio di avviso quando viene aggiunto un nuovo dispositivo, numero di telefono o indirizzo e-mail.

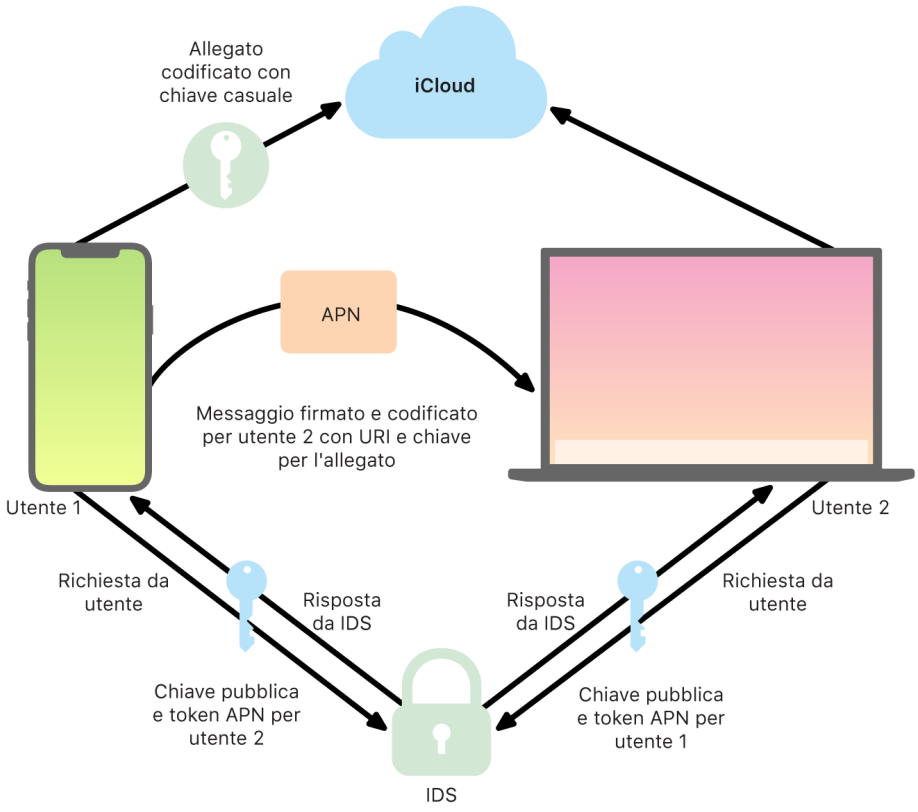
Processo di invio e ricezione sicuri dei messaggi con iMessage

Gli utenti avviano una nuova conversazione iMessage inserendo un indirizzo o un nome. Se inseriscono un numero di telefono o un indirizzo e-mail, il dispositivo contatta Apple Identity Service (IDS) per recuperare le chiavi pubbliche e gli indirizzi APN di tutti i dispositivi associati al destinatario. Se l'utente inserisce un nome, il dispositivo utilizza prima l'app Contatti per ottenere i numeri di telefono e gli indirizzi e-mail associati al nome, quindi recupera le chiavi pubbliche e gli indirizzi APN dall'IDS.

Il messaggio in uscita viene codificato individualmente per ciascun dispositivo del destinatario. Le chiavi pubbliche di codifica e firma dei dispositivi riceventi vengono recuperate dall'IDS. Per ogni dispositivo di ricezione, il dispositivo di invio genera un valore a 88 bit casuale e lo utilizza come chiave HMAC-SHA256 per costruire un valore a 40 bit derivato dalla chiave pubblica del mittente e del ricevente, oltre che dal testo. La concatenazione dei valori a 88 e 40 bit crea una chiave a 128 bit, che codifica il messaggio tramite AES in modalità CTR. Il valore a 40 bit è utilizzato dal ricevente per verificare l'integrità del testo decrittografato. Questa chiave AES per messaggio è codificata utilizzando RSA-OAEP sulla chiave pubblica del dispositivo ricevente. La combinazione tra testo del messaggio codificato e chiave del messaggio codificato viene quindi sottoposta a hashing con SHA-1; a questo punto, l'hash viene firmato tramite l'algoritmo ECDSA utilizzando la chiave privata per la firma del dispositivo mittente. In iOS 13 o versioni successive e iPadOS 13.1 o versioni successive, i dispositivi possono utilizzare la codifica ECIES al posto della codifica RSA.

I messaggi risultanti, uno per ciascun dispositivo ricevente e contenenti il testo del messaggio codificato, la chiave del messaggio codificato e la firma digitale del mittente, sono quindi inviati al servizio APN per la consegna. I metadati, come l'indicazione di data e ora e le informazioni per l'instradamento via APN, non sono codificati. La comunicazione con il servizio APN è codificata utilizzando un canale TLS forward-secret.

Il servizio APN può solo inoltrare messaggi di dimensioni fino a 4 KB o 16 KB, a seconda della versione di iOS o iPadOS. Se il messaggio è troppo lungo, o se contiene un allegato come una foto, l'allegato viene codificato utilizzando AES in modalità CTR con una chiave casuale a 256 bit e quindi caricato su iCloud. La chiave AES per l'allegato, il suo Uniform Resource Identifier (URI) e un hash SHA-1 della sua forma codificata vengono quindi inviati al destinatario come contenuti di un iMessage; la riservatezza e l'integrità dei contenuti sono protette tramite la normale codifica di iMessage, come mostrato nel seguente diagramma.



Per le conversazioni di gruppo, questo processo viene ripetuto per ogni destinatario e per ciascuno dei loro dispositivi.

Sul lato del destinatario, ogni dispositivo riceve la propria copia del messaggio dal servizio APN e, se necessario, recupera l'allegato da iCloud. Il numero di telefono o l'indirizzo e-mail del mittente viene confrontato con i contatti del destinatario per poter visualizzare un nome, se possibile.

Come per tutte le notifiche push, il messaggio viene eliminato dal servizio APN una volta consegnato. Tuttavia, a differenza di altre notifiche APN, i messaggi iMessage vengono messi in coda per essere consegnati ai dispositivi non in linea. I messaggi restano memorizzati sui server Apple per un massimo di 30 giorni.

Condivisione sicura della foto e del nome in iMessage

La condivisione della foto e del nome in iMessage consente all'utente di condividere il proprio nome e la propria foto usando iMessage. L'utente può selezionare le informazioni della scheda personale oppure personalizzare il nome e includere un'immagine di sua scelta. La condivisione del nome e della foto con iMessage utilizza un sistema in due passaggi per distribuire il nome e la foto.

I dati vengono suddivisi in campi, ognuno di questi campi viene codificato e autenticato separatamente e poi tutti i campi vengono autenticati insieme secondo il processo descritto a continuazione. Esistono tre campi:

- Nome
- Foto
- Nome file foto

Un primo passaggio per la creazione dei dati è la generazione casuale di una chiave record a 128 bit sul dispositivo. Tale chiave record viene quindi derivata con HKDF-HMAC-SHA256 per creare tre sotto-chiavi: chiave 1:chiave 2:chiave 3 = HKDF(chiave record, "soprannomi"). Per ogni campo viene generato un vettore di inizializzazione a 96 bit casuale e i dati vengono codificati mediante AES-CTR e la chiave 1. Viene poi elaborato un codice di autenticazione del messaggio (MAC) con HMAC-SHA256 tramite la chiave 2 e coprendo il nome del campo, il vettore di inizializzazione del campo e il ciphertext del campo. Infine, viene concatenato l'insieme dei valori MAC dei singoli campi e il relativo MAC viene elaborato con HMAC-SHA256 tramite la chiave 3. Il MAC a 256 bit viene archiviato insieme dati codificati. I primi 128 bit di questo MAC sono utilizzati come recordID.

Questo record codificato viene poi archiviato nel database pubblico di CloudKit come recordID. Questo record non cambia mai e ogni volta che l'utente sceglie di modificare il nome utente e la foto viene generato un nuovo record. Quando l'utente 1 sceglie di condividere nome e foto con l'utente 2, invia una chiave record insieme al recordID all'interno del payload di iMessage, che è codificato.

Quando il dispositivo dell'utente 2 riceve questo payload di iMessage, nota che contiene una chiave e un recordID per soprannome e foto. Il dispositivo dell'utente 2 recupera dal database pubblico di CloudKit il nome e la foto codificati nel recordID e li invia tramite iMessage.

Una volta ricevuto il messaggio, il dispositivo dell'utente 2 decrittografa il payload e verifica la firma usando il recordID stesso. Se la verifica ha esito positivo, l'utente 2 visualizza il nome e la foto e può scegliere di aggiungerli ai contatti o di usarli per Messaggi.

Sicurezza in Apple Messages for Business

Apple Messages for Business è un servizio di messaggistica che consente agli utenti di comunicare con le aziende tramite l'app Messaggi. Con Apple Messages for Business, l'utente ha sempre il controllo della conversazione. Può anche eliminare le conversazioni e bloccare un'azienda per impedirle di inviargli messaggi in futuro. Per proteggere la privacy, l'azienda non riceve il numero di telefono, l'indirizzo e-mail o le informazioni dell'account iCloud dell'utente. Al loro posto, tramite il servizio IDS viene generato e condiviso con l'azienda un identificativo unico chiamato *Opaque ID*. L'Opaque ID è unico e legato alla relazione tra l'ID Apple dell'utente e l'identificativo dell'azienda. Ogni utente ha un Opaque ID diverso per ciascuna azienda che contatta tramite Apple Messages for Business. L'utente decide se e quando condividere le informazioni che potrebbero consentire di risalire alla sua identità con le aziende e su Apple Messages for Business non viene mai salvata la cronologia delle conversazioni.

Apple Messages for Business supporta gli ID Apple gestiti da Apple Business Manager e determina se sono abilitati per iMessage e FaceTime in Apple School Manager.

I messaggi inviati alle aziende sono codificati tra il dispositivo dell'utente e i server di messaggistica Apple e viene utilizzato lo stesso livello di sicurezza e gli stessi server di messaggistica Apple di iMessage. I server di messaggistica Apple decrittografano tali messaggi nella RAM e li inoltra all'azienda tramite un link crittografato utilizzando il protocollo TLS 1.2. I messaggi non vengono mai archiviati in formato codificato mentre transitano attraverso il servizio Apple Messages for Business. Anche le risposte delle aziende sono inviate tramite TLS 1.2 ai server di messaggistica Apple, dove sono codificati tramite le chiavi pubbliche uniche di ciascun dispositivo destinatario.

Se il dispositivo dell'utente è in linea, il messaggio viene consegnato immediatamente e non è inserito nella cache dei server di messaggistica Apple. Se il dispositivo dell'utente non è in linea, il messaggio codificato viene inserito nella cache per un numero massimo di 30 giorni per consentire all'utente di riceverlo quando il dispositivo torna in linea. Appena il dispositivo torna in linea, il messaggio viene consegnato ed eliminato dalla cache. Dopo 30 giorni, i messaggi non consegnati presenti nella cache scadono e vengono eliminati in modo permanente.

Sicurezza di FaceTime

FaceTime è il servizio di Apple per chiamate video e audio. In modo simile a quanto avviene per iMessage, le chiamate FaceTime utilizzano il servizio di notifiche push di Apple (APN) per stabilire una connessione iniziale con i dispositivi registrati dell'utente. I contenuti audio/video delle chiamate FaceTime sono protetti da codifica end-to-end, in modo che solo il mittente e il destinatario possano accedervi. Apple non può decrittografare i dati.

La connessione FaceTime iniziale viene effettuata tramite un'infrastruttura di server Apple, che fungono da elemento di trasmissione dei pacchetti tra i dispositivi registrati degli utenti. Tramite le notifiche APN e i messaggi STUN (Session Traversal Utilities for NAT) attraverso questa connessione, i dispositivi verificano i propri certificati di identità e stabiliscono un segreto condiviso per ogni sessione. Il segreto condiviso è utilizzato per generare le chiavi di sessione per i canali multimediali trasmessi in streaming tramite il protocollo SRTP (Secure Real-time Transport Protocol). I pacchetti SRTP sono codificati tramite AES256 in Counter Mode e autenticati con HMAC-SHA1. Dopo la configurazione iniziale della connessione e della sicurezza, FaceTime utilizza i protocolli STUN e ICE (Internet Connectivity Establishment) per stabilire una connessione peer-to-peer tra i dispositivi, se possibile.

Le chiamate FaceTime di gruppo estendono le capacità di FaceTime per supportare fino a 33 partecipanti contemporaneamente. Così come per le chiamate FaceTime singole classiche, le chiamate di gruppo usufruiscono della codifica end-to-end tra i dispositivi dei partecipanti invitati. Sebbene le chiamate FaceTime di gruppo riutilizzino gran parte dell'infrastruttura e del design delle chiamate FaceTime singole, sono dotate di un meccanismo per la definizione delle chiavi che va ad aggiungersi all'autenticazione fornita da Apple Identity Service (IDS). Grazie alla segretezza fornita da questo protocollo, la compromissione del dispositivo di un utente non comporterà la diffusione dei contenuti delle chiamate precedenti. Le chiavi della sessione vengono cifrate tramite AES-SIV e distribuite tra i partecipanti tramite una costruzione ECIES (Elliptic Curve Integrated Encryption Scheme) con chiavi effimere P-256 ECDH.

Quando un nuovo numero di telefono o indirizzo email viene aggiunto a una chiamata FaceTime di gruppo in corso, i dispositivi attivi stabiliscono nuove chiavi multimediali e non condivideranno mai le chiavi utilizzate con i nuovi dispositivi invitati.

Dov’è

Sicurezza di Dov’è

L’app Dov’è per i dispositivi Apple si basa su avanzate tecniche di codifica avanzata tramite chiavi pubbliche.

Panoramica

L’app Dov’è riunisce “Trova il mio iPhone” e “Trova i miei amici” in una sola app disponibile per iOS, iPadOS e macOS. Dov’è può aiutare gli utenti a individuare un dispositivo smarrito, persino un Mac offline. Un dispositivo in linea può comunicare semplicemente la propria posizione all’utente tramite iCloud. Dov’è funziona offline inviando segnali Bluetooth a corto raggio dal dispositivo smarrito. Tali segnali possono essere rilevati da altri dispositivi Apple in uso nelle vicinanze. Tali dispositivi vicini possono inoltrare la posizione rilevata del dispositivo smarrito a iCloud e consentire così agli utenti di individuarne la posizione tramite l’app Dov’è. Queste operazioni vengono eseguite proteggendo la privacy e la sicurezza di tutti gli utenti coinvolti. Dov’è funziona anche con un Mac offline e in stato di stop.

Con Bluetooth e i centinaia di milioni di dispositivi iOS, iPadOS e macOS usati attivamente nel mondo, un utente può individuare un dispositivo smarrito persino quando non è connesso a una rete Wi-Fi o cellulare. Qualsiasi dispositivo iOS, iPadOS o macOS con l’opzione di ricerca offline abilitata nelle impostazioni di Dov’è può funzionare da dispositivo per il ritrovamento di altri. Questo significa che quel dispositivo può rilevare tramite Bluetooth la presenza di un altro dispositivo smarrito non in linea e utilizzare quindi la propria connessione di rete per notificare al proprietario la posizione approssimativa del dispositivo smarrito. Quando un dispositivo ha attiva l’opzione di ricerca offline, significa che può essere individuato anche da altri partecipanti nello stesso modo. L’intera interazione è protetta da crittografia end-to-end, anonima e concepita per limitare il consumo della batteria e dei dati. L’impatto sulla durata della batteria e sull’utilizzo dei dati cellulare è ridotto al minimo e la protezione della privacy dell’utente è migliorata.

Nota: Dov’è potrebbe non essere disponibile in tutti i paesi o in tutte le zone.

Codifica end-to-end

Dov'è si basa sulla codifica avanzata tramite chiave pubblica. Quando è abilitato il ritrovamento offline nelle impostazioni di Dov'è, viene generata una coppia di chiavi di codifica privata EC P-224 con notazione {d,P} direttamente sul dispositivo, in cui *d* è la chiave privata e *P* è quella pubblica. Inoltre, un segreto a 256 bit SK_0 e un contatore $_i$ vengono azzerati. Questa coppia di chiavi private e il segreto non vengono mai inviati ad Apple e sono sincronizzati unicamente tra i dispositivi dell'utente tramite codifica end-to-end con il portachiavi iCloud. Il segreto e il contatore sono utilizzati per derivare l'attuale SK_i della chiave simmetrica con la seguente costruzione ricorsiva: $SK_i = KDF(SK_{i-1}$, "aggiornare").

In base allo SK_i della chiave, vengono calcolati due grandi valori interi u_i e v_i con $(u_i,v_i) = KDF(SK_i$, "diversificare"). Sia la chiave privata P-224 denominata *d* sia la chiave pubblica denominata *P* vengono quindi derivate tramite una relazione affine che coinvolge i due interi per elaborare una coppia di chiavi a breve durata: la chiave privata derivata è d_i, dove $d_i = u_i * d + v_i$ (modulo l'ordine della curva P-224) e la parte pubblica corrispondente è P_i e verifica che $P_i = u_i*P + v_i*G$.

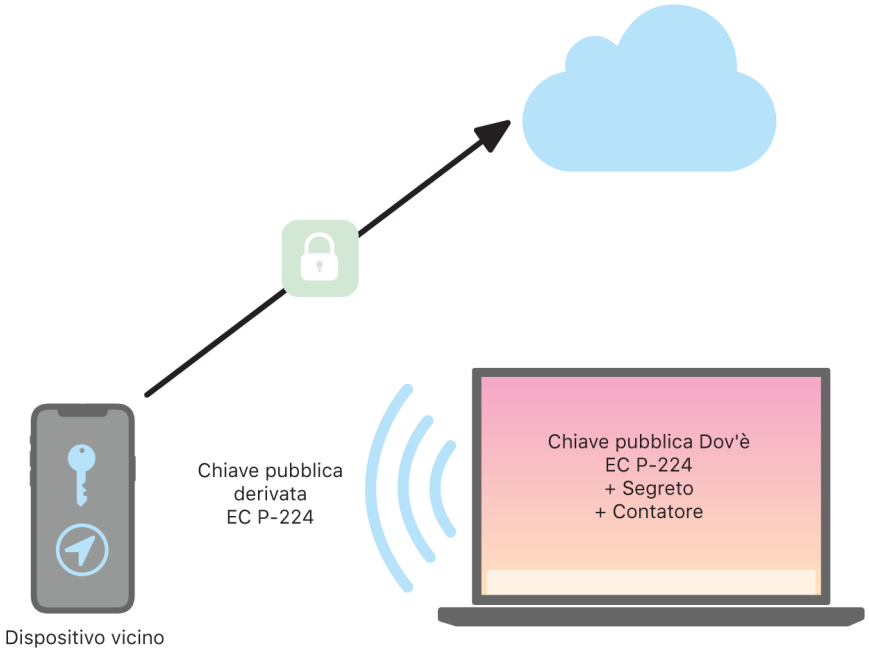
Quando un dispositivo viene smarrito e non può essere connesso al Wi-Fi o alla rete cellulare (per esempio, un MacBook Pro dimenticato su una panchina in un parco), inizia a trasmettere periodicamente la chiave pubblica P_i derivata per un periodo di tempo limitato in un payload Bluetooth. Tramite P-224, la rappresentazione della chiave pubblica può entrare in un singolo payload Bluetooth. I dispositivi circostanti aiutano quindi il ritrovamento del dispositivo offline codificando la propria posizione nella chiave pubblica. Ogni 15 minuti circa, la chiave pubblica viene sostituita da una nuova tramite un valore incrementale del contatore e del processo descritto sopra, in modo da impedire il tracciamento dell'utente da parte di un identificatore persistente. Il meccanismo di derivazione è progettato per impedire che le varie chiavi pubbliche P_i siano collegate allo stesso dispositivo.

