Apple CarPlay

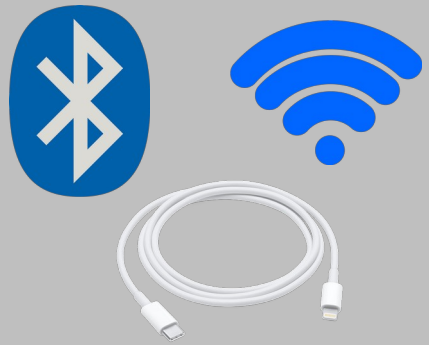
What's Under the Hood

Hannah Nöttgen

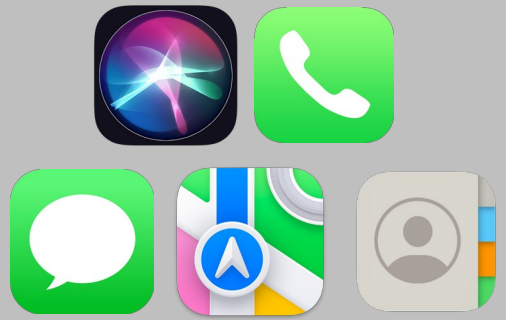
TECHNISCHE UNIVERSITÄT DARMSTADT

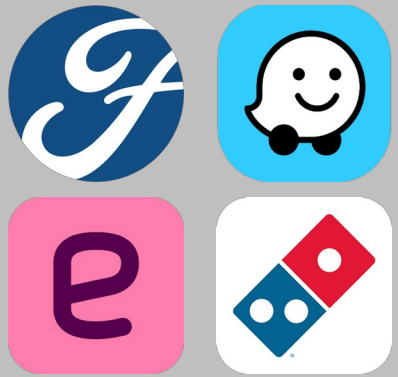
SEEMOO
SECURE MOBILE NETWORKING

What is CarPlay?




4:21 PM
100%
CarPlay

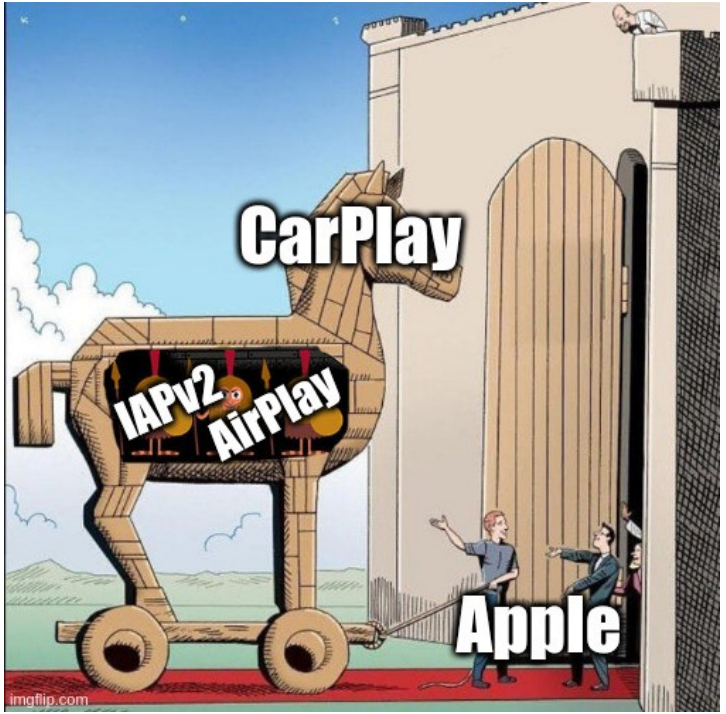





2:48
LTE
Phone
Music
Maps
Messages
Now Playing
Calendar
Podcasts
Audiobooks

Don't Reinvent the Wheel

- Apple CarPlay is a fusion of two protocols
- **IAPv2** for the main purpose of authentication
- **AirPlay** as Apple's known streaming protocol



Why is CarPlay an attractive target?

Launching apps
with voice,
gesture and
keyboard **input**

Access to private information
(iMessage, calls, E-Mail)
→ without unlocking

Compromising
driver safety

Setups

Head Units

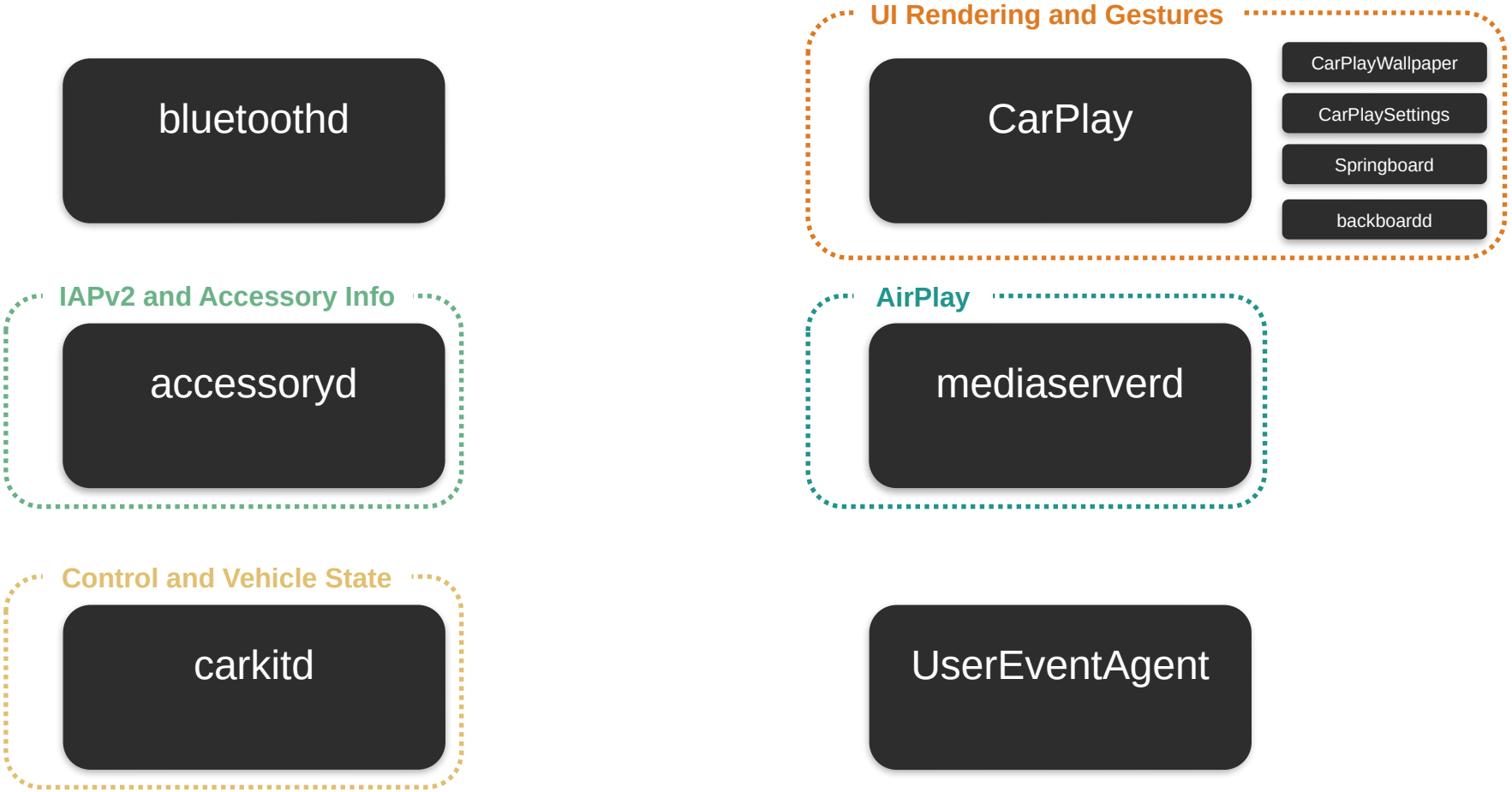
- **Ford SYNC 3** head unit
- Built into a Ford Focus from 2020
- Only wired CarPlay
- Problem: Draining battery and driver safety