Anonimato di utenti e dispositivi

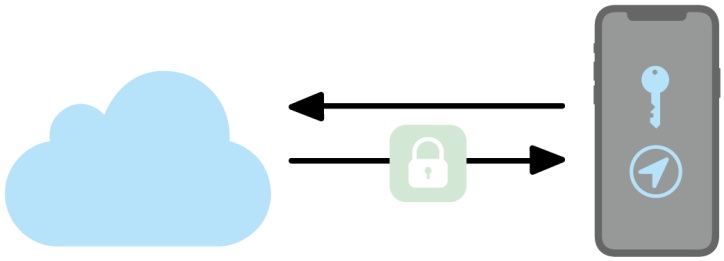
Oltre a garantire che le informazioni sulla posizione e altri dati siano totalmente codificati, le identità dei partecipanti rimangono private sia vicendevolmente che per Apple. Il traffico inviato ad Apple dai dispositivi per il ritrovamento non contengono informazioni relative all'autenticazione nei contenuti né nelle intestazioni. Di conseguenza, Apple non sa quale sia il dispositivo di ritrovamento né quello ritrovato. Apple inoltre non registra informazioni che potrebbero rivelare l'identità del dispositivo di ritrovamento né conserva informazioni che potrebbero consentire a qualcuno di mettere in relazione il dispositivo di ritrovamento con il proprietario. Il proprietario del dispositivo riceve le informazioni crittografate sulla posizione che vengono decrittografate e mostrate nell'app Dov'è senza indicazione riguardo a chi abbia trovato il dispositivo.

Utilizzare Dov'è per individuare dispositivi smarriti

Qualsiasi dispositivo Apple nel raggio di portata del Bluetooth con l'opzione relativa al ritrovamento offline abilitata può rilevare un segnale da un altro dispositivo Apple configurato per consentire Dov'è e leggere la chiave di trasmissione P_i attuale. Tramite una costruzione ECIES e la chiave pubblica P_i della trasmissione, i dispositivi che funzionano da rilevatori codificano le informazioni relative alla propria posizione e le inoltrano ad Apple. La posizione codificata è associata all'indice di un server calcolato come l'hash SHA256 della chiave pubblica P-224 P_i ottenuta dal payload Bluetooth. Apple non dispone mai della chiave di decrittografia, quindi non è in grado di leggere la posizione crittografata dal dispositivo di ritrovamento. Il proprietario del dispositivo smarrito può ricostruire l'indice e decrittografare la posizione crittografata.



Durante il tentativo di individuazione del dispositivo smarrito, viene stimato un intervallo atteso di valori del contatore per il periodo di ricerca della posizione. Conoscendo la chiave privata originale P-224 *d* e lo SK_i dei valori del segreto nell'intervallo dei valori del contatore del periodo di ricerca, il proprietario può ricostruire l'insieme di valori $\{d_i, SHA256(P_i)\}$ per l'intero periodo di ricerca. Il dispositivo utilizzato per individuare quello smarrito può quindi inviare delle query al server usando l'insieme dei valori dell'indice $SHA256(P_i)$ e scaricare le posizioni codificate dal server. L'app Dov'è decrittografa poi localmente le posizioni crittografate con le chiavi private corrispondenti d_i e mostra la posizione approssimata del dispositivo smarrito nell'app. I resoconti sulle posizioni ricevuti dai vari dispositivi per il ritrovamento vengono uniti dall'app del proprietario per generare una posizione più precisa.



Individuare dispositivi non in linea

Se un utente ha abilitato "Trova il mio iPhone" sul dispositivo, il ritrovamento offline viene abilitato di default quando esegue l'aggiornamento del dispositivo a iOS 13 o versioni successive, iPadOS 13.1 o versioni successive e macOS 10.15 o versioni successive. Questo meccanismo è progettato per garantire che ogni utente abbia il maggior numero di probabilità di ritrovare il proprio dispositivo qualora dovesse smarrirlo. Tuttavia, se l'utente preferisce non partecipare alla ricerca, può disabilitare il ritrovamento offline in qualunque momento dalle impostazioni di Dov'è sul dispositivo. Quando il ritrovamento offline è disabilitato, il dispositivo non contribuisce più al ritrovamento di altri dispositivi e non è individuabile da altri dispositivi di ritrovamento. Tuttavia l'utente può comunque localizzare il dispositivo se quest'ultimo è connesso a una rete Wi-Fi o dati cellulare.

Quando viene localizzato un dispositivo offline smarrito, all'utente vengono inviati una notifica e un messaggio email per informarlo che il dispositivo è stato ritrovato. Per visualizzare la posizione del dispositivo smarrito, l'utente apre l'app Dov'è e seleziona il pannello Dispositivi. Invece di visualizzare il dispositivo su una mappa vuota come avverrebbe se il dispositivo non fosse stato individuato, Dov'è mostra una posizione sulla mappa con un indirizzo approssimativo e informazioni sull'ora in cui il dispositivo è stato individuato. Se vengono ricevute ulteriori segnalazioni, la posizione attuale e l'orario sono aggiornati automaticamente. Sebbene gli utenti non possano far emettere un suono a un dispositivo offline né inizializzarlo da remoto, possono utilizzare le informazioni relative alla sua posizione per risalire al dispositivo o intraprendere altre azioni per recuperarlo.

Continuity

Panoramica sulla sicurezza di Continuity

Continuity sfrutta tecnologie come iCloud, Bluetooth e Wi-Fi per consentire agli utenti di riprendere su un dispositivo l'attività cominciata su un altro, di fare e ricevere telefonate, di inviare e ricevere messaggi di testo e di condividere una connessione cellulare a internet.

Sicurezza di Handoff

Apple gestisce la funzionalità Handoff in modo sicuro, sia che venga usata tra un dispositivo e l'altro, tra un'app nativa e un sito web o per trasferire grandi quantità di dati.

Funzionamento sicuro di Handoff

Con Handoff, quando i dispositivi iOS, iPadOS e macOS dell'utente sono vicini, l'utente può trasferire automaticamente ciò a cui sta lavorando da un dispositivo all'altro. Handoff permette all'utente di cambiare dispositivo continuando immediatamente a lavorare.

Quando l'utente accede a iCloud su un secondo dispositivo con funzionalità Handoff, i due dispositivi stabiliscono un abbinamento fuori banda con Bluetooth Low Energy (BLE) 4.2 utilizzando il servizio di notifiche push di Apple (APN). I messaggi individuali sono codificati come gli iMessage. Una volta completato l'abbinamento, ogni dispositivo genera una chiave simmetrica AES a 256 bit che viene archiviata nel portachiavi del dispositivo. Questa chiave può codificare e autenticare le trasmissioni BLE, che comunicano l'attività corrente del dispositivo ad altri dispositivi abbinati via iCloud utilizzando AES256 in modalità GCM, con misure di sicurezza contro i replay attack.

La prima volta che riceve una trasmissione da una nuova chiave, il dispositivo instaura una connessione BLE con il dispositivo di origine ed effettua uno scambio della chiave di codifica della trasmissione. Questa connessione è protetta grazie alla codifica standard Bluetooth Low Energy 4.2 e alla codifica dei singoli messaggi, in maniera simile a quanto avviene per i messaggi iMessage. In alcune situazioni, questi messaggi sono inviati tramite APN invece di BLE. Il payload dell'attività è protetto e trasferito come avviene per iMessage.

Handoff fra app native e siti web

Handoff consente alle app native per iOS, iPadOS e macOS di riprendere l'attività di un utente su una pagina web in domini legittimamente controllati dallo sviluppatore dell'app. Permette inoltre di riprendere in un browser l'attività svolta dall'utente nell'app nativa.

Per aiutare a impedire alle app native di riprendere i siti web non controllati dallo sviluppatore, l'app deve dimostrare di avere un legittimo controllo sui domini web in questione. Il controllo su un sito web si stabilisce attraverso il meccanismo utilizzato per le credenziali web condivise. Per maggiori dettagli, consulta Accesso delle app alle password salvate. Il sistema deve convalidare il controllo dell'app sul nome di dominio prima che sia consentito all'app di accettare l'attività dell'utente via Handoff.

La sorgente di una pagina web trasferita tramite Handoff può essere qualsiasi browser che abbia adottato le API di Handoff. Quando l'utente visualizza una pagina web, il sistema annuncia il nome di dominio della pagina nei byte di trasmissione codificati di Handoff. Solo gli altri dispositivi dell'utente possono decrittografare i byte di trasmissione.

Sul dispositivo ricevente, il sistema rileva che un'app nativa installata accetta il trasferimento Handoff dal nome di dominio annunciato e visualizza l'icona di quell'app nativa come opzione Handoff. Quando viene avviata, l'app nativa riceve l'URL completo e il titolo della pagina web. Fra il browser e l'app nativa non vengono trasferite altre informazioni.

Nella direzione opposta, un'app nativa può specificare un URL alternativo quando un dispositivo che riceve il trasferimento Handoff non dispone della stessa app. In questo caso il sistema visualizza il browser di default dell'utente come opzione Handoff (se tale browser ha adottato le API di Handoff). Quando si richiede il trasferimento Handoff, il browser viene avviato e riceve l'URL alternativo fornito dall'app sorgente. Non è necessario che l'URL alternativo rientri nei nomi di dominio controllati dallo sviluppatore dell'app nativa.

Handoff con volumi elevati di dati

Oltre alle funzionalità di base di Handoff, alcune app possono utilizzare API che supportano l'invio di un volume maggiore di dati attraverso una tecnologia Wi-Fi peer-to-peer creata da Apple (simile ad AirDrop). Ad esempio, l'app Mail utilizza queste API per consentire il trasferimento via Handoff di una bozza, che può contenere allegati di grandi dimensioni.

Quando un'app utilizza queste API, lo scambio fra i due dispositivi ha inizio proprio come in Handoff. Tuttavia, dopo aver ricevuto il payload iniziale via Bluetooth Low Energy (BLE), il dispositivo ricevente avvia una nuova connessione Wi-Fi. Tale connessione è crittografata (tramite TLS) e risulta affidabile grazie all'identità condivisa tramite il portachiavi iCloud. L'identità dei certificati verrà verificata confrontandoli con l'identità dell'utente. Su questa connessione codificata vengono quindi trasferiti ulteriori dati di payload fino a completare il trasferimento.

Appunti condivisi

Gli appunti condivisi si servono di Handoff per trasferire in modo sicuro il contenuto degli appunti tra i dispositivi, perché sia possibile copiare da un dispositivo e incollare su un altro. I contenuti sono protetti nello stesso modo degli altri dati di Handoff e vengono condivisi di default con gli appunti condivisi, salvo nel caso in cui lo sviluppatore decida di non consentire la condivisione.

Le app hanno accesso ai dati degli appunti a prescindere dal fatto che l'utente abbia incollato o meno gli appunti nell'app. Con gli appunti condivisi, l'accesso a tali dati viene esteso alle app presenti sugli altri dispositivi (associati allo stesso account iCloud).

Sicurezza dell'inoltro delle chiamate cellulari tramite iPhone

Quando il Mac, l'iPad o l'HomePod di un utente si trovano sulla stessa rete Wi-Fi di iPhone, possono essere utilizzati per effettuare e ricevere chiamate telefoniche tramite la connessione cellulare di iPhone. Per la configurazione è necessario che sui dispositivi sia stato effettuato l'accesso sia a iCloud che a FaceTime utilizzando lo stesso ID Apple.

Quando arriva una chiamata in entrata, tutti i dispositivi configurati ricevono una notifica tramite il servizio di notifiche push di Apple (APN). Ogni notifica utilizzerà la stessa codifica end-to-end di iMessage. I dispositivi che sono sulla stessa rete mostrano l'interfaccia utente di notifica di chiamata in entrata. Quando l'utente risponde, l'audio viene trasmesso direttamente da iPhone utilizzando una connessione peer-to-peer sicura fra i due dispositivi.

Quando l'utente risponde a una chiamata su uno dei dispositivi, i dispositivi nelle vicinanze abbinati tramite iCloud smettono di suonare dopo una breve trasmissione mediante Bluetooth Low Energy (BLE). I byte di tale notifica sono codificati con lo stesso metodo con cui vengono annunciati i trasferimenti di Handoff.

Anche le chiamate in uscita vengono inoltrate a iPhone tramite APN e l'audio viene trasmesso nella stessa maniera sul collegamento peer-to-peer sicuro fra i dispositivi. Gli utenti possono disabilitare l'inoltro delle chiamate disattivando l'opzione "Chiamate cellulare iPhone" nelle impostazioni di FaceTime.

Sicurezza dell'inoltro dei messaggi di testo tramite iPhone

L'inoltro dei messaggi di testo invia automaticamente i messaggi di testo ricevuti su iPhone al Mac o all'iPad registrati dell'utente. Su ogni dispositivo deve essere stato effettuato l'accesso al servizio iMessage utilizzando lo stesso ID Apple. Quando l'inoltro dei messaggi di testo è attivato e l'autenticazione a due fattori è abilitata, la registrazione dei dispositivi che fanno parte della cerchia di attendibilità dell'utente è automatica. Altrimenti, la registrazione viene verificata su ogni dispositivo inserendo un codice numerico casuale a sei cifre generato da iPhone.

Una volta collegati i dispositivi, iPhone provvede a codificare gli SMS in entrata e li inoltra a ciascun dispositivo, utilizzando i metodi descritti in Panoramica sulla sicurezza di iMessage. Le risposte sono inviate nuovamente a iPhone utilizzando lo stesso metodo, quindi iPhone le invia come messaggi di testo attraverso il meccanismo di trasmissione SMS del gestore. La funzionalità "Inoltro SMS" può essere disattivata nelle impostazioni di Messaggi.

Sicurezza di Instant Hotspot

Instant Hotspot connette gli altri dispositivi Apple a un hotspot personale di iPhone o iPad. Gli iPhone e iPad che supportano Instant Hotspot utilizzano la tecnologia Bluetooth Low Energy (BLE) per rilevare tutti i dispositivi su cui è stato effettuato l'accesso allo stesso account iCloud individuale o ad account utilizzati con "In famiglia" (in iOS 13 e iPadOS) e comunicare con loro. I Mac compatibili dotati di OS X 10.10 o versione successiva utilizzano la stessa tecnologia per rilevare e comunicare con i dispositivi iPhone e iPad con Instant Hotspot.

Inizialmente, quando un utente inserisce le impostazioni Wi-Fi su un dispositivo, quest'ultimo emette una trasmissione BLE che contiene un identificatore concordato tra tutti i dispositivi su cui è stato effettuato l'accesso allo stesso account iCloud. L'identificatore è generato da un DSID (Destination Signaling Identifier) legato all'account iCloud e prevede una rotazione periodica. Se nelle vicinanze ci sono altri dispositivi su cui è stato effettuato l'accesso allo stesso account iCloud e che supportano l'hotspot personale, questi rilevano il segnale e rispondono indicando la loro disponibilità a utilizzare Instant Hotspot.

Quando un utente che non fa parte di "In famiglia" sceglie un iPhone o iPad, viene inviata una richiesta di attivazione dell'hotspot personale a quel dispositivo. La richiesta viaggia su un collegamento protetto dalla codifica BLE ed è codificata in modo simile a quanto avviene per iMessage. Il dispositivo risponde quindi sullo stesso collegamento BLE utilizzando lo stesso tipo di codifica per messaggio e fornendo le informazioni sulla connessione con l'hotspot personale.

Per gli utenti che fanno parte di "In famiglia", le informazioni per la connessione all'hotspot personale vengono condivise in maniera sicura tramite un meccanismo simile a quello utilizzato dai dispositivi HomeKit per sincronizzare le informazioni. Nello specifico, la connessione che condivide le informazioni dell'hotspot tra gli utenti è protetta da una chiave effimera ECDH (Curve25519) che viene autenticata con le rispettive chiavi pubbliche Ed25519 specifiche per il dispositivo degli utenti. Le chiavi pubbliche utilizzate sono quelle che erano state sincronizzate in precedenza tra i membri di "In famiglia" tramite il servizio Apple Identity Service (IDS) nel momento in cui è stato stabilito il gruppo familiare.

Sicurezza della rete

Panoramica sulla sicurezza della rete

Oltre alle misure di sicurezza integrate messe in pratica da Apple per proteggere i dati archiviati sui dispositivi Apple, le aziende possono implementarne molte altre per ottenere un grado maggiore di protezione delle informazioni che vengono trasmesse da e verso un dispositivo. Tutte queste misure di protezione e sicurezza fanno parte della sicurezza della rete.

Dal momento che gli utenti devono poter accedere alle reti aziendali da qualunque parte del mondo, è importante assicurarsi che siano autorizzati a farlo e che durante la trasmissione i loro dati siano protetti. iOS, iPadOS e macOS integrano tecnologie collaudate e gli ultimi standard per raggiungere questi obiettivi di sicurezza, sia per le connessioni a reti Wi-Fi che per quelle a reti dati cellulari. Per questo motivo i nostri sistemi operativi utilizzano e mettono a disposizione degli sviluppatori protocolli di rete standard per comunicazioni autenticate, autorizzate e codificate.

Sicurezza del protocollo TLS

iOS, iPadOS e macOS supportano Transport Layer Security (TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3) e Datagram Transport Layer Security (DTLS). Il protocollo TLS supporta sia AES128 che AES256 e favorisce l'uso di suite di cifratura con forward secrecy. App che fanno uso di internet come Safari, Calendario e Mail utilizzano automaticamente questo protocollo per ottenere un canale di comunicazione codificato tra il dispositivo e i servizi di rete. Le API di alto livello (come CFNetwork) rendono facile l'adozione di TLS nelle app da parte degli sviluppatori, mentre quelle di basso livello (come Network.framework) forniscono un controllo dettagliato. CFNetwork non consente l'uso di SSL 3 e alle app che utilizzano WebKit (come Safari) non è consentito stabilire connessioni SSL 3.

In iOS 11 o versioni successive e macOS 10.13 o versioni successive, i certificati SHA-1 non sono più consentiti per le connessioni TLS, a meno che non siano segnalati come attendibili dall'utente. Inoltre, non sono consentiti neanche i certificati con chiavi RSA inferiori ai 2048 bit. La suite di cifratura simmetrica RC4 è sconsigliata in iOS 10 e macOS 10.12. Di default, i client o server TLS sui cui sono implementate le API SecureTransport non hanno le suite di cifratura RC4 abilitate e non possono connettersi quando RC4 è l'unica suite di cifratura disponibile. Per sicurezza, i servizi e le app che richiedono RC4 devono essere aggiornati per potere utilizzare le suite di cifratura più sicure. In iOS 12.1, i certificati emessi dopo il 15 ottobre 2018 da un certificato root considerato attendibile dal sistema devono essere inseriti in un log attendibile per la trasparenza dei certificati affinché possano effettuare connessioni TLS. In iOS 12.2, TLS 1.3 è abilitato di default per Network.framework e per le API NSURLSession. I client TLS che utilizzano le API SecureTransport non possono utilizzare TLS 1.3.

Sicurezza dei trasferimenti delle app

App Transport Security garantisce requisiti di connessione di default che assicurano il rispetto da parte delle app delle linee guida per le connessioni sicure durante l'utilizzo delle API NSURLConnection, CFURL o NSURLSession. Di default, App Transport Security limita la selezione della cifratura alle suite che forniscono forward secrecy, in particolare:

- ECDHE_ECDSA_AES e ECDHE_RSA_AES in modalità Galois/Counter (GCM)
- Modalità Cipher Block Chaining (CBC)

Le app sono in grado di disabilitare il requisito di forward secrecy per dominio; in quel caso, RSA_AES viene aggiunto all'insieme delle cifrature disponibili.

I server devono supportare TLS 1.2 e il forward secrecy; i certificati devono essere validi e firmati tramite funzioni uguali o superiori a SHA256 con chiavi uguali o superiori a RSA a 2048 bit o a curva ellittica a 256 bit.

Le connessioni di rete che non soddisfano tali requisiti non verranno stabilite, a meno che l'app non ignori App Transport Security. La presenza di certificati non validi comporta sempre un'interruzione forzata e un blocco della connessione. App Transport Security viene applicato automaticamente alle app realizzate per iOS 9 o successivo e macOS 10.11 o versione successiva.

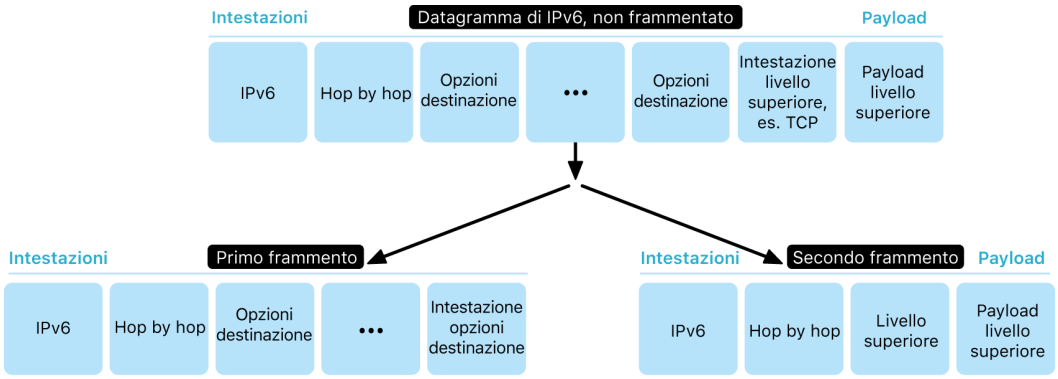
Controllo della convalida dei certificati

La verifica dello stato di attendibilità di un certificato TLS viene effettuata secondo standard di settore stabiliti, così come illustrato nella RFC 5280, e incorpora standard emergenti come quelli della RFC 6962 (trasparenza dei certificati). In iOS 11 o versione successiva e in macOS 10.13 o versione successiva, i dispositivi Apple vengono aggiornati periodicamente in base a un elenco attuale di certificati revocati e limitati. L'elenco è estrapolato dagli elenchi di revoca dei certificati (CRL), che vengono pubblicati da ognuna delle autorità di certificazione principali ritenute attendibili da Apple e dalle loro entità emittenti CA subordinate. L'elenco potrebbe includere anche altre restrizioni a discrezione di Apple. Queste informazioni sono consultate ogni volta che viene usata una funzione API di rete per stabilire una connessione protetta. Qualora i certificati revocati fossero troppi per essere elencati individualmente da una CA, il controllo per la convalida potrebbe invece richiedere una risposta in linea sullo stato del certificato (OCSP) e restituire esito negativo se tale risposta non è disponibile.

Sicurezza di IPv6

Tutti i sistemi operativi Apple supportano IPv6, implementando vari meccanismi per proteggere la privacy degli utenti e la stabilità della rete. Quando viene usata la configurazione automatica senza stato (SLAAC), gli indirizzi IPv6 di tutte le interfacce sono generati in un modo che aiuta a impedire il tracciamento dei dispositivi sulla rete e al tempo stesso consente una buona esperienza utente garantendo la stabilità degli indirizzi quando non vengono effettuate modifiche alla rete. L'algoritmo di generazione degli indirizzi si basa su un processo crittografico secondo lo standard RFC 3972, migliorato da un modificatore specifico per ogni interfaccia che garantisce che persino le varie interfacce sulla stessa rete abbiano indirizzi diversi. Inoltre vengono creati indirizzi temporanei con una durata preferita di 24 ore e questi vengono usati di default per ogni nuova connessione. Coerentemente con la funzionalità "Indirizzo Wi-Fi privato" introdotta in iOS 14, iPadOS 14, watchOS 7, per ogni rete Wi-Fi a cui un dispositivo accede viene generato un indirizzo link-local unico. Successivamente, il SSID della rete verrà incorporato come ulteriore elemento per la generazione dell'indirizzo, in maniera analoga al parametro Network_ID dello standard RFC 7217. Questo approccio è utilizzato in iOS 14, iPadOS 14 e watchOS 7.

Per proteggere da attacchi basati sulle intestazioni di estensione e sulla frammentazione di iPv6, i dispositivi Apple implementano le misure di protezione specificate negli standard RFC 6980, RFC 7112 e RFC 8021. Essi impediscono, insieme ad altre misure, attacchi in cui il livello superiore dell'intestazione può essere trovato solo nel secondo frammento (come mostrato di seguito), che a sua volta può causare ambiguità per i controlli di sicurezza come il filtro dei pacchetti senza stato.



Inoltre, per aiutare a garantire l'affidabilità dello stack IPv6 nei sistemi operativi Apple, i dispositivi Apple impongono vari limiti sulle strutture di dati relative a IPv6, come il numero di prefissi per interfaccia.

Sicurezza delle reti private virtuali (VPN)

I servizi per la protezione delle reti come le VPN solitamente richiedono una configurazione minima per funzionare con iPhone, iPad, and Mac.

Protocolli supportati

Tali dispositivi funzionano con i server VPN che supportano i seguenti protocolli e metodi di autenticazione:

- IKEv2/IPsec con autenticazione tramite segreto condiviso, certificati RSA, certificati ECDSA (Elliptic Curve Digital Signature Algorithm), EAP-MSCHAPv2 o EAP-TLS.
- SSL-VPN con l'app client adeguata scaricata da App Store.
- L2TP/IPsec con autenticazione utente tramite password MS-CHAPV2 e autenticazione automatica tramite segreto condiviso (iOS, iPadOS e macOS) e RSA SecurID o CRYPTOCard (solo macOS).
- Cisco IPsec con autenticazione utente tramite password, RSA SecurID o CRYPTOCard e autenticazione automatica mediante segreto condiviso e certificati (solo macOS).

Tipologie di VPN supportate

iOS, iPadOS e macOS supportano:

- *VPN On Demand:* per reti che usano l'autenticazione basata sui certificati. Le politiche IT specificano quali sono i domini che richiedono una connessione VPN utilizzando un apposito profilo di configurazione.
- *VPN per app:* per facilitare le connessioni VPN su base molto più dettagliata. Le soluzioni MDM possono specificare una connessione per ogni app gestita e/o domini specifici di Safari. Questa funzione garantisce che i dati protetti passino sempre attraverso le reti aziendali, a differenza dei dati personali dell'utente.

iOS e iPadOS supportano:

- *VPN sempre attiva:* per i dispositivi gestiti tramite una soluzione MDM e supervisionati utilizzando Apple Configurator per Mac, Apple School Manager, Apple Business Manager o Apple Business Essentials. In questo modo l'utente non dovrà più attivare la VPN per abilitare la protezione quando si connette a reti cellulari o Wi-Fi. Inoltre, la VPN sempre attiva fa in modo che l'azienda abbia il pieno controllo sul traffico dei dispositivi, attraverso il tunneling di tutto il traffico IP verso l'azienda. Lo scambio di parametri e chiavi di default per la codifica successiva, IKEv2, protegge la trasmissione del traffico con la crittografia dei dati. L'azienda può dunque monitorare e filtrare il traffico tra i dispositivi, proteggere i dati all'interno della propria rete e limitare l'accesso a internet dei dispositivi.

Sicurezza del Wi-Fi

Accesso sicuro alle reti wireless

Tutte le piattaforme Apple supportano i protocolli di codifica e autenticazione Wi-Fi standard nel settore, per fornire accesso autenticato e privacy durante le connessioni alle seguenti reti wireless protette:

- WPA2 Personal
- WPA2 Enterprise
- WPA2/WPA3 Transitional
- WPA3 Personal
- WPA3 Enterprise
- WPA3 Enterprise con sicurezza a 192 bit

WPA2 e WPA3 autenticano ogni connessione e forniscono codifica AES a 128 bit per aiutare a garantire la confidenzialità dei dati inviati in modalità wireless. Questo metodo di codifica fornisce il massimo livello di protezione dei dati durante l'invio e la ricezione di comunicazioni attraverso una connessione di rete Wi-Fi.

Supporto per WPA3

Il protocollo WPA3 è supportato dai seguenti dispositivi Apple:

- iPhone 7 o modelli successivi
- iPad di quinta generazione o modelli successivi
- Apple TV 4K o modelli successivi
- Apple Watch Series 3 o modelli successivi
- Computer Mac (fine del 2013 o modelli successivi, con 802.11ac o versioni successive)

I dispositivi più recenti supportano l'autenticazione con il protocollo di sicurezza WPA3 Enterprise a 192 bit, compreso il supporto per la codifica AES a 256 bit durante la connessione a punti di accesso wireless compatibili (APS). Questa crittografia fornisce una protezione ancora maggiore in termini di confidenzialità dei dati inviati in modalità wireless. La sicurezza WPA3 Enterprise a 192 bit è supportata su tutti i modelli di iPhone 11 o successivi, sui modelli di iPad a partire dalla 7ª generazione e su tutti i Mac dotati di chip Apple.

Supporto per PMF

Oltre a proteggere i dati inviati in modalità wireless, le piattaforme Apple ampliano i livelli di protezione WPA2 e WPA3 a frame di gestione unicast e multicast tramite il servizio PMF (Protected Management Frame) definito nell'802.11w. Il supporto PMF è disponibile sui seguenti dispositivi Apple:

- iPhone 6 o modelli successivi
- iPad Air 2 o modelli successivi
- Apple TV HD o modelli successivi
- Apple Watch Series 3 o modelli successivi
- Computer Mac (fine del 2013 o modelli successivi, con 802.11ac o versioni successive)

Grazie al supporto di 802.1X, i dispositivi Apple possono essere integrati in un'ampia gamma di ambienti di autenticazione RADIUS. I metodi di autenticazione wireless 802.1X supportati comprendono: EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 e PEAPv1.

Protezioni delle piattaforme

I sistemi operativi Apple proteggono i dispositivi dalle vulnerabilità del firmware del processore di rete. Ciò significa che i controller di rete con Wi-Fi hanno accesso limitato alla memoria del processore per le applicazioni.

- Quando la comunicazione con il processore di rete avviene tramite le interfacce USB o SDIO (Secure Digital Input Output), il processore di rete non può instaurare transazioni DMA (Direct Memory Access) con il processore per le applicazioni.
- Quando viene utilizzata l'interfaccia PCIe, ciascun processore di rete si trova sul proprio bus PCIe isolato. Un'unità per la gestione della memoria di input/output su ciascun bus PCIe limita ulteriormente l'accesso DMA del processore solo alla memoria e alle risorse contenenti i pacchetti della rete e le strutture di controllo.

Protocolli obsoleti

I prodotti Apple supportano i seguenti protocolli di codifica e autenticazione Wi-Fi obsoleti:

- WEP aperto, con chiavi a 40 bit e 104 bit
- WEP condiviso, con chiavi a 40 bit e 104 bit
- WEP dinamico
- TKIP (Temporal Key Integrity Protocol)
- WPA
- WPA/WPA2 Transitional

Questi protocolli non sono più considerati sicuri e il loro uso è fortemente sconsigliato per motivi di compatibilità, affidabilità, prestazioni e sicurezza. Sono supportati unicamente a scopo di retrocompatibilità e potrebbero essere rimossi nelle future versioni del software.

Per tutte le implementazioni Wi-Fi, si consiglia di eseguire la migrazione a WPA3 Personal o WPA3 Enterprise per ottenere connessioni Wi-Fi quanto più possibile solide, sicure e compatibili.

Privacy Wi-Fi

Indirizzi MAC casuali

Quando analizzano la connessione Wi-Fi senza essere associati a una rete Wi-Fi, le piattaforme Apple utilizzano un indirizzo MAC (Media Access Control) casuale. Tale analisi può essere effettuata per trovare la rete Wi-Fi conosciuta a cui connettersi oppure per aiutare la localizzazione per le app che utilizzano i perimetri virtuali (geofence), come i promemoria basati sulla posizione, o per correggere una posizione in Mappe di Apple. Le analisi Wi-Fi che si verificano durante il tentativo di connessione a una rete Wi-Fi preferita non avvengono tramite indirizzi casuali. Gli indirizzi MAC Wi-Fi casuali sono supportati su iPhone 5 o modelli successivi.

Le piattaforme Apple utilizzano un indirizzo MAC casuale anche durante le scansioni ePNO (enhanced Preferred Network Offload) quando un dispositivo non è associato a una rete Wi-Fi o il suo processore è in stop. Le scansioni ePNO sono eseguite quando il dispositivo utilizza la localizzazione per le app che usano perimetri virtuali (geofence), come ad esempio i promemoria basati sulla posizione che determinano se il dispositivo si trova nei pressi di un luogo specifico.

Considerando che l'indirizzo MAC di un dispositivo cambia se il dispositivo viene disconnesso da una rete Wi-Fi, non potrà essere utilizzato per seguire continuamente la posizione di un dispositivo da parte di osservatori passivi del traffico Wi-Fi, nemmeno quando il dispositivo è connesso a una rete cellulare. Apple ha informato i produttori di Wi-Fi che le scansioni di iOS e iPadOS utilizzano indirizzi MAC casuali, che non possono essere predetti né da Apple né dai produttori.

In iOS 14 o versioni successive, iPadOS 14 o versioni successive e watchOS 7 o versioni successive, quando iPhone, iPad o Apple Watch si connettono a una rete Wi-Fi, si identificano con un indirizzo MAC unico (casuale) diverso per ciascuna rete. Questa funzionalità può essere disabilitata dall'utente o tramite una nuova opzione nel payload Wi-Fi. In alcune circostanze, il dispositivo tornerà ad avere il proprio effettivo indirizzo MAC.

Per ulteriori informazioni, consulta l'articolo del supporto Apple Usare indirizzi Wi-Fi privati su iPhone, iPad e Apple Watch.

Numeri progressivi casuali dei frame Wi-Fi

I frame Wi-Fi includono un numero progressivo, utilizzato dal protocollo di basso livello 802.11 per abilitare comunicazioni Wi-Fi efficienti e affidabili. Questi numeri progressivi aumentano su ogni frame trasmesso, quindi potrebbero essere utilizzati per mettere in correlazione alcune informazioni trasmesse durante le scansioni Wi-Fi, con altri frame trasmessi dallo stesso dispositivo.

Per proteggere l'utente da questa eventualità, ogni volta che un indirizzo MAC viene modificato in un nuovo indirizzo casuale i dispositivi Apple generano dei numeri progressivi casuali. Anche per ogni nuova richiesta di scansione avviata mentre il dispositivo non è associato vengono quindi generati dei numeri progressivi casuali. Questo comportamento è supportato dai seguenti dispositivi:

- iPhone 7 o successivo
- iPad di quinta generazione o successivo
- Apple TV 4K o successiva
- Apple Watch Series 3 o successivo
- iMac Pro (Retina 5K, 27", 2017) o successivo
- MacBook Pro (13", 2018) o successivo
- MacBook Pro (15", 2018) o successivo
- MacBook Air (Retina, 13", 2018) o successivo
- Mac mini (2018) o successivo
- iMac (Retina 4K, 21,5", 2019) o successivo
- iMac (Retina 5K, 27", 2019) o successivo
- Mac Pro (2019) o successivo

Connessioni Wi-Fi

Apple genera indirizzi MAC casuali per le connessioni Wi-Fi peer-to-peer utilizzate per AirDrop e AirPlay. Inoltre, vengono utilizzati indirizzi MAC casuali anche per l'hotspot personale su iOS e iPadOS (con scheda SIM) nonché per la condivisione internet su macOS.

Ogni volta che vengono avviate queste interfacce, vengono generati degli indirizzi casuali; tali indirizzi sono unici e generati in modo indipendente per ogni interfaccia.

Reti nascoste

Le reti Wi-Fi vengono identificate in base al loro nome di rete, noto con la sigla *SSID (Service Set Identifier)*. Alcune reti Wi-Fi sono configurate per nascondere il proprio SSID; il punto di accesso wireless non trasmette quindi il nome di queste reti. Sono conosciute come *reti nascoste*. iPhone 6s e modelli successivi rilevano automaticamente se una rete è nascosta. Se una rete è nascosta, il dispositivo iOS o iPadOS invia un probe con il SSID incluso nella richiesta. Questo aiuta a impedire al dispositivo di trasmettere il nome delle reti nascoste a cui si è connesso in precedenza un utente, a ulteriore protezione della privacy.

Sicurezza del Bluetooth

Esistono due tipi di Bluetooth nei dispositivi Apple: Bluetooth Classic e Bluetooth Low Energy (BLE). Il modello di sicurezza Bluetooth per entrambe le versioni include le seguenti funzionalità di sicurezza specifiche:

- *Abbinamento:* il processo per la creazione di una o più chiavi di segreti condivisi.
- *Bonding:* l'atto di archiviare le chiavi create durante l'abbinamento in modo che possano essere utilizzate in connessioni successive per formare un abbinamento con un dispositivo autorizzato.
- *Autenticazione:* verifica dell'esistenza delle stesse chiavi sui due dispositivi.
- *Codifica:* confidenzialità dei messaggi.
- *Integrità dei messaggi:* protezione dalle falsificazioni dei messaggi.
- *Secure Simple Pairing:* protezione dalle intercettazioni passive e dagli attacchi MITM.

Nel Bluetooth versione 4.1 è stata aggiunta la funzionalità "Secure Connections" alla trasmissione fisica Bluetooth Classic (BR/EDR).

Le funzionalità di sicurezza per ogni tipo di Bluetooth sono elencate di seguito.

Supporto	**Bluetooth Classic**	**Bluetooth Low Energy**
Abbinamento	Curva ellittica P-256	Algoritmi conformi al FIPS (curva ellittica P-256 e AES-CMAC)
Bonding	Informazioni di abbinamento archiviate in una posizione sicura sui dispositivi iOS, iPadOS, macOS, tvOS e watchOS	Informazioni di abbinamento archiviate in una posizione sicura sui dispositivi iOS, iPadOS, macOS, tvOS e watchOS
Autenticazione	Algoritmi conformi al FIPS (HMAC-SHA256 e AES-CTR)	Algoritmi conformi al FIPS
Codifica	Codifica AES-CCM eseguita nel controller	Codifica AES-CCM eseguita nel controller
Integrità dei messaggi	AES-CCM, utilizzato per l'integrità dei messaggi	AES-CCM, utilizzato per l'integrità dei messaggi
Secure Simple Pairing: protezione dalle intercettazioni passive	Scambio su curve ellittiche Diffie-Hellman con chiavi effimere (ECDHE)	Scambio su curve ellittiche Diffie-Hellman (ECDHE)
Secure Simple Pairing: protezione dagli attacchi man-in-the-middle	Due metodi numerici con intervento dell'utente: confronto numerico o voce codice	Due metodi numerici con intervento dell'utente: confronto numerico o voce codice Gli abbinamenti, incluse tutte le modalità non man-in-the-middle, richiedono una risposta dell'utente

Supporto	Bluetooth Classic	Bluetooth Low Energy
Bluetooth 4.1 o versione successiva	iMac usciti alla fine del 2015 o modelli successivi MacBook Pro usciti all'inizio del 2015 o modelli successivi	iOS 9 o versione successiva iPadOS 13.1 o versione successiva macOS 10.12 o versione successiva tvOS 9 o versione successiva watchOS 2.0 o versione successiva
Bluetooth 4.2 o versione successiva	iPhone 6 o modelli successivi	iOS 9 o versione successiva iPadOS 13.1 o versione successiva macOS 10.12 o versione successiva tvOS 9 o versione successiva watchOS 2.0 o versione successiva

Privacy con Bluetooth Low Energy

Per contribuire alla protezione della privacy dell'utente, BLE include le due seguenti funzionalità: indirizzi casuali e derivazione delle chiavi cross-transport.

Gli *indirizzi casuali* riducono la possibilità di tracciamento di un dispositivo BLE durante un periodo di tempo modificando spesso l'indirizzo del dispositivo Bluetooth. Perché un dispositivo utilizzi la funzionalità di privacy per riconnettersi ai dispositivi noti, l'indirizzo del dispositivo, denominato *indirizzo privato*, deve essere risolvibile dall'altro dispositivo. L'indirizzo privato è generato tramite la chiave per la risoluzione dell'identità del dispositivo scambiata durante il processo di abbinamento.

iOS 13 o versioni successive e iPadOS 13.1 o versioni successive hanno una funzionalità per le chiavi di collegamento chiamata *derivazione delle chiavi cross-transport*. Per esempio, una chiave di collegamento generata con BLE può essere utilizzata per derivare una chiave di collegamento Bluetooth Classic. Inoltre, Apple ha aggiunto il Bluetooth Classic al supporto BLE per i dispositivi che supportano la funzionalità "Secured Connections" introdotta nella versione 4.1 delle specifiche Bluetooth (consulta le specifiche Bluetooth 5.1).