- **Sony XAV-AX1005DB** head unit
- Stand-alone
- Only wired CarPlay

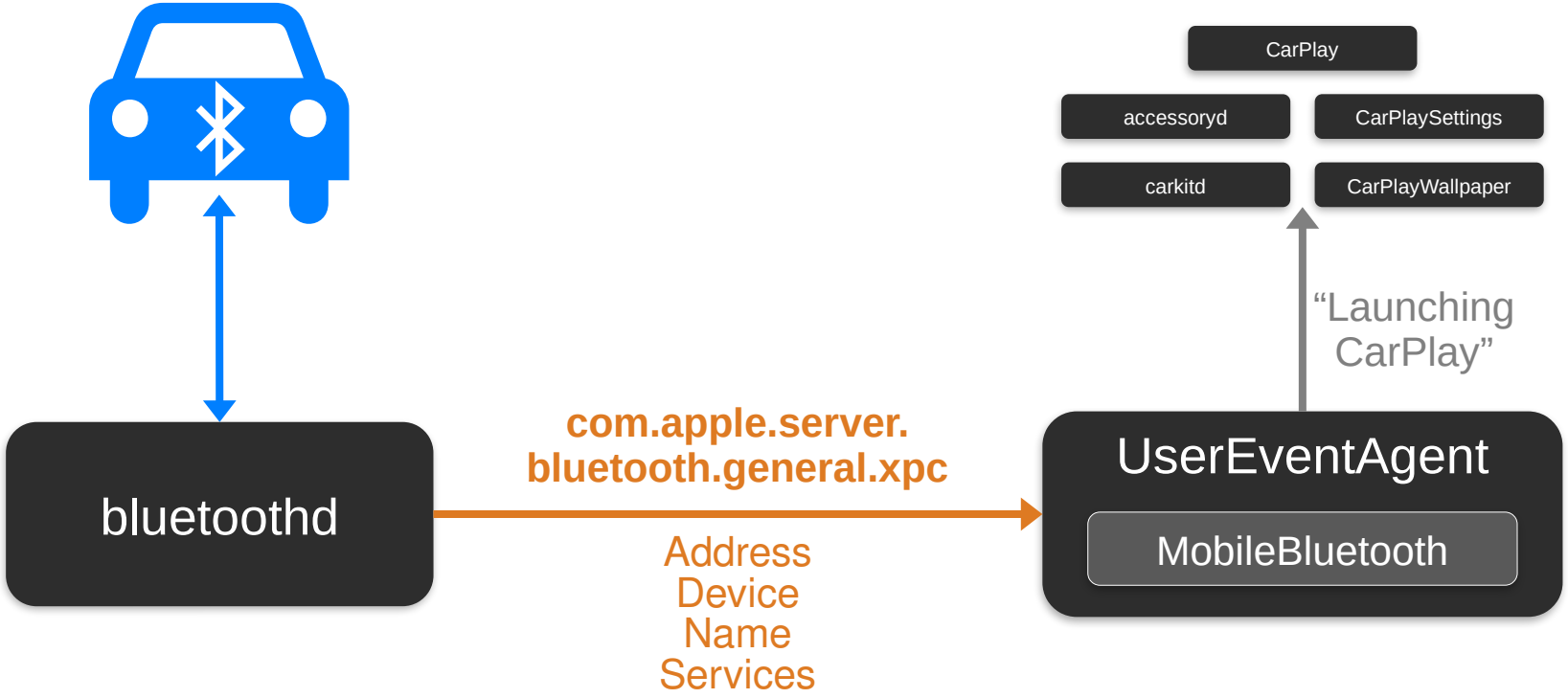

BELL
4:21 PM
100%
CarPlay
FRIDA


Carlinkit
CPC200-CP2A
CarPlay
FRIDA

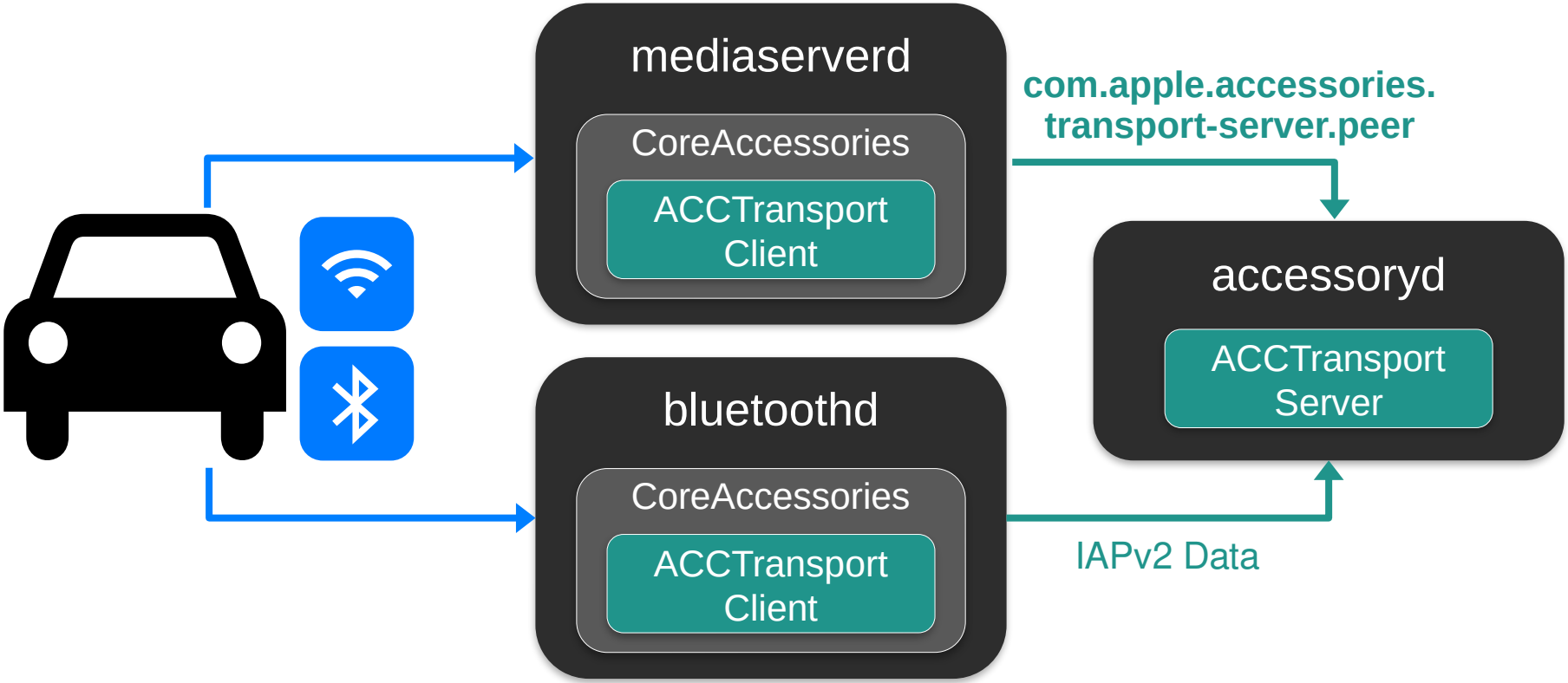
Deamons and Frameworks


bluetoothd
UI Rendering and Gestures
CarPlay
CarPlayWallpaper
CarPlaySettings
Springboard
backboardd
IAPv2 and Accessory Info
accessoryd
AirPlay
mediaserverd
Control and Vehicle State
carkitd
UserEventAgent