Sicurezza della banda ultralarga in iOS

Il nuovo chip U1 di Apple usa la tecnologia a banda ultralarga per la consapevolezza spaziale, che consente a iPhone 11, iPhone 11 Pro e iPhone 11 Pro Max o modelli successivi di iPhone di individuare con precisione altri dispositivi Apple dotati di chip U1. La tecnologia a banda ultralarga usa la stessa tecnologia utilizzata in altri dispositivi Apple compatibili per rendere casuali i dati:

- Indirizzi MAC casuali
- Numeri progressivi casuali dei frame Wi-Fi.

Sicurezza del Single Sign-On

Single Sign-On

iOS e iPadOS supportano l'autenticazione alle reti aziendali attraverso SSO (Single Sign-On). Il SSO funziona con le reti basate su Kerberos per autenticare gli utenti ai servizi a cui sono stati autorizzati ad accedere. La tecnologia SSO può essere utilizzata per una serie di attività di rete, che spazia dalle sessioni sicure di Safari alle app di terze parti. È inoltre supportata l'autenticazione basata su certificati (come PKINIT).

macOS supporta l'autenticazione alle reti aziendali tramite Kerberos. Le app possono usare Kerberos per autenticare gli utenti ai servizi a cui sono stati autorizzati ad accedere. Kerberos può essere utilizzato inoltre per una serie di attività di rete, che spazia dalle sessioni sicure di Safari e l'autenticazione dei file system di rete alle app di terze parti. È supportata anche l'autenticazione che si basa sui certificati, tuttavia è richiesta l'adozione di un'API dello sviluppatore.

La tecnologia SSO di iOS, iPadOS e macOS usa i token SPNEGO e il protocollo HTTP Negotiate, grazie ai quali può lavorare con gateway di autenticazione basati su Kerberos e sistemi con autenticazione integrata di Windows che supportano i ticket Kerberos. Il supporto di SSO si basa sul progetto open source Heimdal.

In iOS, iPadOS e macOS sono supportati i seguenti tipi di codifica:

- AES-128-CTS-HMAC-SHA1-96
- AES-256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Safari supporta SSO e anche le app di terze parti che usano API di networking iOS e iPadOS standard possono essere configurate per poter utilizzare questa tecnologia. Per la configurazione SSO, iOS e iPadOS supportano un payload di un profilo di configurazione che consente alle soluzioni per la gestione dei dispositivi mobili (MDM) di scaricare le impostazioni necessarie. Si tratta dunque di impostare il nome principale dell'utente (cioè, l'account utente Active Directory), le impostazioni dell'area di autenticazione di Kerberos e di indicare le app e gli URL di Safari a cui è consentito l'uso del SSO.

Extensible Single Sign-On

Gli sviluppatori di app possono fornire le proprie implementazioni della tecnologia Single Sign-On tramite estensioni SSO. Tali estensioni vengono invocate quando un'app nativa o web deve utilizzare dei provider di identità per l'autenticazione dell'utente. Gli sviluppatori possono fornire due tipi di estensioni: quelle che reindirizzano a HTTPS e quelle che usano il meccanismo di richiesta/risposta come Kerberos. In questo modo gli schemi di autenticazione di OpenID, OAuth, SAML2 e Kerberos possono essere supportati da Extensible Single Sign-On. Le estensioni SSO possono anche supportare l'autenticazione di macOS adottando un protocollo SSO nativo, che consente di ricevere token SSO durante il login a macOS.

Per usare un'estensione Single Sign-On, un'app può utilizzare l'API AuthenticationServices oppure confidare nel meccanismo di intercettazione dell'URL offerto dal sistema operativo. WebKit e CFNetwork forniscono un livello di intercettazione che consente il pieno supporto SSO per ogni app nativa o WebKit. Perché sia invocata un'estensione SSO, occorre installare tramite un profilo MDM una configurazione fornita da un amministratore. Inoltre, le estensioni di reindirizzamento devono utilizzare il payload "Domini associati" per provare che il server di identità che supportano è consapevole della loro esistenza.

L'unica estensione fornita dal sistema operativo è SSO Kerberos.

Sicurezza di AirDrop

I dispositivi Apple che supportano AirDrop usano Bluetooth Low Energy (BLE) e la tecnologia Wi-Fi peer-to-peer creata da Apple per inviare file e informazioni ai dispositivi nelle vicinanze, compresi i dispositivi iOS e iPad con iOS 7 o versione successiva e i computer Mac con OS X 10.11 o versione successiva che usano AirDrop. Il segnale Wi-Fi è usato per comunicare direttamente tra i dispositivi senza necessità di una connessione internet o di un punto di accesso (AP) wireless. Questa connessione è codificata tramite TLS.

AirDrop è impostato di default per la condivisione con "Solo contatti". Gli utenti possono inoltre decidere se utilizzare AirDrop per la condivisione con tutti oppure se disattivare completamente tale funzione. Le organizzazioni possono limitare l'utilizzo di AirDrop per i dispositivi o le app gestite tramite una soluzione di gestione dei dispositivi mobili (MDM).

Funzionamento di AirDrop

AirDrop usa i servizi iCloud per aiutare gli utenti ad autenticarsi. Quando un utente accede ad iCloud, sul dispositivo viene archiviata un'identità RSA a 2048 bit e, quando l'utente attiva AirDrop, viene creato un hash di identità breve di AirDrop, basato sull'indirizzo email e sui numeri di telefono associati all'ID Apple dell'utente.

Quando un utente sceglie AirDrop come metodo di condivisione di un elemento, il dispositivo da cui viene effettuato l'invio emette un segnale AirDrop attraverso BLE che include l'hash di identità breve di AirDrop dell'utente. Altri dispositivi Apple che sono attivi, nelle vicinanze e con AirDrop attivo rilevano il segnale e rispondono tramite Wi-Fi peer-to-peer, in modo che il dispositivo da cui viene effettuato l'invio possa scoprire l'identità di qualsiasi dispositivo che risponde.

Nella modalità "Solo contatti", l'hash di identità breve di AirDrop ricevuto viene confrontato con quelli delle persone presenti nell'app Contatti del dispositivo ricevente. Se viene trovata una corrispondenza, il dispositivo ricevente risponde tramite Wi-Fi peer-to-peer con le proprie informazioni identificative. Se non viene trovata nessuna corrispondenza, il dispositivo non risponde.

Nella modalità Tutti, il processo è analogo, tuttavia il dispositivo ricevente risponde anche se non viene trovata nessuna corrispondenza nell'app Contatti.

Il dispositivo da cui viene effettuato l'invio inizia quindi una connessione AirDrop tramite Wi-Fi peer-to-peer e, tramite questa connessione, invia un hash di identità lungo al dispositivo ricevente. Se l'hash di identità lungo corrisponde a quello di una persona conosciuta nei contatti del ricevente, quest'ultimo risponde con i propri hash di identità lunghi.

Se gli hash sono verificati, nella finestra di condivisione di AirDrop del mittente vengono visualizzati il nome e la foto del destinatario (se presenti in Contatti). In iOS e iPadOS, sono mostrati nella sezione Persone o Dispositivi. I dispositivi che non sono verificati o autenticati vengono mostrati nella schermata di condivisione di AirDrop del mittente con l'icona e il nome del dispositivo come definito in Impostazioni > Generali > Info > Nome. In iOS e iPadOS, si trovano nella sezione "Altre persone" del pannello di condivisione di AirDrop.

L'utente che invia può quindi decidere con chi effettuare la condivisione. Dopo aver selezionato l'utente, il dispositivo di invio avvia una connessione codificata (TLS) con il dispositivo ricevente e avviene lo scambio dei rispettivi certificati di identità iCloud. L'identità nei certificati è verificata confrontando le informazioni con i dati presenti nell'app Contatti di ogni utente.

Se i certificati vengono verificati, all'utente che riceve viene chiesto di accettare il trasferimento in entrata dall'utente o dal dispositivo identificati. Se sono stati selezionati più destinatari, questo processo viene ripetuto per ogni destinatario.

Sicurezza della condivisione della password Wi-Fi su iPhone e iPad

Gli iPhone e gli iPad che supportano la condivisione della password Wi-Fi utilizzano un meccanismo simile a AirDrop per inviare una password Wi-Fi da un dispositivo a un altro.

Quando un utente seleziona una rete Wi-Fi (richiedente) e viene richiesta la password Wi-Fi, il dispositivo Apple avvia una ricerca tramite Bluetooth Low Energy (BLE) indicando che necessita della password Wi-Fi. Gli altri dispositivi Apple che sono attivi, nelle immediate vicinanze e che dispongono della password per la rete Wi-Fi selezionata si connettono tramite BLE al dispositivo richiedente.

Il dispositivo con la password Wi-Fi (concedente) chiede le informazioni di contatto del richiedente, che deve dimostrare la propria identità tramite un meccanismo simile a AirDrop. Una volta provata l'identità, il concedente invia al richiedente il codice che può essere utilizzato per accedere alla rete.

Le organizzazioni possono limitare l'utilizzo della condivisione di password Wi-Fi per i dispositivi o le app gestite tramite una soluzione di gestione dei dispositivi mobili (MDM).

Sicurezza del firewall in macOS

macOS include un firewall integrato per proteggere il Mac dall'accesso di rete e dagli attacchi DoS. Può essere configurato in Impostazioni di Sistema > Privacy e sicurezza (macOS 13 o versioni successive), nel pannello Sicurezza e Privacy di Preferenze di Sistema (macOS 12 o versioni precedenti) oppure utilizzando un profilo di configurazione con il payload Firewall installato manualmente o fornito da una soluzione MDM. Sono supportate le seguenti configurazioni:

- Impedisce tutte le connessioni in entrata, indipendentemente dall'app.
- Consente automaticamente al software integrato di ricevere le connessioni in entrata.
- Consente automaticamente al software attendibile scaricato di ricevere le connessioni in entrata.
- Aggiunge o rifiuta l'accesso in base alle app specificate dall'utente.
- Impedisce al Mac di rispondere a richieste ICMP (Internet Control Message Protocol) e a richieste di port scanning.

Sicurezza del kit per sviluppatori

Panoramica sulla sicurezza del kit per sviluppatori

Apple fornisce diversi framework per consentire agli sviluppatori di terze parti di ampliare i servizi Apple. Tali framework sono progettati mettendo al centro la privacy e la sicurezza degli utenti:

- HomeKit
- CloudKit
- SiriKit
- WidgetKit
- DriverKit
- ReplayKit
- ARKit

Sicurezza di HomeKit

Sicurezza delle comunicazioni di HomeKit

HomeKit fornisce un'infrastruttura di automazione domestica che utilizza funzionalità di sicurezza di iCloud e dei dispositivi per proteggere e sincronizzare i dati privati senza rivelarli ad Apple.

L'identità e la sicurezza di HomeKit sono basate su coppie di chiavi pubbliche-private Ed25519. La coppia di chiavi Ed25519 è generata sul dispositivo dell'utente e diviene la sua identità di HomeKit. La coppia di chiavi viene usata nel protocollo HAP (HomeKit Accessory Protocol) per eseguire l'autenticazione della comunicazione diretta tra i dispositivi Apple dell'utente e i suoi accessori HomeKit.

Per le abitazioni con un hub domestico, i membri dell'abitazione condivisa possono inviare comandi agli accessori tramite tale hub. Questi comandi vengono inviati, protetti tramite crittografia end-to-end e autenticati dal dispositivo dell'utente all'hub domestico tramite il servizio IDS (Apple Identity Service), dove vengono inoltrati all'accessorio pertinente tramite il protocollo HAP o Matter, uno standard di connettività per abitazioni smart.

Le chiavi, archiviate nel portachiavi e incluse solo nei backup codificati del portachiavi, vengono mantenute aggiornate tra i dispositivi tramite il portachiavi iCloud.

Comunicazione tra gli accessori HomeKit

Gli accessori HomeKit generano una loro coppia di chiavi Ed25519 da utilizzare nelle comunicazioni con i dispositivi Apple. Se l'accessorio è ripristinato alle impostazioni di fabbrica, viene generata una nuova coppia di chiavi.

Per stabilire una relazione tra un dispositivo Apple e un accessorio HomeKit, le chiavi vengono scambiate utilizzando il protocollo Secure Remote Password (a 3072 bit) con un codice a otto cifre fornito dal produttore dell'accessorio, inserito sul dispositivo dell'utente e successivamente codificato mediante ChaCha20-Poly1305 AEAD con chiavi derivate da HKDF-SHA512. Durante la configurazione viene verificata anche la certificazione MFi dell'accessorio. Gli accessori senza un chip MFi possono integrare il supporto per l'autenticazione software su iOS 11.3 o versione successiva.

Quando il dispositivo e l'accessorio HomeKit comunicano durante l'utilizzo, si autenticano reciprocamente utilizzando le chiavi scambiate nel processo descritto sopra. Ogni sessione è stabilita utilizzando il protocollo Station-to-Station ed è codificata con chiavi derivate da HKDF-SHA512 basate su chiavi Curve25519 per sessione. Questo meccanismo è valido sia per accessori basati su IP che per quelli Bluetooth Low Energy (BLE).

Per i dispositivi BLE che supportano le notifiche broadcast, all'accessorio viene fornita una chiave di codifica broadcast da un dispositivo abbinato tramite una sessione sicura. Tale chiave è utilizzata per codificare i dati riguardo alle modifiche di stato sull'accessorio, che vengono comunicate tramite trasmissioni BLE. La chiave di codifica broadcast è una chiave derivata tramite HKDF-SHA512 e i dati sono codificati con l'algoritmo ChaCha20-Poly1305 AEAD (Authenticated Encryption with Associated Data). La chiave di codifica broadcast viene modificata periodicamente e aggiornata su altri dispositivi che utilizzano iCloud, come descritto nella sezione Sicurezza dei dati di HomeKit.

Comunicazione con gli accessori Matter

L'identità e la sicurezza con gli accessori Matter sono basate sui certificati. Per le abitazioni Apple, l'autorità di certificazione radice di attendibilità viene generata sul dispositivo iniziale dell'utente (la "persona responsabile") e la chiave privata per l'autorità di certificazione viene archiviata nel suo portachiavi iCloud. Ciascun dispositivo Apple nell'abitazione genera una richiesta di firma del certificato utilizzando la curva NIST P-256. Questa richiesta viene ricevuta dal dispositivo della persona responsabile, che crea un certificato di identità Matter per il dispositivo utilizzando la propria chiave privata dell'autorità di certificazione. Questo certificato viene successivamente utilizzato per autenticare la comunicazione tra i dispositivi degli utenti e gli accessori.

Gli accessori Matter generano la propria coppia di chiavi NIST P-256 e la propria richiesta di firma del certificato e ricevono un certificato dall'autorità di certificazione durante l'abbinamento. Prima della generazione delle coppie di chiavi, l'accessorio Matter e i dispositivi della persona responsabile scambiano le chiavi (tramite il protocollo SPAKE2+ con un PIN fornito dal produttore dell'accessorio) e viene eseguito un processo di attestazione del dispositivo. La richiesta di firma del certificato e il certificato vengono quindi scambiati tramite questo canale, crittografati utilizzando AES-CCM con chiavi derivate da HKDF-SHA256. Se per l'accessorio vengono ripristinate le impostazioni di fabbrica, vengono generate una nuova coppia di chiavi e una nuova richiesta di firma del certificato e durante l'abbinamento viene emesso un nuovo certificato per l'accessorio.

Quando un dispositivo Apple e l'accessorio Matter comunicano durante l'utilizzo, si autenticano a vicenda utilizzando i propri certificati. Ogni sessione è stabilita utilizzando un protocollo a tre fasi (sigma) ed è codificata con chiavi derivate da HKDF-SHA256 basate su chiavi P256 per sessione.

Per ulteriori informazioni su come i dispositivi Apple interagiscono in modo sicuro con gli accessori Matter, consulta la pagina sul supporto di Matter in iOS 16 sul sito web di Apple Developer.

HomeKit e Siri

Siri può essere utilizzato per inviare richieste agli accessori, controllarli e per attivare le scene. Siri riceve le informazioni essenziali sulla configurazione dell'abitazione, in modo da fornire i nomi di stanze, accessori e scene necessari al riconoscimento dei comandi. L'audio inviato a Siri potrebbe indicare dei comandi o degli accessori specifici, ma tali dati di Siri non sono associati ad altre funzionalità di Apple come HomeKit.

Accessori di HomeKit compatibili con Siri

Utilizzando l'app Casa, gli utenti possono abilitare Siri e le altre funzionalità di HomePod come i timer, gli avvisi, l'interfono e il campanello sugli accessori compatibili con Siri. Quando queste sono abilitate, l'accessorio si coordina con l'HomePod abbinato e collegato alla rete locale che supporta queste funzionalità Apple. La trasmissione dell'audio tra i dispositivi avviene mediante canali crittografati, utilizzando sia i protocolli HomeKit che AirPlay.

Quando "Abilita Ehi Siri" è attivato, l'accessorio attende che venga pronunciata la frase "Ehi Siri" e la identifica mediante un motore di rilevamento delle frasi trigger eseguito in locale. Se quest'ultimo rileva la frase, i frame audio vengono inviati direttamente all'HomePod abbinato tramite HomeKit. L'HomePod controlla l'audio una seconda volta e potrebbe cancellare la sessione in corso se la frase trigger non viene rilevata.

Quando la funzionalità di attivazione di Siri tramite tocco è attiva, l'utente può iniziare una conversazione con Siri premendo il tasto dedicato sull'accessorio. I frame audio vengono inviati direttamente all'HomePod abbinato.

Dopo che viene rilevata un'attivazione di Siri, HomePod invia l'audio ai server di Siri e attua l'intento dell'utente utilizzando la stessa crittografia e le stesse misure per tutelare la sicurezza e la privacy che applica alle richieste che gli utenti rivolgono direttamente a HomePod. Se Siri produce una risposta audio, questa viene inviata all'accessorio tramite un canale audio AirPlay. Per alcune richieste di Siri è necessario che l'utente fornisca ulteriori informazioni, ad esempio, viene chiesto se voglia ascoltare più opzioni. In questi casi, l'accessorio riceve l'istruzione di fare delle domande all'utente e l'audio aggiuntivo viene trasmesso in streaming all'HomePod.

L'accessorio deve essere dotato un indicatore visivo per segnalare all'utente quando è in ascolto, ad esempio, un indicatore LED. L'accessorio non è a conoscenza dell'intenzione della richiesta fatta a Siri, ad eccezione dei flussi audio; nessun dato dell'utente viene salvato sull'accessorio.

Sicurezza dei dati di HomeKit

Per le abitazioni che hanno effettuato l'aggiornamento alla nuova architettura HomeKit (disponibile in iOS 16.2 e iPadOS 16.2), i dati di HomeKit vengono sincronizzati in modo sicuro tra i dispositivi di un utente tramite iCloud e il portachiavi iCloud. Durante tale processo, i dati di HomeKit vengono protetti tramite la crittografia end-to-end di iCloud e non sono accessibili da parte di Apple.

I nuovi utenti possono essere aggiunti dall'utente che ha inizialmente creato l'abitazione in HomeKit (la "persona responsabile)" o da un altro utente con permessi di modifica. Il dispositivo del proprietario configura gli accessori con la chiave pubblica del nuovo utente affinché l'accessorio possa autenticarsi e accettare comandi dall'utente nuovo. Quando un utente che dispone di permessi di modifica aggiunge un nuovo utente, il processo viene delegato a un hub domestico per completare l'operazione.

Dati abitazione e app

L'accesso ai dati dell'abitazione da parte delle app è controllato dagli utenti nelle impostazioni sulla privacy. Agli utenti viene chiesto di concedere l'accesso quando le app richiedono dati dell'abitazione, come avviene per l'accesso a Contatti, Foto e altre sorgenti di dati su iOS, iPadOS e macOS. Se l'utente dà la propria autorizzazione, le app avranno accesso ai nomi delle stanze, ai nomi degli accessori, a informazioni sull'ubicazione degli accessori nelle stanze e ad altri dati, come spiegato in dettaglio nella documentazione su HomeKit per gli sviluppatori, disponibile su https://developer.apple.com/homekit/.

Archiviazione locale dei dati

HomeKit archivia sul dispositivo Apple dell'utente i dati relativi ad abitazione, accessori, scene e utenti. Tali dati sono archiviati utilizzando la classe di protezione dati "Protetto fino alla prima autenticazione utente" e sono inseriti in un data vault. I dati di HomeKit non sono inclusi nei backup locali.

Protezione dei router con HomeKit

Gli utenti possono migliorare la sicurezza della propria rete domestica utilizzando router che supportano HomeKit. Con tali router, gli utenti possono gestire l'accesso Wi-Fi degli accessori HomeKit alla rete locale e a internet. Tali router supportano anche l'autenticazione PPSK, quindi gli accessori possono essere aggiunti alla rete Wi-Fi tramite una chiave specifica per l'accessorio che può essere revocata se necessario. L'autenticazione PPSK migliora la sicurezza evitando di esporre la password principale del Wi-Fi agli accessori e consentendo al router di identificare in sicurezza un accessorio anche se questo dovesse cambiare indirizzo MAC.

Utilizzando l'app Casa, un utente può configurare restrizioni di accesso per gruppi di accessori nei seguenti modi:

- *Nessuna restrizione:* consente l'accesso senza restrizioni a internet e alla rete locale.
- *Automatico:* questa è l'impostazione di default. Consente l'accesso a internet e alla rete locale in base a un elenco di siti internet e porte locali fornito a Apple dal produttore dell'accessorio. L'elenco include tutti i siti e le porte necessari per il corretto funzionamento dell'accessorio. (Finché tale elenco non è disponibile, viene applicata l'opzione "Nessuna restrizione").
- *Limita all'abitazione:* nessun accesso a internet o alla rete locale, fatta eccezione per le connessioni richieste da HomeKit per scoprire e controllare l'accessorio dalla rete locale (incluse quelle dall'hub domestico per supportare il controllo da remoto).

Una chiave PPSK è una password sicura di tipo WPA2 Personal specifica per l'accessorio che viene generata automaticamente da HomeKit e revocata se l'accessorio viene successivamente rimosso dall'abitazione. Una chiave PPSK viene utilizzata quando un accessorio viene aggiunto alla rete Wi-Fi da HomeKit in un'abitazione che è stata configurata con un router HomeKit; dopo l'aggiunta, "Credenziali Wi-Fi"risulterà impostato su "*Gestito tramite HomeKit*" nella schermata delle impostazioni dell'accessorio nell'app Casa. Gli accessori che erano stati aggiunti alla rete Wi-Fi prima dell'aggiunta del router vengono riconfigurati per l'uso di PPSK, se l'accessorio lo supporta, altrimenti verranno mantenute le credenziali esistenti.

Come misura di sicurezza aggiuntiva, gli utenti devono configurare il router HomeKit tramite l'app del produttore del router, in modo tale che l'app possa verificare che gli utenti sono autorizzati ad accedere al router e ad aggiungerlo all'app Casa.

Sicurezza delle videocamere per HomeKit

Le videocamere dotate di indirizzo IP (Internet Protocol) in HomeKit inviano stream video e audio direttamente al dispositivo iOS, iPadOS, tvOS e macOS sulla rete locale che ha accesso allo stream. Gli stream sono codificati tramite chiavi generate casualmente sul dispositivo e sulla videocamera IP, scambiate tramite la sessione HomeKit protetta con la videocamera. Quando un dispositivo non si trova sulla rete locale, gli stream codificati sono trasmessi attraverso l'hub domestico verso il dispositivo. L'hub domestico non decrittografa gli stream; funge solo da elemento di trasmissione tra il dispositivo e la videocamera IP. Quando un'app mostra il video della videocamera IP di HomeKit all'utente, HomeKit elabora i fotogrammi in maniera protetta da un processo di sistema separato. In questo modo, l'app non è in grado di accedere allo stream video o di archiviarlo. Inoltre, alle app non è consentito eseguire istantanee schermo dello stream.

Video sicuro di HomeKit

HomeKit fornisce un meccanismo sicuro e privato per registrare, analizzare e visualizzare clip da videocamere IP compatibili con HomeKit senza esporre tali contenuti video a Apple o a terze parti. Quando la fotocamera IP rileva del movimento, i clip video vengono inviati direttamente a un dispositivo Apple che agisce da hub domestico, tramite una connessione di rete locale dedicata tra l'hub domestico e la videocamera IP. La connessione di rete locale è codificata con una coppia di chiavi derivate tramite HKDF-SHA512 per sessione, negoziata attraverso la sessione HomeKit tra l'hub domestico e la videocamera IP. HomeKit decrittografa gli stream audio e video sull'hub domestico e analizza i fotogrammi video localmente per rilevare eventuali eventi significativi. Se viene rilevato un evento significativo, HomeKit codifica il clip video tramite AES-256-GCM con una chiave AES256 generata in maniera casuale. HomeKit genera anche fotogrammi poster per ciascun clip, che vengono codificati utilizzando la stessa chiave AES256. I fotogrammi poster e i dati audio e video codificati vengono caricati sui server di iCloud. I metadati relativi a ciascun clip, compresa la chiave di codifica, vengono caricati su CloudKit utilizzando la codifica end-to-end di iCloud.

Per la classificazione dei volti, HomeKit archivia tutti i dati usati per classificare il viso di una particolare persona in CloudKit utilizzando la codifica end-to-end di iCloud. I dati archiviati includono informazioni su ciascuna persona, come il nome e le immagini che rappresentano il volto. Questi volti possono arrivare dalla libreria di Foto dell'utente, se quest'ultimo ha dato il consenso, oppure possono essere raccolti da video provenienti dalla videocamera IP analizzati in precedenza. Una sessione di analisi video sicura di HomeKit utilizza questi dati di classificazione per identificare i volti nello stream video sicuro che riceve direttamente dalla videocamera IP e include le informazioni di classificazione nei metadati del clip citati precedentemente.

Quando viene utilizzata l'app Casa per visualizzare i clip di una videocamera, i dati vengono scaricati da iCloud e le chiavi per decrittografare gli stream vengono decifrate localmente utilizzando la decrittografia end-to-end di iCloud. I contenuti video codificati vengono trasmessi dai server e decrittografati localmente sul dispositivo iOS prima di essere mostrati nel visualizzatore. Ciascuna sessione di clip video può essere scomposta in sotto sezioni, ciascuna delle quali codifica lo stream di contenuti tramite la propria chiave unica.

Sicurezza di HomeKit con Apple TV

HomeKit può connettere in maniera sicura alcuni accessori remoti di terze parti ad Apple TV e supporta l'aggiunta di profili utente al proprietario dell'Apple TV dell'abitazione.

Utilizzare accessori remoti di terze parti con Apple TV

Alcuni accessori remoti di terze parti forniscono eventi HID (Human Interface Design) e audio Siri a un'Apple TV associata aggiunta tramite l'app Casa. L'accessorio remoto invia gli eventi HID tramite la sessione sicura ad Apple TV. Un telecomando TV compatibile con Siri invia dati audio a Apple TV quando l'utente attiva esplicitamente il microfono sul telecomando tramite un tasto dedicato per Siri. Il telecomando invia i fotogrammi audio direttamente ad Apple TV utilizzando una connessione di rete locale dedicata. La connessione di rete locale è codificata con una coppia di chiavi derivate tramite HKDF-SHA512 per sessione, negoziata attraverso la sessione HomeKit tra Apple TV e il telecomando TV. HomeKit decrittografa i fotogrammi audio su Apple TV e li inoltra all'app Siri, dove vengono trattati con le stesse protezioni della privacy applicate a tutti gli input audio di Siri.

Profili Apple TV per abitazioni con HomeKit

Quando l'utente di un'abitazione con HomeKit aggiunge il proprio profilo all'Apple TV del proprietario dell'abitazione, quest'ultimo dà all'utente l'accesso ai propri programmi TV, alla propria musica e ai propri podcast. Le impostazioni di utilizzo del profilo di ogni utente su Apple TV sono condivise con l'account iCloud del proprietario tramite la codifica end-to-end di iCloud. I dati sono di proprietà di ogni utente e vengono condivisi con il proprietario dell'abitazione in modalità di sola lettura. Ogni utente dell'abitazione può modificare questi valori nell'app Casa e l'Apple TV del proprietario fa uso delle impostazioni indicate.

Quando viene attivata un'impostazione, l'account iTunes dell'utente è reso disponibile su Apple TV, mentre quando viene disattivata un'impostazione, tutti gli account e i dati di proprietà di quell'utente vengono eliminati da Apple TV. La condivisione iniziale di CloudKit viene avviata dal dispositivo dell'utente e il token per stabilire la condivisione protetta di CloudKit viene inviato tramite lo stesso canale sicuro che viene utilizzato per sincronizzare i dati tra gli utenti dell'abitazione.

Sicurezza di SiriKit per iOS, iPadOS e watchOS

Siri utilizza il sistema delle estensioni delle app per comunicare con le app di terze parti. Su un dispositivo, Siri può accedere ai contatti dell'utente e alla posizione attuale del dispositivo. Tuttavia, prima di fornire dati protetti a un'app, Siri verifica i permessi di accesso controllati dall'utente. In base a tali permessi, Siri passa all'estensione dell'app solo il frammento pertinente dell'affermazione originale dell'utente. Ad esempio, se un'app non ha accesso ai contatti, Siri non risolverà la relazione contenuta in una richiesta dell'utente del tipo "Invia 10 € a mia madre con (app di pagamento)". In questo caso, l'app vedrebbe solo il termine "mia madre".

Se tuttavia l'utente ha concesso all'app l'accesso ai contatti, l'app riceve le informazioni sulla madre dell'utente. Se la relazione viene indicata nel corpo di un messaggio, come ad esempio "Di' a mia mamma in MessageApp che mio fratello è stato bravissimo", Siri non risolverà "mio fratello", a prescindere dai permessi dell'app.

Le app compatibili con SiriKit possono inviare termini specifici dell'app o dell'utente a Siri, come i nomi dei contatti dell'utente. Queste informazioni consentono al riconoscimento vocale di Siri e alla comprensione del linguaggio naturale di identificare il vocabolario per quell'app e sono associati a un identificatore casuale. Le informazioni personalizzate rimangono disponibili finché è in uso l'identificatore o finché l'utente non disabilita l'integrazione di Siri dell'app in Impostazioni oppure finché l'app compatibile con SiriKit non viene disinstallata.

Per un'affermazione come "Portami a casa di mia madre con l'app RideShareApp", la richiesta necessita dei dati della posizione presenti nei contatti dell'utente. Solo per questa richiesta, Siri fornisce le informazioni necessarie all'estensione dell'app, a prescindere dalle impostazioni dei permessi dell'utente per la posizione o delle informazioni di contatto per l'app.

Sicurezza di WidgetKit

WidgetKit è il framework utilizzato dagli sviluppatori per creare widget e complicazioni di Apple Watch. Entrambi possono mostrare informazioni sensibili che potrebbero essere molto visibili, soprattutto per i dispositivi con lo schermo sempre attivo.

In iOS, gli utenti possono scegliere se mostrare i dati sensibili sulla schermata di blocco e quando la modalità "Schermo sempre attivo" è abilitata. In Impostazioni, possono disattivare l'accesso ai dati per i widget della schermata di blocco nella sezione "Consenti accesso se bloccato" in Impostazioni > Face ID e codice.

Su Apple Watch, gli utenti possono scegliere se monitorare i dati sensibili con "Schermo sempre attivo" in Impostazioni > Schermo e luminosità > Sempre attivo > Nascondi complicazioni sensibili. Inoltre, possono scegliere di mostrare contenuti oscurati per tutte o per le singole complicazioni.

Se un utente sceglie di nascondere contenuti che ritiene confidenziali, WidgetKit li sostituisce con un placeholder o li oscura. Per configurare i contenuti oscurati, lo sviluppatore deve:

1. Implementare il callback `redacted(reason:)`.

2. Esplicitare la proprietà `privacy`.

3. Fornire viste dei placeholder personalizzate.

Gli sviluppatori possono anche rendere una vista come non oscurata con il modificatore vista un`redacted()`.

Invece di rendere i contenuti delle singole viste privati, nel caso in cui tutti i contenuti di un widget siano tali, lo sviluppatore può aggiungere la funzionalità di protezione dei dati all'estensione del widget. Fino a quando l'utente non selezionerà il corrispondente livello di privacy nel dispositivo, WidgetKit mostrerà i placeholder al posto dei contenuti del widget. Lo sviluppatore deve abilitare la funzionalità di protezione dei dati per l'estensione del widget in Xcode, quindi impostare il permesso `Data Protection` sul valore corrispondente al livello di privacy che vuole rendere disponibile:

- `NSFileProtectionComplete`
- `NSFileProtectionCompleteUnlessOpen`

WidgetKit nasconde i contenuti di questi widget quando il dispositivo è bloccato da codice e mostra un Placeholder fino a quando un utente esegue l'autenticazione in seguito al riavvio del dispositivo. Inoltre, i widget di iOS non sono disponibili come widget di iPhone sul Mac.

Sicurezza di DriverKit per macOS

DriverKit è il framework che consente agli sviluppatori di creare driver per dispositivi installabili dall'utente sul proprio Mac. I driver creati con DriverKit sono eseguiti nello spazio utente invece che come estensioni del kernel, in modo da migliorare la stabilità e la sicurezza del sistema. In questo modo, l'installazione è più semplice e la stabilità e la sicurezza di macOS sono migliori.

L'utente deve semplicemente scaricare l'app (non sono necessari programmi di installazione quando si usano le estensioni di sistema o DriverKit) e l'estensione viene abilitata solo quando necessario. Questa procedura sostituisce l'uso delle kexts in molte situazioni in cui sono necessari privilegi di amministratore per installare in /Sistema/Libreria o in /Libreria.

Gli amministratori IT che usano driver dispositivo, soluzioni di archiviazione cloud, networking e app per la sicurezza che richiedono le estensioni del kernel sono invitati a passare a versioni più recenti progettate per lavorare con le estensioni di sistema. Queste nuove versioni, che riducono notevolmente sia la possibilità di kernel panic sul Mac che la superficie di attacco, sono eseguite nello spazio utente, non richiedono privilegi particolari di installazione e vengono rimosse automaticamente quando l'app da cui provengono viene spostata nel Cestino.

Il framework DriverKit fornisce classi C++ per i servizi I/O, corrispondenza tra dispositivi, descrittori di memoria e code di invio. Definisce inoltre i tipi di I/O appropriati per numeri, raccolte, stringhe a altri tipi comuni, che l'utente usa con framework driver di una famiglia determinata, come ad esempio USBDriverKit e HIDDriverKit. Utilizza il framework per le estensioni del sistema per installare e aggiornare un driver.

Sicurezza di ReplayKit in iOS e iPadOS

ReplayKit è un framework che consente agli sviluppatori di aggiungere possibilità di registrazione e trasmissione live alle app. Inoltre, consente agli utenti di commentare le registrazioni e le trasmissioni utilizzando la videocamera anteriore e il microfono del dispositivo.

Registrazione di filmati

Nella registrazione di un filmato sono integrati vari livelli di sicurezza:

- *Finestra di dialogo con richiesta di permesso:* prima che la registrazione abbia inizio, ReplayKit visualizza un avviso in cui viene richiesto all'utente di dare il proprio consenso per la registrazione dello schermo e per l'uso del microfono e della fotocamera anteriore. Tale avviso viene presentato una sola volta per ogni processo dell'app; se l'app viene lasciata in background per più di 8 minuti, l'avviso viene visualizzato nuovamente.
- *Registrazione di schermo e audio:* la registrazione dello schermo e dell'audio avviene al di fuori del processo dell'app nel daemon replayd di ReplayKit. Questo meccanismo è progettato per garantire che il contenuto della registrazione non sia mai accessibile al processo dell'app.
- *Registrazione di schermo e audio in-app:* consente a un'app di ottenere buffer campione e video, protetti dalla finestra di dialogo con richiesta di permesso.
- *Creazione e archiviazione di un filmato:* il file del filmato è scritto in una directory che è accessibile unicamente ai sottosistemi di ReplayKit e non è accessibile alle app. Questo meccanismo aiuta a impedire che le registrazioni possano essere utilizzate da terze parti senza il consenso dell'utente.
- *Anteprima e condivisione da parte dell'utente finale:* l'utente dispone della possibilità di visualizzare in anteprima il filmato e di condividerlo con l'interfaccia utente di ReplayKit. L'interfaccia utente è presentata al di fuori del processo tramite l'infrastruttura delle estensioni di iOS e ha accesso al file del filmato generato.

Trasmissione con ReplayKit

Nella trasmissione di un filmato sono integrati vari livelli di sicurezza:

- *Registrazione di schermo e audio:* il meccanismo di registrazione dello schermo e dell'audio durante la trasmissione è identico a quello della registrazione dei filmati e avviene in `replayd`.
- *Estensioni di trasmissione:* perché i servizi di terze parti partecipino alla trasmissione di ReplayKit, devono creare due nuove estensioni configurate con l'endpoint com.apple.broadcast-services:
  - Un'estensione dell'interfaccia utente che consenta all'utente di configurare la trasmissione.
  - Un'estensione di upload che gestisca gli upload dei dati di video e audio sui server di back-end del servizio.

L'architettura aiuta a garantire che le app host non abbiano privilegi sui contenuti video e audio trasmessi. L'accesso è consentito solo a ReplayKit e alle estensioni di trasmissione di terze parti.

- *Selezione trasmissione:* consente agli utenti di avviare una trasmissione di sistema direttamente dall'app utilizzando la stessa interfaccia utente definita dal sistema che è accessibile tramite Centro di Controllo. L'interfaccia utente è implementata tramite un'API privata ed è un'estensione che risiede all'interno del framework di ReplayKit. Si trova al di fuori del processo dell'app di hosting.
- *Estensione di upload:* l'estensione implementata dai servizi di trasmissione di terze parti per la gestione dei contenuti video e audio durante la trasmissione usa buffer di campioni non codificati e non elaborati. Durante questa modalità di gestione, i dati video e audio vengono serializzati e passati all'estensione di upload di terze parti in tempo reale mediante una connessione diretta XPC. I dati video vengono codificati estraendo l'oggetto IOSurface dal buffer campione del video, codificandolo in modo sicuro come oggetto XPC, inviandolo quindi all'estensione di terze parti via XPC e decrittografandolo infine nuovamente in modo sicuro nell'oggetto IOSurface.

Sicurezza di ARKit in iOS e iPadOS

ARKit è un framework che consente agli sviluppatori di produrre esperienze in realtà aumentata per la propria app o il proprio gioco. Gli sviluppatori possono aggiungere elementi 2D o 3D utilizzando la fotocamera anteriore o posteriore di un dispositivo iOS o iPadOS.

Apple ha progettato le fotocamere pensando in primo luogo alla privacy dell'utente e le app di terze parti dovranno ottenere il consenso da parte dell'utente prima di poter accedere alla fotocamera. In iOS e iPadOS, le app a cui l'utente concede accesso alla fotocamera possono accedere alle immagini in tempo reale della fotocamera anteriore e posteriore. Le app non sono autorizzate a usare la fotocamera senza mostrare in modo trasparente che la fotocamera è in uso.

Le foto e i video acquisiti con la fotocamera potrebbero contenere altre informazioni, come il luogo e l'ora in cui sono stati realizzati, la profondità di campo e altre immagini attorno all'inquadratura. Se l'utente non vuole che le foto e i video acquisti con l'app Fotocamera includano dati sulla posizione, può modificare la relativa impostazione in qualsiasi momento in Impostazioni > Privacy > Localizzazione > Fotocamera. Se l'utente non vuole che le foto e i video includano i dati sulla posizione quando vengono condivisi, può disattivare la localizzazione nel menu Opzioni della schermata di condivisione.