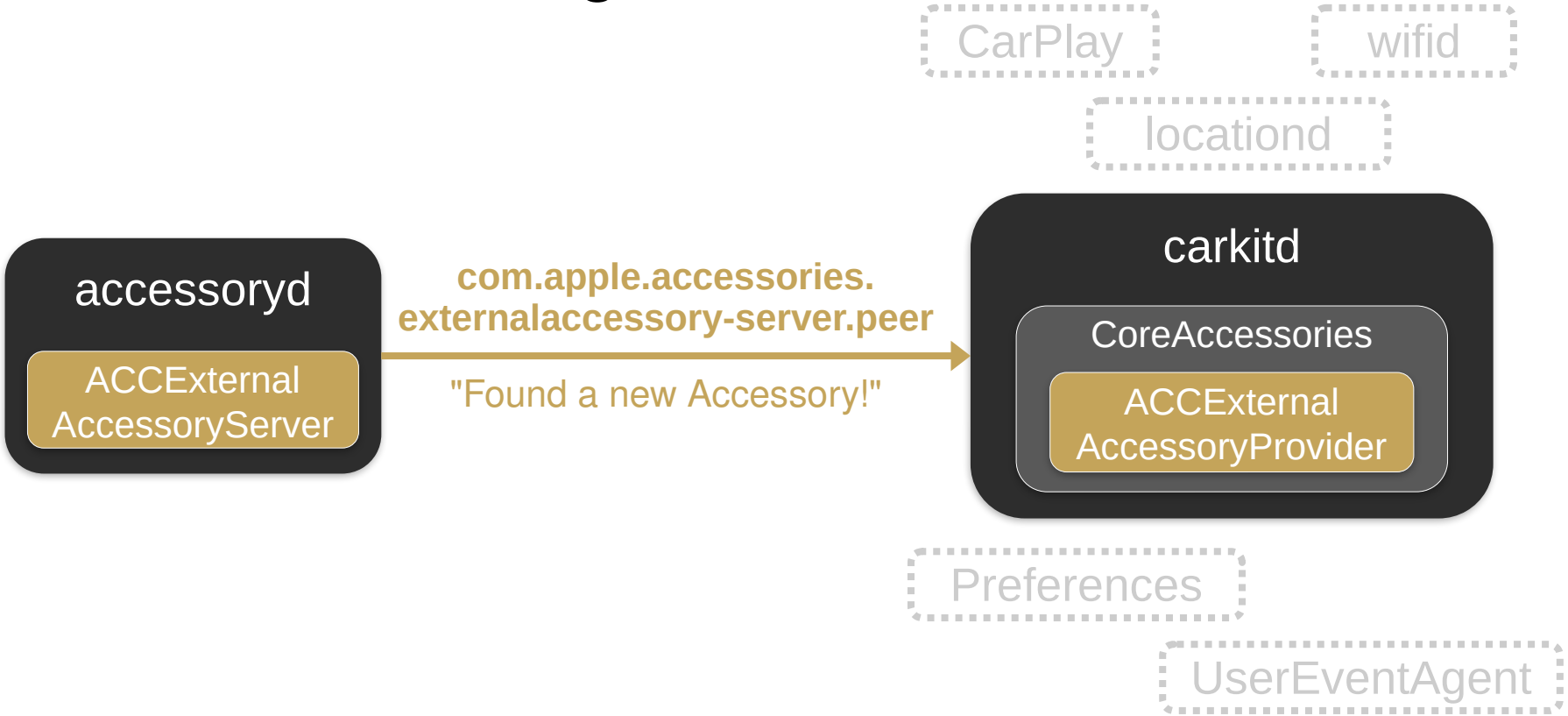
Starting CarPlay



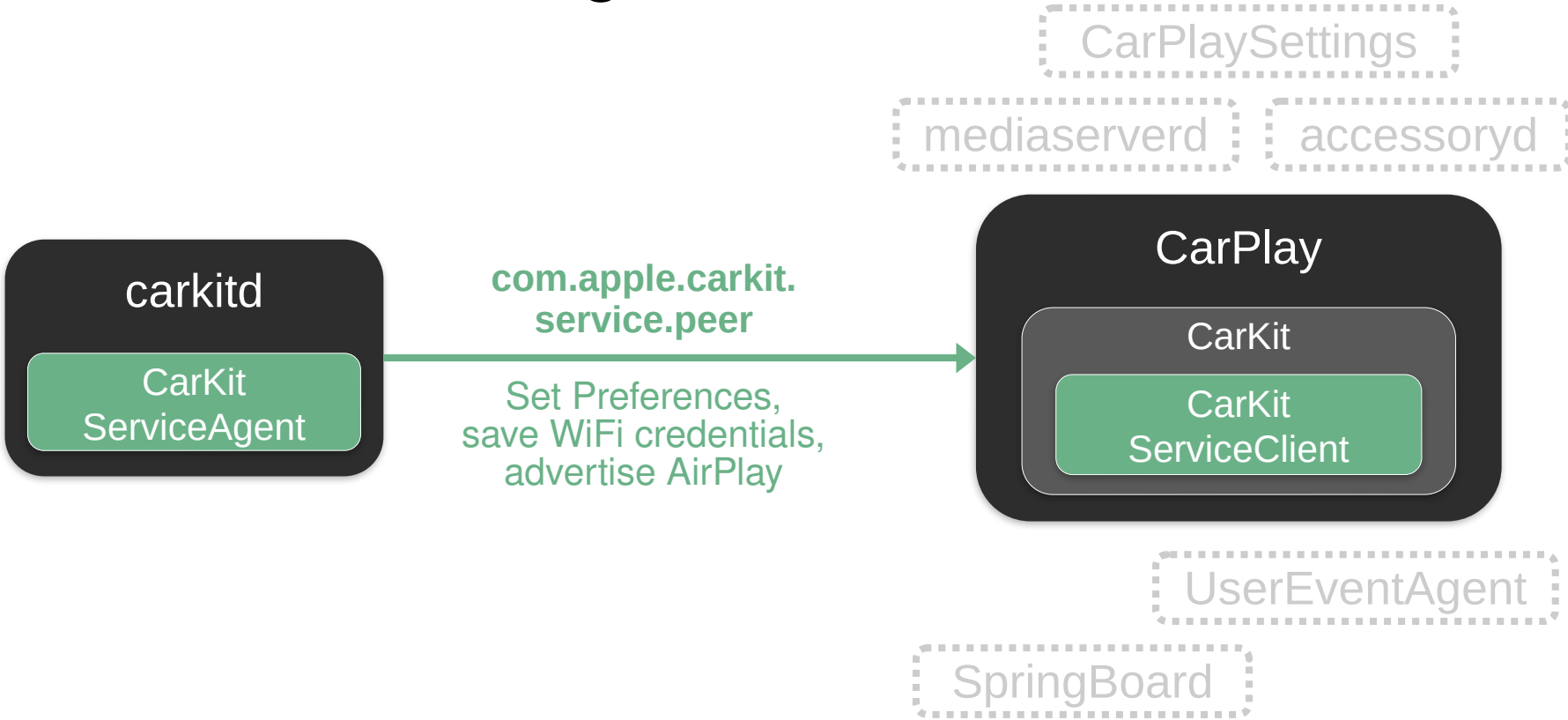
Forwarding iAPv2 Data



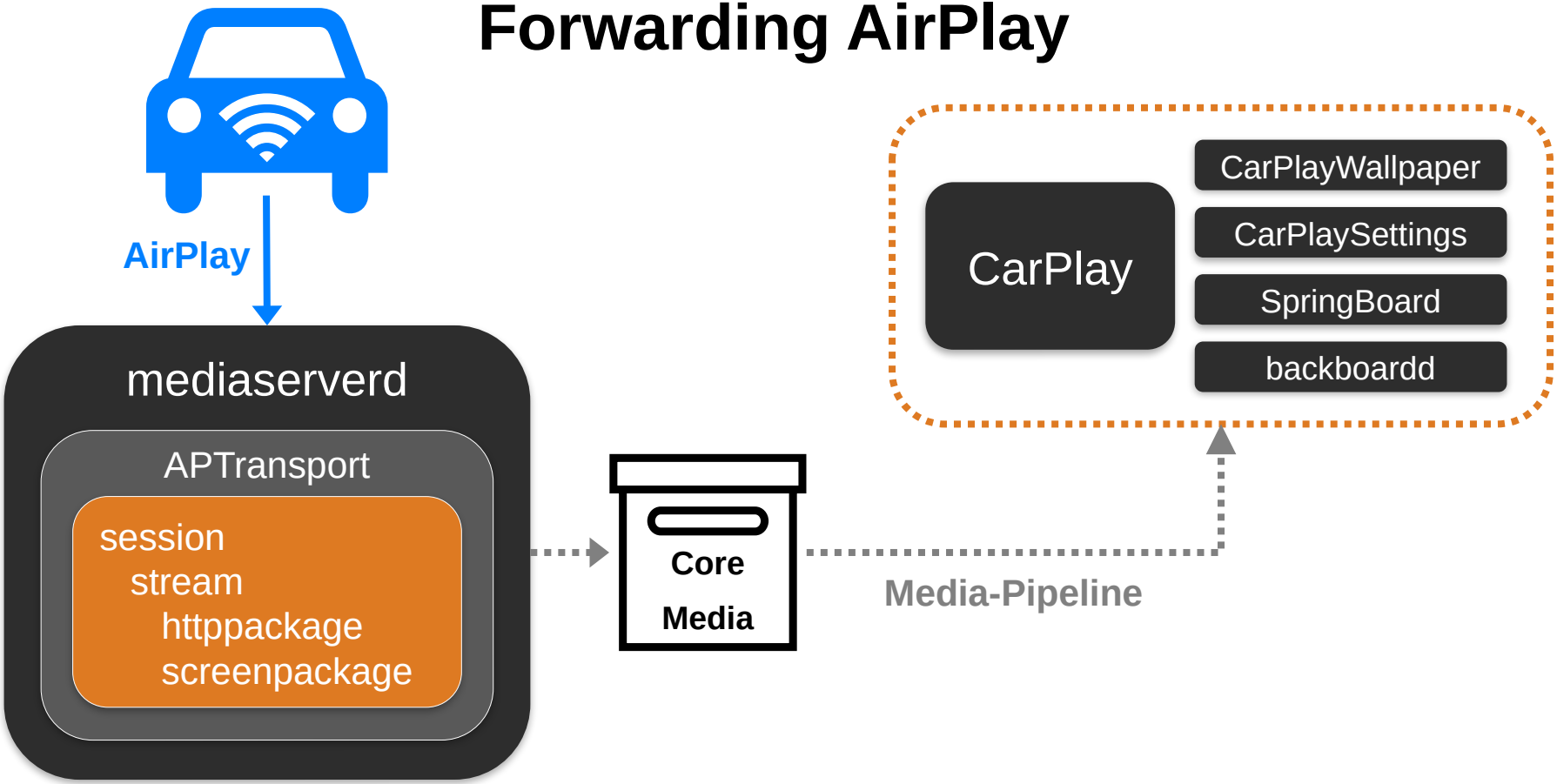
Distributing Vehicle Information



Distributing Vehicle Information



Forwarding AirPlay

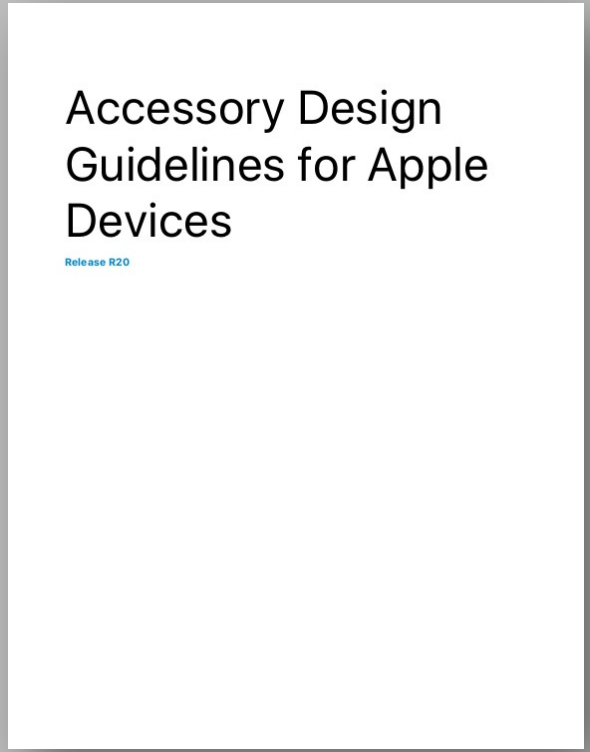


iPod Accessory Protocol Version 2