Per offrire una migliore esperienza AR all'utente, le app che usano ARKit possono utilizzare le informazioni di rilevamento della scena o del volto dall'altra fotocamera. L'opzione di rilevamento della scena usa degli algoritmi sul dispositivo dell'utente per elaborare le informazioni dei sensori in modo da determinare la posizione dell'utente nello spazio fisico. Tale opzione abilita funzionalità come l'orientamento ottico in Mappe.

Gestione sicura dei dispositivi

Panoramica sulla gestione sicura dei dispositivi

iOS, iPadOS, macOS, tvOS e watchOS supportano configurazioni e politiche di sicurezza flessibili, facili da applicare e da gestire. Grazie a tali configurazioni e politiche, le organizzazioni sono in grado di proteggere le informazioni aziendali e possono essere aiutate a garantire che i dipendenti rispettino i requisiti dell'azienda anche quando utilizzano i loro dispositivi personali, come nel caso di un programma BYOD (Bring Your Own Device).

Le organizzazioni possono avvalersi del framework per la gestione dei dispositivi mobili (MDM) implementato da una soluzione MDM per applicare i requisiti per il passcode, configurare le impostazioni, limitare le funzionalità e perfino inizializzare da remoto i dati aziendali sui dispositivi gestiti. In questo modo, i dati aziendali rimarranno sempre al sicuro, anche quando i dipendenti accedono ai dati tramite i propri dispositivi personali.

Sicurezza del modello di abbinamento per iPhone e iPad

iOS e iPadOS utilizzano un modello di abbinamento per controllare l'accesso al dispositivo da un computer host. L'abbinamento instaura una relazione attendibile fra il dispositivo e l'host connesso, indicata da uno scambio di chiavi pubbliche. iOS e iPadOS utilizzano questa firma di attendibilità per abilitare ulteriori funzionalità con l'host connesso, come la sincronizzazione dei dati. In iOS 9 o versione successiva, i servizi:

- Se richiedono un abbinamento, non possono essere avviati finché il dispositivo non viene sbloccato dall'utente.
- Non si avviano a meno che il dispositivo non sia stato sbloccato di recente.
- Per poter essere avviati potrebbero richiedere (per esempio nel caso della sincronizzazione delle foto) che il dispositivo sia sbloccato.

In fase di abbinamento l'utente deve sbloccare il dispositivo e accettare la richiesta proveniente dall'host. In iOS 9 o versione successiva, l'utente deve inserire anche il codice; dopodiché, l'host e il dispositivo scambiano e salvano le chiavi pubbliche RSA a 2048 bit. All'host viene quindi assegnata una chiave a 256 bit in grado di sbloccare una keybag Escrow archiviata sul dispositivo. Le chiavi scambiate vengono utilizzate per iniziare una sessione SSL codificata, richiesta dal dispositivo prima di inviare dati protetti all'host o prima di avviare un servizio (sincronizzazione iTunes o Finder, trasferimento di file, sviluppo Xcode, ecc.). Per utilizzare questa sessione codificata per tutte le comunicazioni, il dispositivo richiede connessioni da un host tramite Wi-Fi, quindi deve aver effettuato l'abbinamento in precedenza mediante USB. L'abbinamento abilita anche una serie di funzionalità di diagnostica. In iOS 9, se un record di abbinamento non viene utilizzato da più di 6 mesi, viene considerato scaduto. In iOS 11 o versione successiva, questo periodo viene accorciato a 30 giorni.

Alcuni servizi di diagnosi, tra cui com.apple.mobile.pcapd, possono solo funzionare via USB. Inoltre, il servizio com.apple.file_relay richiede che sia installato un profilo di configurazione firmato da Apple. In iOS 11 o versioni successive, Apple TV può utilizzare il protocollo SRP per stabilire una relazione di abbinamento in modalità wireless.

L'utente può azzerare l'elenco degli host attendibili utilizzando le opzioni "Ripristina impostazioni rete" o "Ripristina posizione e privacy".

Gestione dei dispositivi mobili

Panoramica sulla sicurezza della gestione dei dispositivi mobili

I sistemi operativi Apple supportano la gestione dei dispositivi mobili (MDM), che consente alle organizzazioni di configurare e gestire in modo sicuro i dispositivi Apple distribuiti.

Funzionamento sicuro della gestione dei dispositivi mobili

Le funzionalità MDM sono integrate nelle tecnologie nel sistema operativo, come le configurazioni, la registrazione in modalità wireless e il servizio di notifiche push di Apple (APN). Ad esempio, il servizio APN è utilizzato per attivare il dispositivo e attivare così la comunicazione diretta con la soluzione MDM tramite una connessione protetta. Non vengono trasmesse informazioni confidenziali o proprietarie.

Utilizzando MDM, i reparti IT possono registrare i dispositivi Apple in un ambiente aziendale o educativo, configurare e aggiornare le impostazioni in modalità wireless, monitorare la conformità, gestire le politiche di aggiornamento del software e perfino cancellare o bloccare a distanza i dispositivi gestiti.

Con iOS 13, iPadOS 13.1 e macOS 10.15 o versioni successive, i dispositivi Apple supportano una nuova opzione per la registrazione progettata appositamente per i programmi BYOD. "Registrazione utente" offre maggiore autonomia agli utenti sui propri dispositivi, aumentando al tempo stesso la sicurezza dei dati aziendali mediante la separazione dei dati gestiti tramite crittografia. Questo consente di ottenere un miglior equilibrio tra sicurezza, privacy ed esperienza utente per i programmi BYOD. Un meccanismo di separazione simile è stato aggiunto per le registrazioni dei dispositivi basate su account in iOS 17, iPadOS 17 e macOS 14, o versioni successive.

Tipi di registrazione

- *Registrazione utente:* è progettata per i dispositivi di proprietà dell'utente, è integrata negli ID Apple gestiti e serve a stabilire l'identità di un utente sul dispositivo. Per avviare la registrazione sono richiesti gli ID Apple gestiti e l'utente deve autenticarsi, affinché la registrazione vada a buon fine. Gli ID Apple gestiti possono essere utilizzati insieme a un ID Apple personale con cui l'utente ha già effettuato l'accesso. Le app e gli account gestiti utilizzano l'ID Apple gestito, mentre le app e gli account personali utilizzano l'ID Apple personale.
- *Registrazione dispositivo:* consente alle organizzazioni di far registrare manualmente i dispositivi agli utenti e quindi di gestire molti diversi aspetti legati all'uso degli stessi, tra cui la possibilità di inizializzarli. La registrazione dei dispositivi ha inoltre un più ampio insieme di configurazioni e restrizioni applicabili ai dispositivi. Quando un utente rimuove un profilo di registrazione, vengono rimosse anche tutte le configurazioni, le relative impostazioni e le app gestite basate su di esso. Analogamente a "Registrazione utente", anche "Registrazione dispositivo" può essere integrata con un ID Apple gestito. Questa registrazione del dispositivo basata su account offre anche la possibilità di utilizzare un ID Apple gestito insieme a un ID Apple personale, separando crittograficamente i dati aziendali.
- *Registrazione automatizzata dispositivo:* consente alle organizzazioni di configurare e gestire i dispositivi dal momento in cui vengono utilizzati per la prima volta. Tali dispositivi vengono detti *supervisionati* ed è possibile impedire la rimozione da parte dell'utente del profilo MDM. La registrazione automatizzata dei dispositivi è pensata per i dispositivi di proprietà delle organizzazioni.

Restrizioni dei dispositivi

Le restrizioni possono essere abilitate, e in alcuni casi disabilitate, dagli amministratori per impedire che gli utenti accedano ad app, servizi o funzionalità specifiche su iPhone, iPad, Mac o Apple TV o Apple Watch registrati in una soluzione MDM. Le restrizioni vengono inviate ai dispositivi in un apposito payload, incluso in una configurazione. Alcune restrizioni applicate a un iPhone potrebbero essere applicate anche sull'Apple Watch abbinato.

Gestione delle impostazioni di password e codici

Di default, il codice si può definire come un PIN numerico su iOS, iPadOS e watchOS. Sugli iPhone e iPad con Face ID o Touch ID, la lunghezza predefinita del codice è di sei cifre, con una lunghezza minima di quattro cifre. I codici più lunghi e complessi sono più difficili da indovinare o da attaccare, quindi sono consigliati.

Gli amministratori possono implementare requisiti complessi per i codici e altre politiche utilizzando MDM oppure, su iOS e iPadOS, Microsoft Exchange. Per l'installazione manuale del payload sulle politiche dei codici di macOS è necessaria una password da amministratore. Le politiche dei codici possono richiedere che il codice abbia una certa lunghezza, una certa composizione o altri attributi.

Su Apple Watch i codici sono numerici di default. Se una politica per il codice applicata a un Apple Watch gestito richiede l'utilizzo di caratteri non numerici, sarà necessario sbloccare il dispositivo tramite l'iPhone abbinato.

Applicazione della configurazione

I profili sono lo strumento principale tramite il quale una soluzione MDM invia e gestisce politiche e restrizioni sui dispositivi gestiti. Se la tua organizzazione ha bisogno di configurare un grande numero di dispositivi o se occorre fornire a svariati dispositivi molte impostazioni personalizzate per le email, le impostazioni di rete o i certificati, le configurazioni sono uno strumento sicuro per farlo.

Configurazioni

Una *configurazione* è un profilo file XML o json formattato con una determinata struttura, composto da payload che caricano impostazioni e informazioni sulle autorizzazioni sui dispositivi Apple. Le configurazioni rendono automatica la configurazione di impostazioni, account, restrizioni e credenziali. Questi file possono essere creati da una soluzione MDM o da Apple Configurator per Mac, oppure possono essere creati manualmente. Prima di inviare una configurazione a un dispositivo Apple, quest'ultimo deve essere registrato nella soluzione MDM tramite un profilo di registrazione.

Nota: Apple Configurator per Mac può essere utilizzato soltanto per gestire i profili di configurazione su iPhone, iPad e Apple TV.

Profili di registrazione

Un *profilo di registrazione* è una configurazione con un payload MDM che serve a registrare un dispositivo nella soluzione MDM specificata per il dispositivo. Ciò consente alla soluzione MDM di inviare comandi configurazioni al dispositivo e di inviare query su determinati aspetti. Quando un utente rimuove un profilo di registrazione, vengono rimossi anche tutte le configurazioni, le relative impostazioni e le app gestite basate su di esso. Su un dispositivo può essere presente un solo profilo di registrazione per volta.

Esempi di configurazioni

Una configurazione contiene diverse impostazioni configurabili all'interno di payload specifici, tra cui, ad esempio:

- Politiche relative a codici e password.
- Restrizioni alle funzionalità dei dispositivi (per esempio, disabilitazione della fotocamera).
- Impostazioni della rete e della VPN.
- Impostazioni di Microsoft Exchange.
- Impostazioni per la posta.
- Impostazioni account.
- Impostazioni del servizio di directory LDAP.
- Impostazioni del servizio di calendario CalDAV.
- Credenziali e identità
- Certificati
- Aggiornamenti software.

Codifica e firma dei profili

È possibile firmare i profili di configurazione per confermarne l'origine e codificarli per aiutare ad assicurarne l'integrità e proteggerne il contenuto. I profili di configurazione per iOS e iPadOS sono codificati tramite la Cryptographic Message Syntax (CMS) specificata nella RFC 5652, che supporta 3DES e AES128.

Installazione dei profili

Le configurazioni possono essere installate sui dispositivi con una soluzione MDM oppure manualmente dagli utenti. In alternativa, è possibile utilizzare Apple Configurator per Mac per implementare le configurazioni su dispositivi iOS, iPadOS e tvOS. Alcune configurazioni richiedono un'installazione utilizzando una soluzione MDM. Per informazioni su come rimuovere i profili, vedi Introduzione alla gestione dei dispositivi mobili in "Distribuzione della piattaforma Apple".

Nota: sui dispositivi supervisionati, i profili di configurazione possono anche essere bloccati su un dispositivi specifico. Questa opzione è progettata per impedirne la rimozione o per consentirne la rimozione solo tramite un codice.

Registrazione automatizzata dei dispositivi

Le organizzazioni possono registrare automaticamente i dispositivi iOS, iPadOS, macOS e tvOS a una soluzione di gestione dei dispositivi mobili (MDM) senza doverli toccare o preparare materialmente prima di consegnarli agli utenti. Una volta registrati per uno dei servizi in Apple School Manager, Apple Business Manager o Apple Business Essential, gli amministratori accedono al relativo sito web e collegano il programma alla propria soluzione MDM. I dispositivi che hanno acquistato possono quindi essere assegnati agli utenti tramite MDM. Durante la procedura di configurazione del dispositivo, questo invia una query ai server Apple richiedendo un MDM assegnato e, se viene individuato, contatta la soluzione MDM per procedere con la registrazione. L'uso della registrazione automatizzata dei dispositivi e di una soluzione MDM compatibile consente alle organizzazioni di implementare le seguenti misure di sicurezza:

- Fare in modo che gli utenti effettuino l'autenticazione durante la configurazione iniziale in Impostazione Assistita sul dispositivo Apple durante l'attivazione.
- Fornire una configurazione preliminare con accesso limitato e richiedere una configurazione aggiuntiva del dispositivo per accedere ai dati sensibili.
- Richiedere ai dispositivi di eseguire una versione minima del sistema operativo prima della registrazione.
- Applicare l'abilitazione FileVault sui Mac.

In seguito alla registrazione di un dispositivo con MDM, le configurazioni, le restrizioni o i controlli vengono installati automaticamente.

È possibile semplificare ulteriormente il processo di configurazione eliminando passaggi specifici in Impostazione Assistita per i dispositivi, in modo che l'utente possa essere operativo in poco tempo. Se alcuni passaggi non vengono eseguiti, verrà utilizzata l'impostazione che tutela maggiormente la privacy. Ad esempio, se viene saltato il pannello per la configurazione dei servizi di localizzazione, questi non verranno abilitati durante Impostazione Assistita.

Gli amministratori possono anche controllare se l'utente può rimuovere o meno il profilo MDM dal dispositivo e verificare che le configurazioni e le restrizioni siano applicate al dispositivo durante tutto il suo ciclo di vita.

Apple School Manager, Apple Business Manager e Apple Business Essentials

Apple School Manager, Apple Business Manager e Apple Business Essentials sono servizi che permettono agli amministratori IT di distribuire in maniera efficiente i dispositivi Apple che un'organizzazione ha acquistato direttamente da Apple o tramite rivenditori e gestori autorizzati Apple.

Quando questi servizi sono utilizzati con una soluzione MDM, gli amministratori possono semplificare il processo di configurazione per gli utenti, configurare le impostazioni dei dispositivi e distribuire app e libri acquistati tramite questi tre servizi. Apple School Manager può anche integrarsi con sistemi SIS (Student Information Systems) direttamente o tramite SFTP, e tutti e tre i servizi supportano la sincronizzazione delle directory o l'autenticazione federata, in modo che sia possibile eseguire il provisioning, l'aggiornamento o l'annullamento del provisioning degli account sulla base del provider d'identità dell'organizzazione.

Apple mantiene certificazioni che soddisfano gli standard ISO/IEC 27001 e 27018, per consentire ai clienti Apple di adempiere ai propri obblighi legali e contrattuali. Tali certificazioni forniscono ai nostri clienti un'attestazione indipendente riguardo alle pratiche di Apple per la privacy delle informazioni e per la sicurezza nei sistemi pertinenti. Per ulteriori informazioni, consulta Certificazioni di sicurezza per i servizi internet Apple in Certificazioni delle piattaforme Apple.

Nota: per sapere se un programma di Apple è disponibile in un paese o in una zona specifici, consulta l'articolo del supporto Apple Disponibilità dei programmi Apple e dei metodi di pagamento per i settori Education e Business.

Supervisione dei dispositivi

In genere la *supervisione* denota che il dispositivo è di proprietà dell'organizzazione ed è quindi presente un controllo maggiore su configurazione e restrizioni. Per ulteriori informazioni consulta Informazioni sulla supervisione dei dispositivi Apple in Distribuzione della piattaforma Apple.

Quando si utilizza la registrazione automatizzata dei dispositivi, la supervisione viene abilitata automaticamente sul dispositivo.

Sicurezza del blocco attivazione

L'implementazione del blocco attivazione da parte di Apple varia a seconda del tipo di dispositivo: iPhone o iPad, Mac dotato di chip Apple o Mac dotato di processore Intel con chip di sicurezza Apple T2.

Funzionamento su iPhone e iPad

Su iPhone e iPad, il blocco attivazione viene implementato durante il processo di attivazione, dopo la schermata di selezione del Wi-Fi in Impostazione Assistita di iOS e iPadOS. Quando il dispositivo segnala di essere in fase di attivazione, invia una richiesta a un server Apple per ottenere un certificato di attivazione. I dispositivi su cui è attivo il blocco attivazione richiedono all'utente di inserire le credenziali di iCloud dell'utente che ha abilitato il blocco attivazione. Impostazione Assistita di iOS e iPadOS non continua il processo di attivazione finché non ottiene un certificato valido.

Funzionamento sui Mac dotati di chip Apple

Nei Mac dotati di chip Apple, il bootloader di livello inferiore verifica che sia presente un LocalPolicy valido per il dispositivo e che i valori anti-replay delle politiche di LocalPolicy corrispondano ai valori archiviati nel componente Secure Storage. Il bootloader di livello inferiore si riavvia in recoveryOS se:

- Non è presente un LocalPolicy per l'attuale versione di macOS.
- LocalPolicy non è valido per tale versione di macOS.
- I valori degli hash dei valori anti-replay di LocalPolicy non corrispondono a quelli archiviati nel componente Secure Storage.

recoveryOS rileva che il Mac non è attivato e contatta il server di attivazione per ottenere un certificato. Se sul dispositivo è attivo il blocco attivazione, recoveryOS richiede all'utente di inserire le credenziali di iCloud dell'utente che a abilitato il blocco attivazione. Una volta ottenuto un certificato di attivazione valido, la relativa chiave viene usata per ottenere un certificato RemotePolicy. Il computer Mac utilizza la chiave di LocalPolicy e il certificato di RemotePolicy per produrre un LocalPolicy valido. Il bootloader di livello inferiore non consentirà l'avvio di macOS finché non è presente un LocalPolicy valido.

Comportamento sui computer Mac dotati di processore Intel

Sui Mac dotati di processore Intel con chip di sicurezza Apple T2, il firmware del chip T2 verifica che sia presente un certificato di attivazione valido prima di consentire l'avvio del computer in macOS. Il firmware UEFI caricato dal chip T2 si occupa di controllare lo stato di attivazione del dispositivo dal chip T2 stesso e di eseguire l'avvio in recoveryOS invece di macOS se non è presente un certificato di attivazione valido. recoveryOS rileva che il Mac non è attivato e contatta il server di attivazione per ottenere un certificato. Se sul dispositivo è attivo il blocco attivazione, recoveryOS richiede all'utente di inserire le credenziali di iCloud dell'utente che a abilitato il blocco attivazione. Il firmware UEFI non consentirà l'avvio di macOS finché non è presente un certificato di attivazione valido.

Modalità smarrito gestita e inizializzazione da remoto

La modalità smarrito gestita è utilizzata per localizzare i dispositivi supervisionati quando vengono rubati. Una volta localizzati, possono essere bloccati o inizializzati da remoto.

Modalità smarrito gestita

Se un dispositivo iOS o iPadOS supervisionato con iOS 9 o versione successiva viene smarrito o rubato, l'amministratore di una soluzione MDM può abilitare remotamente la modalità smarrito sul dispositivo (chiamata, in questo caso, modalità smarrito gestita). Quando la modalità smarrito gestita è abilitata, l'utente attuale viene disconnesso e il dispositivo non può essere sbloccato. Sullo schermo viene visualizzato un messaggio, personalizzabile dall'amministratore, che può contenere ad esempio un numero di telefono da chiamare nel caso in cui il dispositivo venga trovato. L'amministratore anche può richiedere al dispositivo di inviare la propria posizione attuale (anche se la localizzazione è disattivata) e, facoltativamente, di emettere un suono. Quando un amministratore disattiva la modalità smarrito gestita (questo è l'unico caso in cui l'opzione può essere disattivata), l'utente viene informato tramite un messaggio sulla schermata di blocco o un avviso sullo schermata Home.