Information provided by Apple:

"Accessories may use the iAP2 protocol to access advanced device features."

- Specification is closed source and part of the MFi program
- Every manufactured device is charged with a fee and has an Apple authentication processor

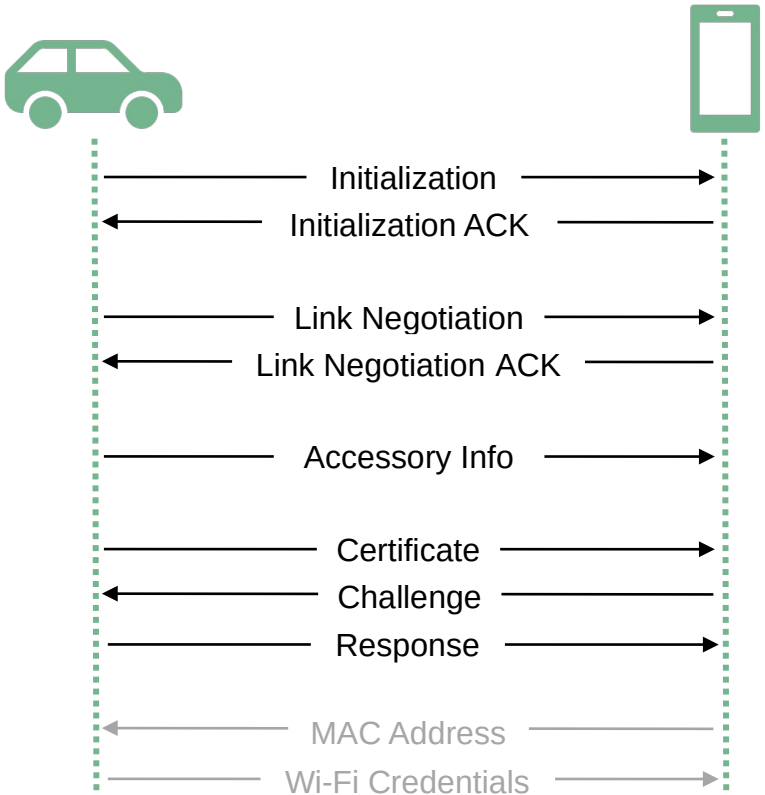


What we found out so far ...

- Proprietary protocol from Apple for …
  - ... transmitting accessory data
  - … accessory authentication
  - ... out-of-band establishment of Wi-Fi connections

- Build on top of varoius communication stacks

iAPv2 Protocol



- Link initialization
- Accessory information
- Authentication
- Wi-Fi Handover

iAPv2 Packets

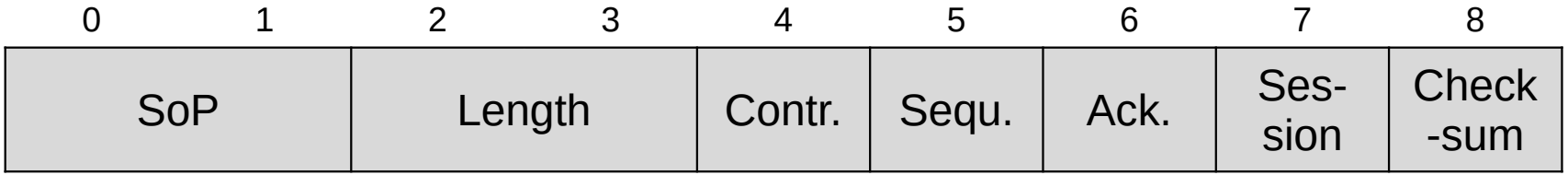
ff55 type

0	1	2	3	4	5
SoP MSB	SoP LSB	Length	Lingo	Command ID LSB	Checksum

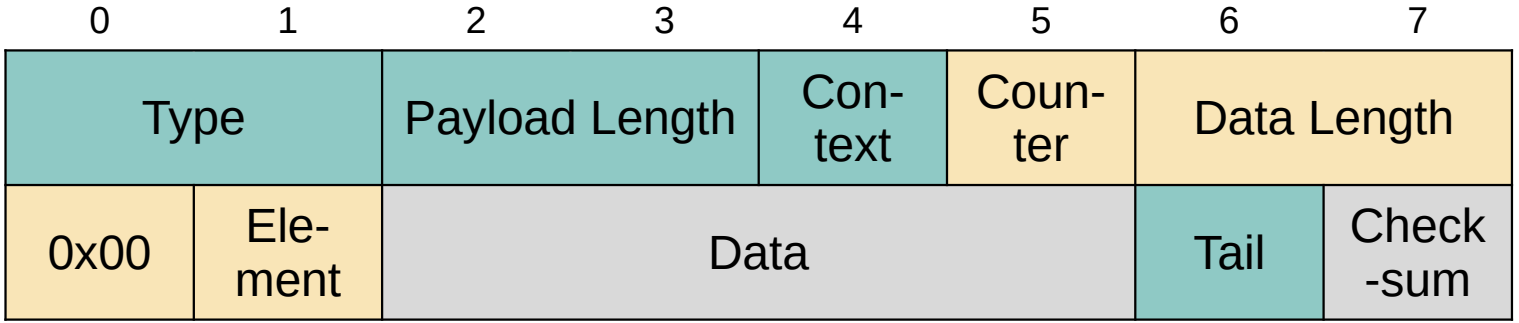
- Only the first two packets are ff55 types
- Has always the same content: 0x ff 55 02 00 ee 10
- Checksum is a one-byte 2’s complement

iAPv2 Packets

ff5a type



… plus session data



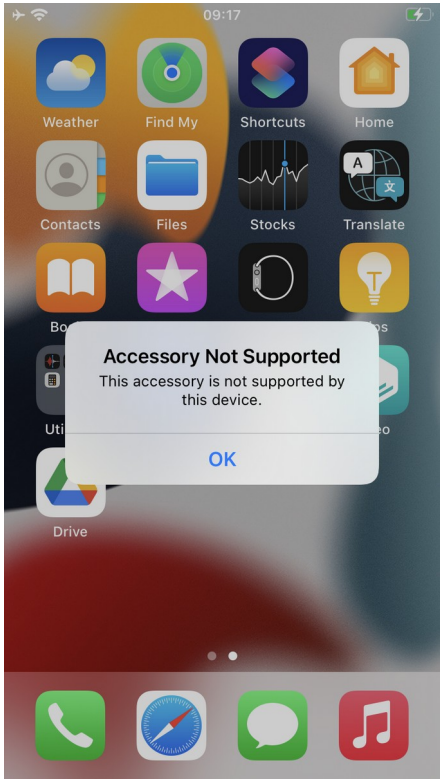
iAPv2 Accessory Authentication

Certificate

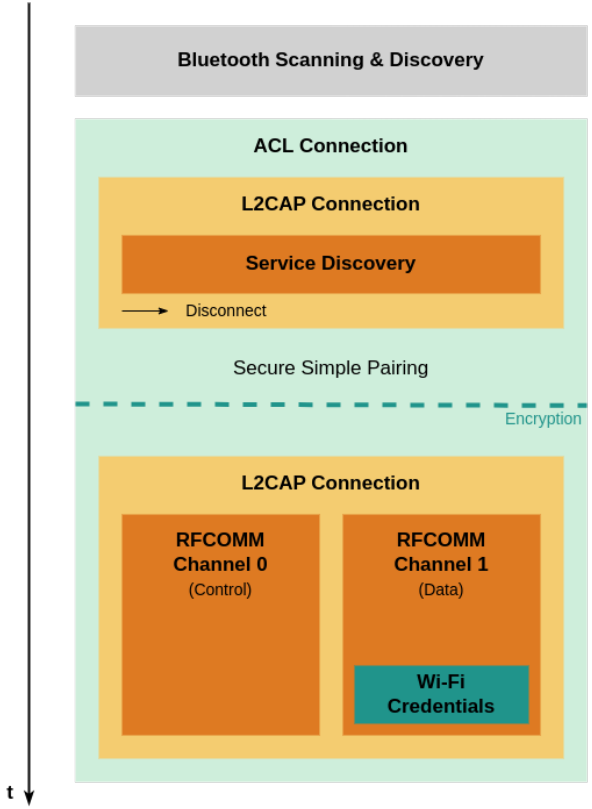
- MFi chip of each accessory holds a X.509 certificate
- Only the accessory authenticates

Challenge-Response

- iPhone generating a 19-byte nonce
- Head unit signs it with RSA signature



Wi-Fi Handover for Wireless CarPlay

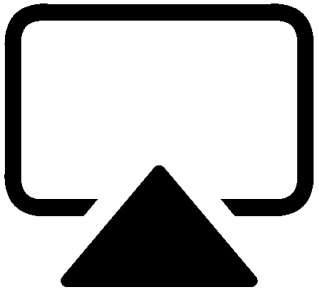


- Standard device discovery
- Running Service Discovery Protocol on top of L2CAP
- Traffic is encrypted after pairing
- Establishment of two RFCOMM channels
  - Channel 0: Multiplexing between ports
  - Channel 1: For communication via iAPv2