Inizializzazione da remoto

iPhone, iPad, Mac, Apple TV e Apple Watch possono essere inizializzati da remoto da un amministratore o da un utente, in modo da rendere illeggibili tutti i dati.

Quando il comando è attivato dal server MDM o da iCloud, i dispositivi inviano una conferma alla soluzione MDM e procedono all'inizializzazione. Per l'inizializzazione da remoto con Microsoft Exchange ActiveSync, il dispositivo accede a Microsoft Exchange Server prima di avviare l'inizializzazione.

L'inizializzazione da remoto non è possibile nei seguenti casi:

- Con la registrazione utente
- Usando Microsoft Exchange ActiveSync se l'account è stato installato con la registrazione utente
- Usando Microsoft Exchange ActiveSync se il dispositivo è supervisionato

Gli utenti possono inizializzare anche i dispositivi supportati in loro possesso tramite Impostazioni su iPhone e iPad o in Impostazioni di Sistema su Mac. Inoltre, come accennato in precedenza, è possibile impostare iPhone, iPad e Apple Watch in modo da avviare automaticamente la cancellazione dopo una serie di tentativi non riusciti di inserimento del codice.

L'inizializzazione istantanea da remoto è disponibile sui Mac dotati di chip Apple e di chip di sicurezza Apple T2, oppure se FileVault è attivato. L'inizializzazione istantanea da remoto si ottiene eliminando in modo sicuro la chiave multimediale.

Sicurezza di "iPad condiviso" in iPadOS

"iPad condiviso" è una modalità multiutente per l'uso di iPad in contesti distribuiti. Consente agli utenti di condividere un iPad mantenendo separati i documenti e i dati di ognuno. Ciascun utente ottiene una posizione di archiviazione privata e riservata, implementata sotto forma di volume APFS protetto dalle proprie credenziali. Un iPad condiviso richiede l'utilizzo di un ID Apple gestito, emesso dall'organizzazione e di sua proprietà.

Con un iPad condiviso, gli utenti sono in grado di accedere a qualsiasi dispositivo posseduto dall'organizzazione configurato per l'utilizzo da parte di più utenti. I dati degli utenti vengono suddivisi in directory separate, ognuna delle quali si trova nel proprio dominio di protezione dati ed è protetta da permessi UNIX e sandbox. In iPadOS 13.4 o versioni successive, gli utenti possono accedere anche con una sessione temporanea. Quando l'utente esce da una sessione temporanea, il relativo volume APFS viene eliminato e lo spazio a esso riservato viene restituito al sistema.

Accesso a un iPad condiviso

Per l'accesso a un iPad condiviso sono supportati gli ID Apple gestiti, sia nativi che federati. Quando un account federato è usato per la prima volta, l'utente è reindirizzato al portale di accesso del provider di identità. Una volta eseguita l'autenticazione, viene rilasciato un token di accesso di breve durata per gli ID Apple gestiti di supporto e il login continua in modo simile per la procedura di accesso degli ID Apple gestiti nativi. Quando è stato eseguito l'accesso, Impostazione Assistita sull'iPad condiviso richiede all'utente di stabilire un codice (credenziale) usato per proteggere i dati locali sul dispositivo e per eseguire l'autenticazione nella schermata di login in futuro. Come su un dispositivo di un solo utente, in cui l'utente accederebbe una volta al proprio ID Apple gestito usando l'account federato e sbloccherebbe quindi il dispositivo con il codice, sull'iPad condiviso l'utente accede una volta con l'account federato e, da lì in poi, usa il codice stabilito.

Quando un utente effettua l'accesso senza autenticazione federata, l'ID Apple gestito viene autenticato tramite il servizio Apple Identity Service (IDS) utilizzando il protocollo SRP. Se l'autenticazione avviene correttamente, al dispositivo viene assegnato un token specifico di breve durata per l'accesso. Se l'utente ha già utilizzato il dispositivo, dispone già di un account utente locale, che viene sbloccato tramite le stesse credenziali.

Se l'utente non ha ancora utilizzato il dispositivo o se sta utilizzando la funzionalità di sessione temporanea, l'iPad condiviso fornisce un nuovo ID utente UNIX, un volume APFS per l'archiviazione dei dati personali dell'utente e un portachiavi locale. Dal momento che lo spazio di archiviazione viene allocato (riservato) per l'utente nel momento in cui viene creato il volume APFS, potrebbe non esserci spazio a sufficienza per creare un nuovo volume. In tale caso, il sistema identifica un utente esistente per il quale è terminata la sincronizzazione dei dati sul cloud e lo espelle dal dispositivo per consentire l'accesso al nuovo utente. Nel raro caso in cui nessuno degli utenti esistenti abbia completato il caricamento dei dati sul cloud, l'accesso del nuovo utente non andrà a buon fine. Per accedere, il nuovo utente avrà bisogno di attendere il termine della sincronizzazione dei dati di un'altra persona oppure chiedere a un amministratore di forzare l'eliminazione di un account utente esistente, con il rischio di perdere alcuni dati.

Se il dispositivo non è connesso a internet (ad esempio, se l'utente non dispone di un punto di accesso per il Wi-Fi), l'autenticazione può essere effettuata con l'account locale per un numero limitato di giorni. In una situazione di questo tipo possono accedere solo gli utenti che dispongono di account locali preesistenti o di una sessione temporanea. Una volta scaduto il tempo limite, agli utenti viene richiesto di eseguire l'autenticazione in linea, anche se esiste già un account locale.

Una volta creato o sbloccato l'account locale dell'utente, se l'autenticazione è avvenuta da remoto, il token temporaneo emesso dai server di Apple viene trasformato in un token di iCloud che consente l'accesso a iCloud. Successivamente, vengono ripristinate le impostazioni dell'utente e i suoi dati e documenti vengono sincronizzati da iCloud.

Mentre è attiva la sessione dell'utente e il dispositivo è in linea, i documenti e i dati vengono archiviati su iCloud nel momento stesso in cui vengono creati o modificati. Inoltre, un meccanismo di sincronizzazione attivo in background aiuta a garantire che, quando l'utente ha effettuato il logout, le modifiche vengano inviate ad iCloud o altri servizi web usando sessioni di background NSURLSession. Una volta completata la sincronizzazione in background per l'utente, il relativo volume APFS viene disattivato e non potrà essere riattivato se l'utente non effettua nuovamente l'accesso.

Con le sessioni temporanee non avviene la sincronizzazione con iCloud e sebbene una sessione temporanea possa accedere a un servizio di sincronizzazione di terze parti come Box o Google Drive, non è possibile continuare la sincronizzazione dei dati una volta conclusa la sessione temporanea.

Uscita da un iPad condiviso

Quando un utente esce da un iPad condiviso, la sua keybag utente viene immediatamente bloccata e tutte le app vengono chiuse. Per accelerare l'accesso di un nuovo utente, iPadOS rimanda temporaneamente alcune azioni ordinarie di logout e presenta all'utente una nuova finestra di login. Se un utente accede durante questo intervallo di tempo (circa 30 secondi), l'iPad condiviso esegue le operazioni rinviate come parte della procedura di accesso al nuovo account utente. Tuttavia, se l'iPad condiviso rimane inattivo, le azioni di chiusura rinviate vengono eseguite. Durante la fase di chiusura, la finestra di login viene riavviata come se si fosse verificato un altro logout.

Quando una sessione temporanea viene terminata, l'iPad condiviso esegue la sequenza di logout completa ed elimina immediatamente il relativo volume APFS.

Sicurezza di Apple Configurator

Apple Configurator per Mac ha un design flessibile, sicuro e incentrato sul dispositivo che consente a un amministratore di configurare in modo semplice e veloce uno o decine di dispositivi iOS, iPadOS e tvOS connessi a un Mac tramite USB (o dispositivi tvOS abbinati tramite Bonjour) prima di consegnarli agli utenti. Con Apple Configurator per Mac, un amministratore può aggiornare il software, installare app e profili di configurazione, rinominare e modificare gli sfondi dei dispositivi, esportare documenti e informazioni del dispositivo e molto altro ancora.

Inoltre, Apple Configurator per Mac è in grado di ripristinare i Mac con chip Apple e quelli con chip di sicurezza Apple T2. Quando un Mac viene ripristinato in questo modo, il file contenente gli ultimi aggiornamenti secondari per i sistemi operativi (macOS, recoveryOS per chip Apple o sepOS per T2) viene scaricato in modo sicuro dai server Apple e installato direttamente sul Mac. Al termine del ripristino, il file viene eliminato dal Mac su cui è in esecuzione Apple Configurator. L'utente non potrà in nessun caso ispezionare o utilizzare il file al di fuori di Apple Configurator.

Gli amministratori possono anche scegliere di aggiungere i dispositivi ad Apple School Manager o Apple Business Essentials tramite Apple Configurator per Mac o Apple Configurator per iPhone, anche se i dispositivi non sono stati acquistati direttamente da Apple o da un rivenditore o gestore autorizzato. Quando l'amministratore configura un dispositivo registrato manualmente, il dispositivo si comporta come qualsiasi altro dispositivo in uno dei tre servizi, con supervisione obbligatoria e registrazione in una soluzione MDM. Per i dispositivi che non sono stati acquistati direttamente, l'utente dispone di un periodo temporaneo di 30 giorni per dissociare il dispositivo da uno dei tre servizi, supervisione ed MDM.

Inoltre, le organizzazioni possono utilizzare Apple Configurator per Mac per attivare i dispositivi iOS, iPadOS e tvOS che non dispongono di alcuna connessione internet, connettendoli a un host Mac dotato di connessione mentre vengono configurati. Gli amministratori possono ripristinare, attivare e preparare i dispositivi con le configurazioni necessarie, tra cui app, profili e documenti, senza doverli mai connettere al Wi-Fi o alla rete cellulare. Questa funzionalità non consente a un amministratore di bypassare eventuali requisiti del blocco attivazione normalmente necessari durante l'attivazione senza collegamento fisico a un host.

Sicurezza di “Tempo di utilizzo”

È una funzionalità integrata che consente di gestire il tempo che gli adulti e i minori dedicano all’utilizzo di app, siti web e altro ancora. Esistono due tipi di utenti: adulti e minori (gestiti).

Sebbene “Tempo di utilizzo” non sia una nuova funzionalità di sicurezza del sistema, è importante comprendere come protegge la privacy e la sicurezza dei dati raccolti e condivisi tra i dispositivi. “Tempo di utilizzo” è disponibile con iOS 12 e versioni successive, iPadOS 13.1 e versioni successive, macOS 10.15 e versioni successive e per alcune funzionalità di watchOS 6 e versioni successive.

La tabella di seguito descrive le funzionalità principali di “Tempo di utilizzo”.

Funzionalità	**Sistema operativo supportato**
Visualizzare i dati di utilizzo	iOS iPadOS macOS
Stabilire restrizioni aggiuntive	iOS iPadOS macOS watchOS
Impostare limitazioni per l’uso del web	iOS iPadOS macOS
Impostare limitazioni per l’uso delle app	iOS iPadOS macOS watchOS
Configurare pause di utilizzo	iOS iPadOS macOS watchOS

Per gli utenti che gestiscono l’utilizzo del proprio dispositivo, i controlli e i dati di utilizzo di “Tempo di utilizzo” possono essere sincronizzati tra i dispositivi associati allo stesso account iCloud tramite la codifica end-to-end di CloudKit. Per questo è necessario che sull’account dell’utente sia abilitata l’autenticazione a due fattori (di default la sincronizzazione è attiva). “Tempo di utilizzo” sostituisce la funzionalità Restrizioni presente nelle versioni precedenti di iOS e iPadOS e la funzionalità Controlli Parentali presente nelle versioni precedenti di macOS.

In iOS 13 o versioni successive, iPadOS 13.1 o versioni successive e macOS 10.15 o versioni successive, gli utenti e i bambini gestiti in “Tempo di utilizzo” condividono automaticamente l’utilizzo su tutti i dispositivi se per il loro account iCloud è attivata l’autenticazione a due fattori. Quando un utente cancella la cronologia di Safari o elimina un’app, i dati di utilizzo corrispondenti vengono rimossi dal dispositivo e da tutti quelli sincronizzati.

Genitori e “Tempo di utilizzo”

I genitori possono utilizzare “Tempo di utilizzo” sui dispositivi iOS, iPadOS e macOS anche per capire e controllare l’utilizzo del dispositivo da parte dei loro figli. Se il genitore è l’organizzatore di una famiglia (in “In famiglia” di iCloud), può visualizzare i dati di utilizzo e gestire le impostazioni di “Tempo di utilizzo” per i propri figli. I figli vengono informati del fatto che i genitori hanno attivato “Tempo di utilizzo” e possono monitorare il proprio utilizzo anche personalmente. Quando i genitori attivano “Tempo di utilizzo” per i figli, impostano un codice che impedisce ai figli di effettuare modifiche. Al compimento della maggiore età (che varia a seconda del paese o della zona), i figli possono disattivare il monitoraggio.

I dati di utilizzo e le impostazioni di configurazione vengono trasferite tra i dispositivi dei genitori e dei figli tramite il protocollo codificato end-to-end Apple Identity Service (IDS). I dati codificati potrebbero essere brevemente archiviati sui server di IDS finché non vengono letti dal dispositivo ricevente (ad esempio, appena iPhone o iPad vengono accesi, se erano spenti). I dati non possono essere letti da Apple.

Analisi di “Tempo di utilizzo”

Se l’utente attiva “Condividi dati iPhone e Watch”, solo i seguenti dati resi anonimi vengono raccolti, in modo che Apple possa capire in che modo viene usato “Tempo di utilizzo”:

- Se “Tempo di utilizzo” è stato attivato durante Impostazione Assistita o in seguito in Impostazioni.
- In caso di modifica nell’uso di una categoria dopo che è stato creato un limite apposito (entro 90 giorni).
- Se “Tempo di utilizzo” è attivato.
- Se è abilitata una pausa di utilizzo.
- Il numero di volte che “Richiedi più tempo” è stato utilizzato.
- Numero di limitazioni per le app.
- Numero di volte in cui gli utenti hanno visualizzato l’uso nella schermata delle impostazioni di “Tempo di utilizzo”, per tipo di utente e per tipo di visualizzazione (locale, remota, widget).
- Numero di volte in cui gli utenti ignorano un limite, per tipo di utente.
- Numero di volte in cui gli utenti eliminano un limite, per tipo di utente.

Apple non raccoglie nessun dato specifico sull’utilizzo delle app o del web. Quando un utente visualizza un elenco di app nelle informazioni di utilizzo di “Tempo di utilizzo”, le icone delle app vengono prelevate direttamente da App Store, che non conserva nessun dato da questa richiesta.

Glossario

Accesso diretto alla memoria (DMA) Funzionalità che consente ai sottosistemi hardware di accedere direttamente alla memoria principale a prescindere dalla CPU.

AES (Advanced Encryption Standard) Noto standard per la codifica dei dati che consente di mantenere private le informazioni.

AES-XTS Modalità di AES definita nell'IEEE 1619-2007 ideata per la codifica dei supporti di archiviazione.

APFS (Apple File System) Il file system di default per iOS, iPadOS, tvOS, watchOS e per i Mac con macOS 10.13 o versioni successive. APFS fornisce una codifica sicura, condivisione dello spazio, istantanee, dimensionamento rapido delle directory e funzionalità fondamentali migliorate.

Apple Business Manager Un portale web di facile utilizzo pensato per gli amministratori IT. Offre un metodo rapido ed efficiente per la distribuzione dei dispositivi che le organizzazioni acquistano direttamente da Apple o da un rivenditore o gestore autorizzato. Le organizzazioni possono registrare automaticamente i dispositivi in una soluzione di gestione dei dispositivi mobili (MDM) senza doverli toccare o preparare materialmente prima di consegnarli agli utenti.

Apple Identity Service (IDS) Directory Apple contenente le chiavi pubbliche di iMessage, gli indirizzi APN nonché i numeri di telefono e gli indirizzi e-mail utilizzati per cercare le chiavi e gli indirizzi dei dispositivi.

Apple School Manager Un portale web di facile utilizzo pensato per gli amministratori IT. Offre un metodo rapido ed efficiente per la distribuzione dei dispositivi che le organizzazioni acquistano direttamente da Apple o da un rivenditore o gestore autorizzato. Le organizzazioni possono registrare automaticamente i dispositivi in una soluzione di gestione dei dispositivi mobili (MDM) senza doverli toccare o preparare materialmente prima di consegnarli agli utenti.

ASLR (Address Space Layout Randomization) Tecnica adottata dai sistemi operativi per rendere la riuscita di un attacco da parte di un bug software molto più difficile. Dato che gli indirizzi e gli offset della memoria sono imprevedibili, questi valori non possono essere fissati nel codice di exploit.

Autorizzazione software di sistema Un processo che unisce le chiavi di codifica integrate nell'hardware a un servizio in linea per verificare che con la nuova versione venga fornito e installato unicamente software valido di Apple, appropriato per i dispositivi supportati.

Bit seed del software Bit dedicati nel motore AES di Secure Enclave che vengono applicati all'UID quando vengono generate chiavi da quest'ultimo. Ogni bit seed del software ha un bit di blocco corrispondente. La ROM di avvio di Secure Enclave e il sistema operativo possono modificare indipendentemente il valore di ogni bit seed del software solo se il bit di blocco corrispondente non è stato impostato. Una volta che il bit di blocco è stato impostato, non è possibile modificare né il bit seed del software né il bit di blocco. I bit seed del software e i rispettivi blocchi vengono ripristinati quando Secure Enclave si riavvia.

Boot Camp Utility del Mac che supporta l'installazione di Microsoft Windows sui computer Mac supportati.

Boot ROM Il primo codice eseguito dal processore di un dispositivo al momento dell'avvio. In quanto parte integrante del processore, non può essere alterato né da Apple né da un malintenzionato.

Bootloader di livello inferiore Sui computer Mac con un'architettura di avvio a due fasi, il bootloader di livello inferiore contiene il codice invocato dalla ROM di avvio e che a sua volta carica iBoot nell'ambito della procedura di avvio sicura.

Bus eSPI (Enhanced Serial Peripheral Interface) Bus all-in-one progettato per le comunicazioni seriali sincrone.

Chiave del file system Chiave che codifica i metadati di ciascun file, inclusa la relativa chiave di classe. È conservata nella Effaceable Storage per consentire un'inizializzazione veloce più che per garantirne la riservatezza.

Chiave derivata dal codice Chiave di codifica derivata dalla combinazione tra la password dell'utente, la chiave SKP a lungo termine e l'UID di Secure Enclave.

Chiave multimediale Parte della gerarchia delle chiavi di codifica che aiuta a fornire un'inizializzazione sicura e immediata. Su iOS, iPadOS, tvOS e watchOS, la chiave multimediale cifra i metadati sul volume di dati (quindi, senza di essa, l'accesso a tutte le chiavi per file è impossibile e tutti i file protetti dalla protezione dati sono inaccessibili). In macOS, la chiave multimediale cifra i contenuti delle chiavi, tutti i metadati e i dati sul volume protetto da FileVault. In ogni caso, la cancellazione della chiave multimediale rende inaccessibili i dati codificati.

Chiave per file La chiave utilizzata dalla protezione dati per codificare un file sul file system. La chiave per file è cifrata da una chiave di classe e archiviata nei metadati del file.

Cifratura della chiave Codificare una chiave con un'altra. iOS e iPadOS utilizzano l'algoritmo di cifratura chiavi NIST AES, come da RFC 3394.

Circuito integrato Detto anche *microchip*.

CKRecord Dizionario delle coppie chiave-valore che contengono dati salvati o recuperati da CloudKit.

Componente Secure Storage Un chip progettato con un codice immutabile di sola lettura, un generatore di numeri casuali hardware, motori crittografici e un sistema di rilevamento di manomissione fisica. Sui dispositivi supportati, Secure Enclave è abbinato a un componente di archiviazione sicura per l'archiviazione dei valori anti-replay. Per leggere e aggiornare i valori anti-replay, Secure Enclave e il chip di archiviazione impiegano un protocollo sicuro che aiuta a garantire un accesso esclusivo ai valori anti-replay. Esistono varie generazioni di questa tecnologia, ognuna con differenti capacità di sicurezza.