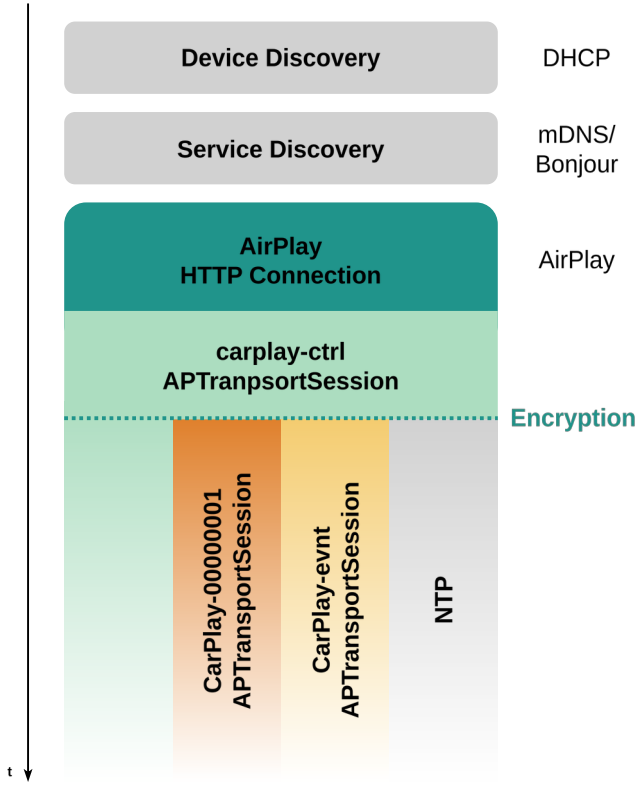
Apple AirPlay

What is known about AirPlay?

- Apple's proprietary protocol for transmission of video and audio
- Communication between two devices that share the same Wi-Fi network
- Partly open source, partly close source (MFi)
- Some reversing effort of other researchers and open-source implementations like OpenAirplay

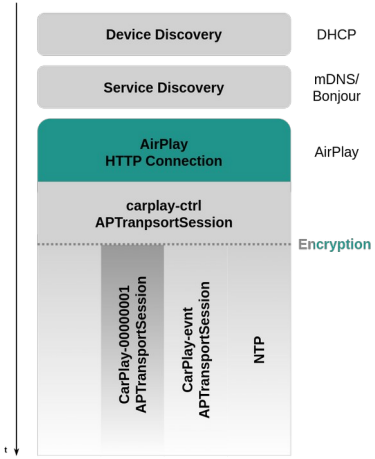


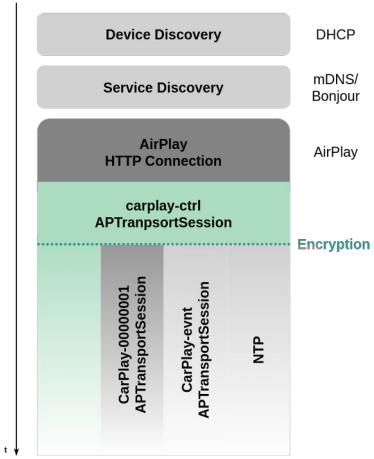
AirPlay for CarPlay



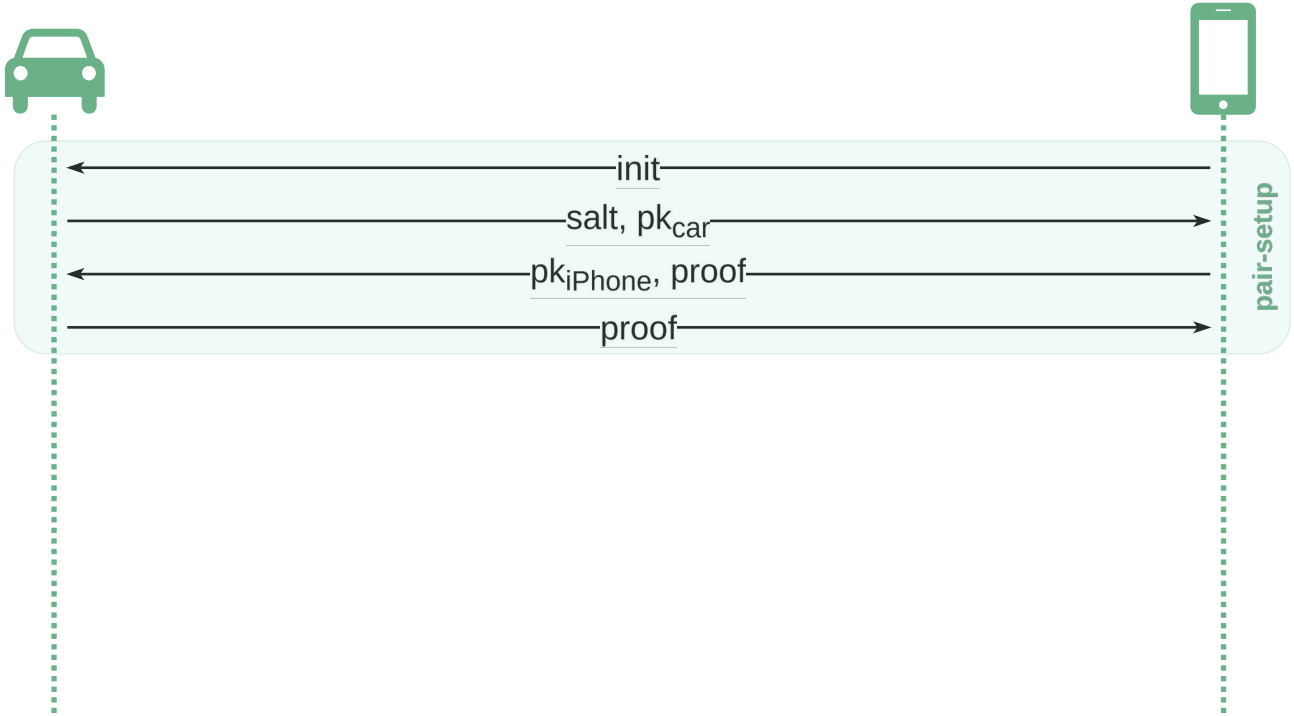
- Device discovery over IPv6 Neighbor Discovery Protocol (NDP) or IPv4 Dynamic Host Configuration Protocol (DHCP)
- Service Discovery over Apple’s custom mDNS protocol Bonjour
- Starting four TCP streams for AirPlay and one UDP stream for time synchronization