Controller della memoria Sottosistema nel SoC che controlla l'interfaccia tra il SoC e la relativa memoria principale.

Controller SSD Sotto-sistema hardware che gestisce il supporto di archiviazione (SSD).

Data vault Un meccanismo, implementato dal kernel, che ha lo scopo di proteggere dall'accesso non autorizzato ai dati, indipendentemente dal fatto che l'app che li richiede sia in sandbox.

Derivazione Processo tramite il quale il codice di un utente viene trasformato in una chiave crittografica e rinforzato con l'UID del dispositivo. Questo processo aiuta a garantire che un eventuale attacco di forza bruta debba essere effettuato direttamente sul dispositivo, e quindi sia limitato per numero di tentativi possibili e non eseguibile in parallelo. L'algoritmo di derivazione è PBKDF2, che utilizza la codifica AES basata sull'UID del dispositivo come funzione pseudo casuale per ciascuna iterazione.

ECDSA (Elliptic Curve Digital Signature Algorithm) Un algoritmo di firma digitale basato sulla crittografia a curva ellittica.

ECID (Identificatore unico del processore) Identificatore a 64 bit specifico del processore in ciascun dispositivo iPhone o iPad.

Effaceable Storage Area dedicata della memoria NAND utilizzata per memorizzare chiavi di codifica; può essere interrogata direttamente e cancellata in maniera sicura. Anche se non costituisce una protezione quando il malintenzionato è materialmente in possesso del dispositivo, le chiavi conservate nella Effaceable Storage possono essere utilizzate nell'ambito di una gerarchia di chiavi per consentire un'inizializzazione veloce e aumentare così la sicurezza.

Firmware UEFi (Unified Extensible Firmware Interface) Tecnologia che sostituisce il BIOS per connettere il firmware al sistema operativo di un computer.

Gatekeeper Una tecnologia disponibile con macOS per aiutarti a garantire che sul Mac di un utente venga eseguito unicamente software attendibile.

Gestione dei dispositivi mobili (MDM) Servizio che consente a un amministratore di gestire da remoto i dispositivi registrati. Dopo che un dispositivo è registrato, l'amministratore può utilizzare il servizio MDM sulla rete per configurare le impostazioni ed eseguire altre attività sul dispositivo senza l'interazione dell'utente.

GID Identificatore per i gruppi di dispositivi, simile all'UID, ma comune a tutti i processori all'interno di una classe.

HMAC Un codice di autenticazione dei messaggi basato su hash che fa uso di una funzione hash crittografica.

iBoot Bootloader di seconda fase per tutti i dispositivi Apple. Codice che carica XNU nell'ambito della procedura di avvio sicura. A seconda della generazione del SoC, iBoot può essere caricato dal bootloader di livello inferiore o direttamente dalla ROM di avvio.

ID unico (UID) Chiave AES a 256 bit impressa in ciascun processore nella fase di fabbricazione. Non può essere letta dal firmware o dal software ed è utilizzata solo dal motore AES hardware del processore. Per ottenere la chiave effettiva, un hacker dovrebbe sferrare un attacco fisico altamente sofisticato e costoso contro il chip del processore. L'UID non è collegato a nessun altro identificatore sul dispositivo, nemmeno all'UDID.

JTAG (Joint Test Action Group) Strumento standard per il debug dell'hardware utilizzato dai programmatori e dagli sviluppatori di circuiti.

Keybag Struttura di dati utilizzata per conservare una raccolta di chiavi di classe. Ogni tipo (Utente, Dispositivo, Sistema, Backup, Escrow o Backup iCloud) ha lo stesso formato, ossia:

Un'intestazione contenente: versione (impostata su quattro in iOS 12 o versione successiva), tipo (sistema, backup, escrow o backup di iCloud), UUID della keybag, HMAC se la keybag è firmata e il metodo usato per la cifratura delle chiavi della classe, vincolato all'UID o PBKDF2 e insieme al salt e al conteggio delle iterazioni.

Un elenco delle chiavi di classe: UUID delle chiavi, classe (quale classe di protezione dei dati del portachiavi o del file), tipo di cifratura (solo chiave derivata da UID; chiave derivata da UID e chiave derivata da codice di accesso), chiave della classe cifrata e una chiave pubblica per le classi asimmetriche.

Mappatura angolare del disegno papillare Rappresentazione matematica della direzione e dell'ampiezza delle creste estrapolate da una porzione di impronta digitale.

Modalità DFU (Device Firmware Upgrade) Modalità in cui il codice Boot ROM del dispositivo attende di essere recuperato via USB. Lo schermo è nero, ma alla connessione con un computer su cui è installato iTunes o il Finder compare il seguente messaggio: "iTunes (o il Finder) ha rilevato un (iPhone o iPad) in modalità di recupero. L'utente deve ripristinare (iPhone o iPad) prima di usarlo con il Finder o con iTunes".

Modalità di recupero Una modalità utilizzata per ripristinare qualsiasi dispositivo, consentendo all'utente di reinstallare il sistema operativo.

Modulo di sicurezza hardware (HSM) Computer specializzato anti-manomissione che protegge e gestisce le chiavi digitali.

Motore di codifica AES Componente hardware dedicato che implementa l'AES.

NAND Memoria flash non volatile.

Portachiavi Infrastruttura e set di API utilizzati dai sistemi operativi Apple e dalle app di terze parti per archiviare e recuperare password, chiavi e altre credenziali sensibili.

Profilo di provisioning File di proprietà (.plist) firmato da Apple contenente un set di entità e autorizzazioni che permettono di installare e testare app su un dispositivo iOS o iPadOS. Un profilo di provisioning di sviluppo elenca i dispositivi scelti dallo sviluppatore per la distribuzione personalizzata, mentre il profilo di provisioning di distribuzione contiene l'ID di un'app sviluppata dall'azienda.

Programma di bug bounty sulla sicurezza di Apple (Apple Security Bounty) Riconoscimento dato da Apple ai ricercatori che segnalano una vulnerabilità riscontrata nell'ultimo sistema operativo e, se pertinente, nell'hardware più recente.

Protezione dei dati Meccanismo di protezione dei file e del portachiavi per i dispositivi Apple supportati. Può anche riferirsi alle API utilizzate dalle app per proteggere i file e gli elementi del portachiavi.

Protezione dell'integrità dei coprocessori di sistema (SCIP) Un meccanismo adoperato da Apple progettato per impedire la modifica del firmware dei coprocessori.

Protezione SKP (Sealed Key Protection) Tecnologia per la protezione dei dati che difende le chiavi di codifica *sigillandole* attraverso misurazioni del software di sistema e chiavi disponibili sono nell'hardware (come l'UID di Secure Enclave).

Registro di avanzamento dell'avvio (BPR) Insieme di marcatori hardware del SoC che il software può utilizzare per tenere traccia delle modalità di avvio intraprese dal dispositivo, come la modalità DFU o la modalità di recupero. Una volta che un marcatore del registro di avanzamento dell'avvio è impostato, non può essere eliminato. Questo consente al software successivo di ottenere un indicatore attendibile dello stato del sistema.

Scambio su curve ellittiche Diffie-Hellman con chiavi effimere (ECDHE) Un meccanismo per lo scambio di chiavi basato sulle curve ellittiche. ECDHE consente a due parti di accordarsi su una chiave segreta in un modo che impedisce alla chiave di essere scoperta da un soggetto che intercetta i messaggi scambiati dalle due parti.

sepOS Il firmware di Secure Enclave, basato su una versione personalizzata da Apple del microkernel L4.

Servizio di notifiche push di Apple (APN) Servizio fornito da Apple che trasmette notifiche push ai dispositivi Apple in tutto il mondo.

SoC (System on Chip) Circuito integrato che riunisce vari componenti su un singolo chip. Il processore per le applicazioni, Secure Enclave e altri coprocessori sono componenti del SoC.

Unità per la gestione della memoria di input/output Un'unità per la gestione della memoria di input/output. Un sottosistema in un chip integrato che controlla l'accesso allo spazio degli indirizzi da altri dispositivi e periferiche di input/output.

URI (Uniform Resource Identifier) Stringa di caratteri che identifica una risorsa web.

xART (eXtended Anti-Replay Technology) Abbreviazione di eXtended Anti-Replay Technology. Insieme di servizi che fornisce un'archiviazione codificata, autenticata e persistente a Secure Enclave, con capacità anti replay basate sull'architettura fisica dell'archiviazione. Consulta "Componente Secure Storage".

XNU Kernel alla base dei sistemi operativi Apple. È considerato attendibile e applica misure di sicurezza come la firma del codice, il sandboxing, la verifica delle autorizzazioni e la ASLR (Address Space Layout Randomization).

XProtect Tecnologia antivirus integrata in macOS per il rilevamento e la rimozione del malware basati su firme.

Cronologia delle revisioni del documento

Cronologia delle revisioni del documento

Maggio 2024

Argomenti aggiunti:

- Hash del manifesto Image4 di Cryptex1 (spih)
- Generazione Cryptex1 (stng)
- BlastDoor per Messaggi e IDS
- Sicurezza con la “Modalità di isolamento”
- Sicurezza dell’App Store
- Sicurezza di WidgetKit

Argomenti aggiornati:

- Introduzione alla sicurezza delle piattaforme Apple
- Sicurezza del SoC Apple
- Secure Enclave
- Face ID, Touch ID, codici e password
- Sicurezza del riconoscimento facciale
- Utilizzi di Face ID e Touch ID
- Carte rapide in modalità “Basso consumo”
- Integrità del sistema operativo
- Attivazione sicura delle connessioni dati
- Verifica degli accessori per iPhone e iPad
- Sicurezza del sistema in watchOS
- Codici e password
- Panoramica della protezione dati
- Keybag per la protezione dei dati
- Protezione delle chiavi nelle modalità di avvio alternative
- Protezione dei dati dell’utente dagli attacchi
- Gestire FileVault in macOS

- Introduzione alla sicurezza delle app in iOS e iPadOS
- Protezione in fase di esecuzione e Gatekeeper in macOS
- Sicurezza dell'ID Apple gestito
- Crittografia iCloud
- Sicurezza dei contatti per il recupero dell'account
- Sicurezza del contatto erede
- Panoramica sulla sicurezza del portachiavi iCloud
- Sincronizzazione sicura del portachiavi
- Sicurezza del servizio di deposito per il portachiavi iCloud
- Panoramica sulla sicurezza dell'aggiunta delle carte
- Aggiungere carte di credito o di debito ad Apple Pay
- Pagare con le carte tramite Apple Pay
- Sicurezza di Apple Card
- Sicurezza di Tap to Pay on iPhone
- Accesso tramite Apple Wallet
- Tipi di chiavi di accesso
- Documenti d'identità in Apple Wallet
- La sicurezza dei documenti d'identità in Apple Wallet
- Panoramica sulla sicurezza del kit per sviluppatori
- Sicurezza delle comunicazioni di HomeKit
- Panoramica sulla sicurezza della gestione dei dispositivi mobili
- Applicazione della configurazione

Dicembre 2022

Argomenti aggiunti:

- Protezione avanzata dei dati per iCloud

Argomenti aggiornati:

- Panoramica della sicurezza di iCloud
- Crittografia iCloud
- Sicurezza del backup di iCloud
- Sicurezza dei contatti per il recupero dell'account
- Sicurezza del contatto erede

Maggio 2022

Aggiornato per:

- iOS 15.4
- iPadOS 15.4
- macOS 12.3
- tvOS 15.4
- watchOS 8.5

Argomenti aggiunti:

- Restrizioni applicate a recoveryOS abbinato
- Versione locale del sistema operativo (Local Operating System Version, love)
- Condivisione dell'app Salute
- Sicurezza dei contatti per il recupero dell'account
- Sicurezza del contatto erede
- Sicurezza di Tap to Pay on iPhone
- Accesso tramite Apple Wallet
- Tipi di chiavi di accesso
- Documenti d'identità in Apple Wallet
- Accessori di HomeKit compatibili con Siri

Argomenti aggiornati:

- Magic Keyboard con Touch ID
- Face ID, Touch ID, codici e password
- Sicurezza del riconoscimento facciale
- Carte rapide in modalità "Basso consumo"
- Modalità di avvio per i Mac dotati di chip Apple
- Contenuti del file LocalPolicy per i Mac dotati di chip Apple
- Sicurezza del volume di sistema firmato
- Sicurezza del sistema in watchOS
- Dispositivo Apple per la ricerca sulla sicurezza
- Ruolo di Apple File System
- Protezione dell'accesso delle app ai dati utente
- Introduzione alla sicurezza delle app in macOS
- Protezione dai malware in macOS
- Panoramica della sicurezza di iCloud
- Sincronizzazione sicura del portachiavi
- Recupero sicuro del portachiavi iCloud
- Pagare con le carte tramite Apple Pay

- Biglietti contactless in Apple Pay
- Disabilitare l'uso delle carte con Apple Pay
- Richiedere Apple Card
- Sicurezza di Apple Cash
- Aggiungere carte trasporti e per i pagamenti elettronici ad Apple Wallet
- Sicurezza in Apple Messages for Business
- Sicurezza di FaceTime
- Sicurezza delle chiavi dell'automobile in iOS
- Sicurezza di Apple Configurator

Argomenti eliminati:

- Accessori HomeKit e iCloud

Maggio 2021

Aggiornato per:

- iOS 14.5
- iPadOS 14.5
- macOS 11.3
- tvOS 14.5
- watchOS 7.4

Argomenti aggiunti:

- Magic Keyboard con Touch ID.
- Rilevamento sicuro dell'intenzione e collegamenti a Secure Enclave.
- Sblocco automatico e Apple Watch.
- Hash del manifesto Image4 di CustomOS (coih).

Argomenti aggiornati:

- Aggiunte due nuove transazioni in modalità rapida in Carte rapide in modalità "Basso consumo".
- Modificata la sezione Riepilogo delle funzionalità di Secure Enclave.
- Contenuti dell'aggiornamento software aggiunti ad Avvio multiplo protetto (smb3).
- Contenuti aggiuntivi per Protezione SKP (Sealed Key Protection).

Febbraio 2021

Aggiornato per:

- iOS 14.3
- iPadOS 14.3
- macOS 11.1
- tvOS 14.3
- watchOS 7.2

Argomenti aggiunti:

- Implementazione di iBoot per la protezione della memoria
- Processo di avvio per i Mac dotati di chip Apple
- Modalità di avvio per i Mac dotati di chip Apple
- Controllo delle politiche di sicurezza per il disco di avvio per i Mac dotati di chip Apple
- Creazione e gestione della chiave per la firma di LocalPolicy
- Contenuti del file LocalPolicy per i Mac dotati di chip Apple
- Sicurezza del volume di sistema firmato
- Dispositivo Apple per la ricerca sulla sicurezza
- Monitoraggio delle password
- Sicurezza di IPv6
- Sicurezza delle chiavi dell'automobile in iOS

Argomenti aggiornati:

- Secure Enclave
- Scollegamento hardware del microfono
- Ambienti di diagnosi e recoveryOS per i Mac dotati di processore Intel
- Protezioni dell'accesso diretto alla memoria per i computer Mac
- Estensione sicura del kernel in macOS
- Protezione dell'integrità del sistema
- Sicurezza del sistema in watchOS
- Gestire FileVault in macOS
- Accesso delle app alle password salvate
- Consigli sulla sicurezza delle password
- Sicurezza di Apple Cash
- Sicurezza in Apple Messages for Business
- Privacy Wi-Fi
- Sicurezza del blocco attivazione
- Sicurezza di Apple Configurator

Aprile 2020

Aggiornato per:

- iOS 13.4
- iPadOS 13.4
- macOS 10.15.4
- tvOS 13.4
- watchOS 6.2

Aggiornamenti:

- Scollegamento hardware del microfono in iPad aggiunto a Scollegamento hardware del microfono.
- Data vault aggiunto a Protezione dell'accesso delle app ai dati utente.
- Aggiornamenti a Gestione di FileVault in macOS e Strumenti a linea di comando.
- Aggiunte a Strumento di rimozione del malware in Protezione dai malware in macOS.
- Aggiornamenti a Sicurezza di "iPad condiviso" in iPadOS.

Dicembre 2019

Unione della guida di riferimento sulla sicurezza di iOS, della panoramica sulla sicurezza di macOS e della panoramica sul chip di sicurezza Apple T2

Aggiornato per:

- iOS 13.3
- iPadOS 13.3
- macOS 10.15.2
- tvOS 13.3
- watchOS 6.1.1

Le sezioni riguardanti i controlli per la privacy, Siri e i suggerimenti di Siri e la prevenzione intelligente del tracciamento di Safari sono stati rimossi. Consulta https://www.apple.com/it/privacy/ per le informazioni più recenti su tali funzionalità.

Maggio 2019

Aggiornato per iOS 12.3

- Supporto per TLS 1.3
- Revisione della descrizione della sicurezza di AirDrop
- Modalità DFU e modalità di recupero
- Richiesta del codice per il collegamento agli accessori

Novembre 2018

Aggiornato per iOS 12.1

- Chiamate FaceTime di gruppo

Settembre 2018

Aggiornato per iOS 12 Secure Enclave

- Protezione dell'integrità del sistema operativo
- Carte rapide in modalità "Basso consumo"
- Modalità DFU e modalità di recupero
- Telecomandi TV HomeKit
- Biglietti contactless
- Tessere identificative studente
- Suggerimenti di Siri
- Abbreviazioni in Siri
- App Comandi Rapidi
- Gestione delle password dell'utente
- Tempo di utilizzo
- Certificazioni e programmi di sicurezza

Luglio 2018

Aggiornato per iOS 11.4

- Politiche per le rilevazioni biometriche
- HomeKit
- Apple Pay
- Business Chat
- Messaggi su iCloud
- Apple Business Manager

Dicembre 2017

Aggiornato per iOS 11.2

- Apple Pay Cash

Ottobre 2017

Aggiornato per iOS 11.1

- Certificazioni e programmi di sicurezza
- Touch ID/Face ID
- Note condivise
- Codifica end-to-end di CloudKit
- Aggiornamento TLS
- Apple Pay, acquisti con Apple Pay sul web
- Suggerimenti di Siri
- iPad condiviso

Luglio 2017

Aggiornato per iOS 10.3

- Secure Enclave
- Protezione dati dei file
- Keybag
- Certificazioni e programmi di sicurezza
- SiriKit
- HealthKit
- Sicurezza della rete
- Bluetooth
- iPad condiviso
- Modalità smarrito
- Blocco attivazione
- Controlli per la privacy

Marzo 2017

Aggiornato per iOS 10 Sicurezza del sistema

- Classi di protezione dati
- Certificazioni e programmi di sicurezza
- HomeKit, ReplayKit, SiriKit
- Apple Watch
- Wi-Fi, VPN
- Single Sign-On
- Apple Pay, acquisti con Apple Pay sul web
- Aggiunta di carte di credito, di debito e prepagate
- Suggerimenti di Safari

Maggio 2016

Aggiornato per iOS 9.3

- ID Apple gestito
- Autenticazione a due fattori per l'ID Apple
- Keybag
- Certificazioni di sicurezza
- Modalità smarrito, blocco attivazione
- Note protette
- Apple School Manager
- iPad condiviso

Settembre 2015

Aggiornato per iOS 9 Blocco attivazione di Apple Watch

- Politiche per il codice
- Supporto per l'API di Touch ID
- La protezione dati su A8 utilizza AES-XTS
- Keybag per aggiornamenti software automatici
- Aggiornamenti delle certificazioni
- Modello di attendibilità delle app aziendali
- Protezione dati per i segnalibri di Safari
- Sicurezza dei trasferimenti delle app
- Specifiche VPN
- Accesso remoto iCloud per HomeKit
- Carte fedeltà di Apple Pay, app dell'ente di emissione della carta di Apple Pay
- Indicizzazione sul dispositivo di Spotlight
- Modello di abbinamento di iOS
- Apple Configurator 2
- Restrizioni

Copyright

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

T028-00780