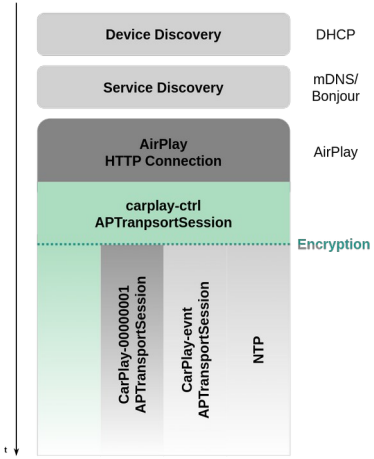
HTTP Connection



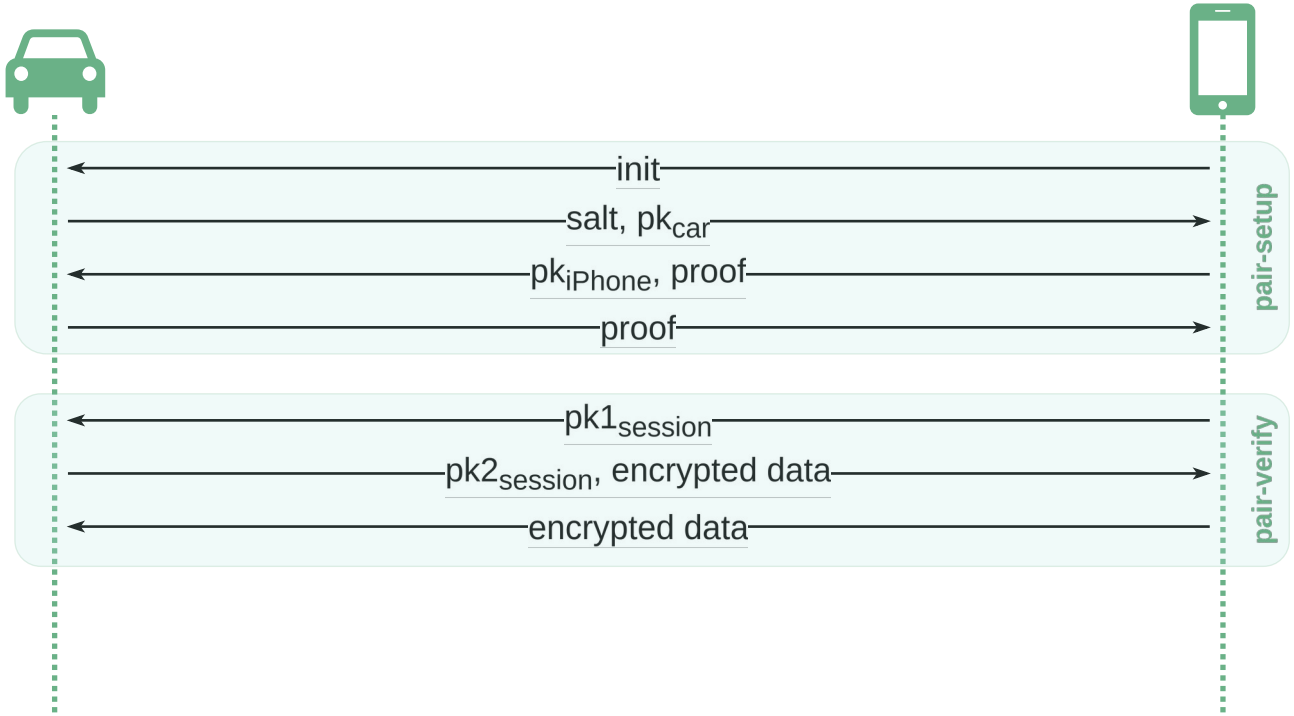


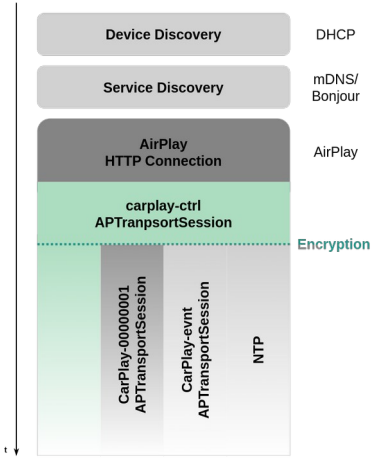
carplay-ctrl



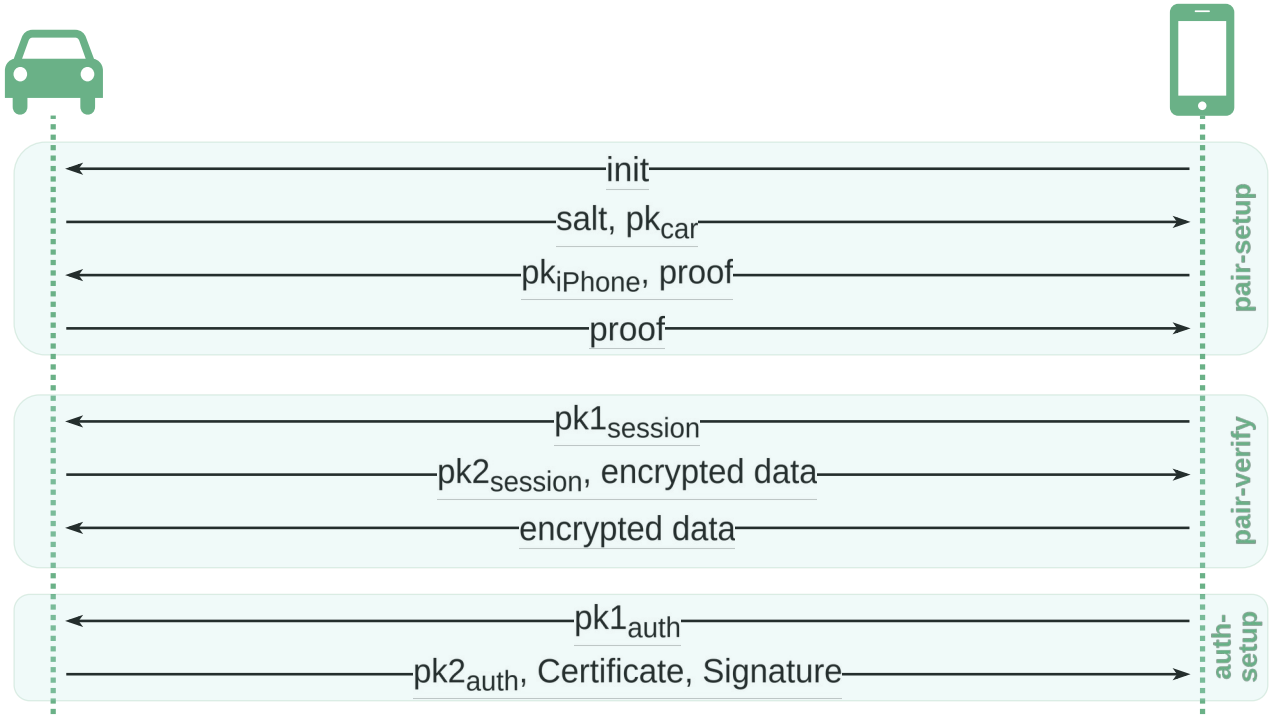


carplay-ctrl





carplay-ctrl



Further carplay-ctrl Tasks

Setup streams

```
SETUP rtsp://192.168.50.2/16...
Content-Length: 451
Content-Type:
  application/x-apple-binary-plist
CSeq: 6

Data:
  <plist version="1.0">
  <dict>
    <key>timingPort</key>
    <integer>63778</integer>
    ...
```

Setup HID

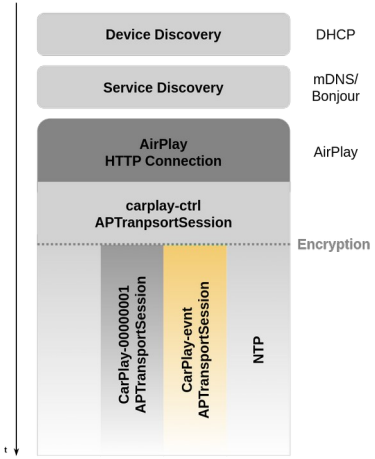
```
RTSP/1.0 200 OK
Content-Length: 1997
Content-Type:
  application/x-apple-binary-plist
Server: AirTunes/320.17
CSeq: 7


Data:
  <plist version="1.0">
  ...
  <dict>
    <key>hidCountryCode</key>
    <integer>33</integer>
    <key>displayUUID</key>
    <string>e5f7a68d-7b0f-4305-
            984b-974f677a150b
    </string>
    <key>name</key>
    <string>MultiTouchScreen</string>
    ...
```

Switch-off Bluetooth

```
POST /command RTSP/1.0
Content-Length: 115
Content-Type:
  application/x-apple-binary-plist
CSeq: 10

Data:
  <plist version="1.0">
  <dict>
    <key>type</key>
    <string>disableBluetooth</string>
    <key>params</key>
    <dict>
      <key>deviceID</key>

<string>70:ef:00:7f:ab:f4</string>
      ...
```

Feedback

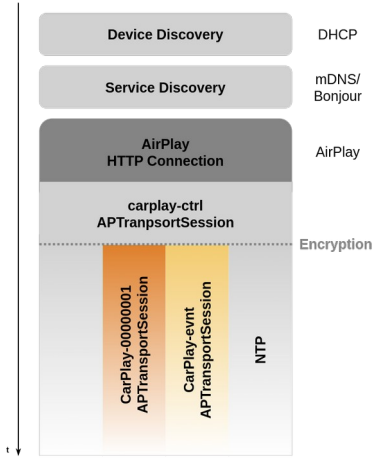
```
POST /feedback RTSP/1.0
CSeq: 27


RTSP/1.0 200 OK
Content-Length: 0
Server: AirTunes/320.17
CSeq: 27
```



carplay-evnt

- the same iAPv2 communication as via Bluetooth/USB
- Redundant since we had a *auth-setup* phase

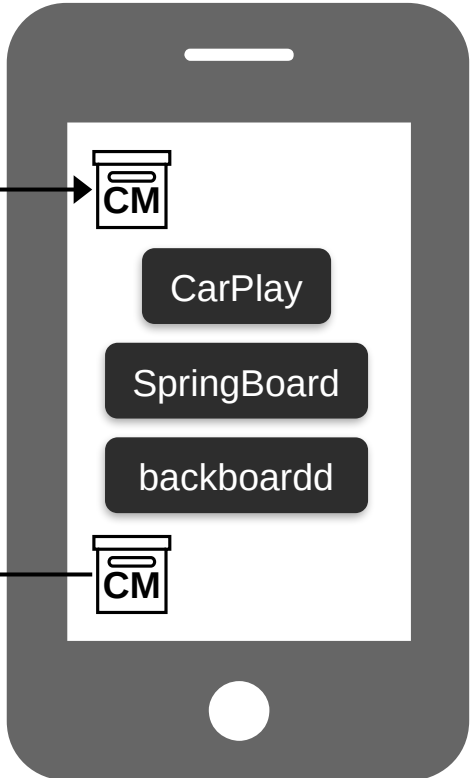
- **Possible reasons:**
  - *accessoryd* has no access to AirPlay
  - Compatibility between wireless and wired CarPlay



carplay-evnt

carplay-evnt

“HID Report”



CarPlay-00000001

HEVC Video

Security Analysis

Disclosure

Reported on 27.03.2024

Request for confidentiality 17.06.2024

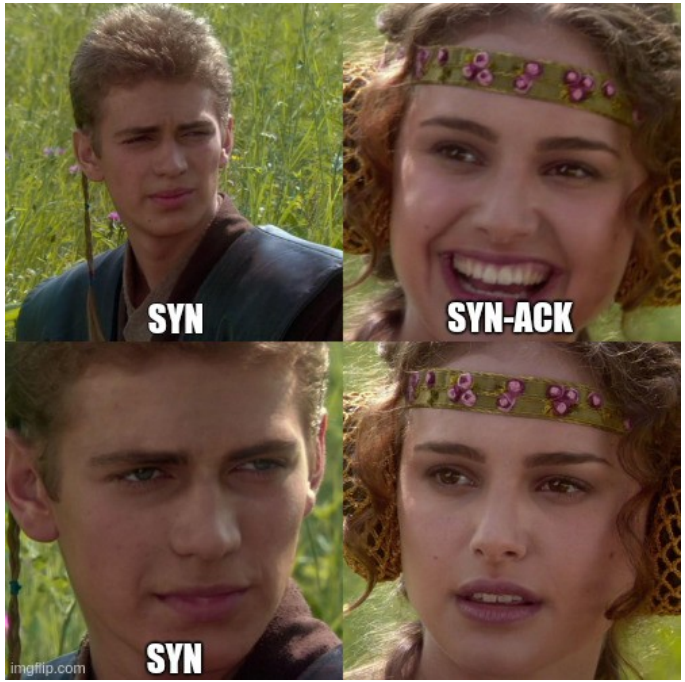
Planned patching date still open

Availability

- **DoS:** SYN-Flooding AirPlay on iPhone or head unit ✓

  → Attacker needs access to the WiFi Hotspot

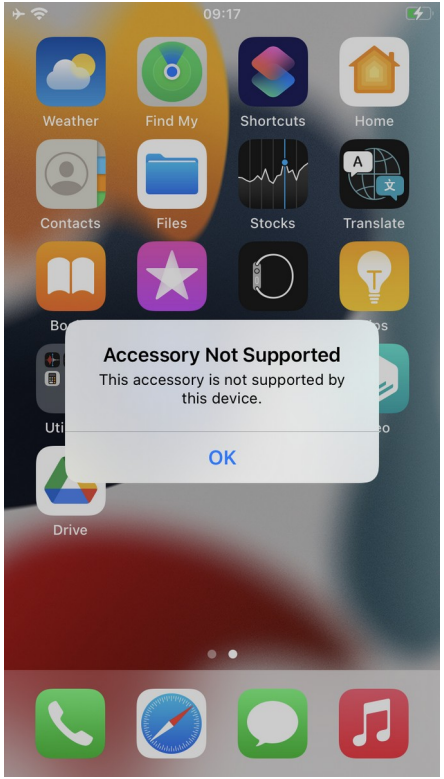
- **Jamming** Bluetooth or WiFi could be a easier solution ✓
- **Cache Manipulation** did not work ✗
  - /private/var/mobile/Library/Preferences/com.apple.accessoryd.plist



Authentication

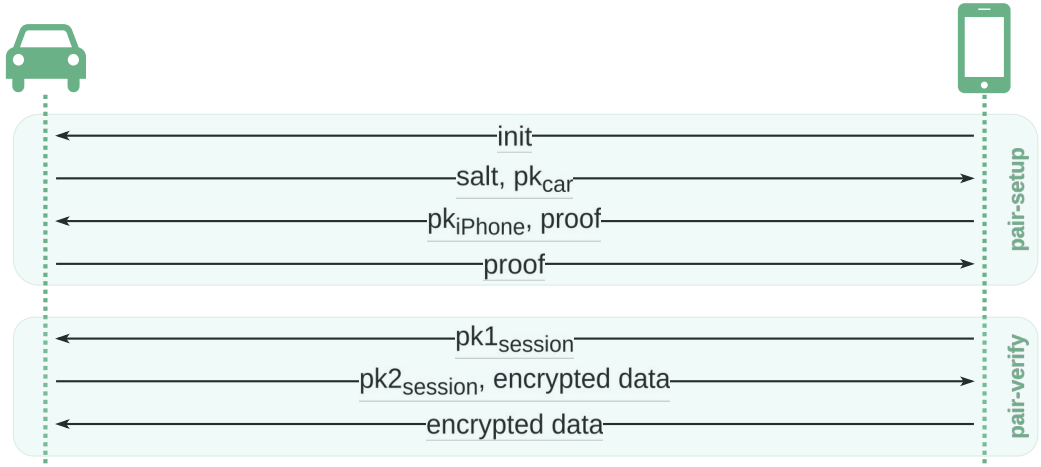
- To authorize an illegitimate device an attacker has to pass **3 rounds** of challenge-response
- in the weakest case, the challenge is **19 bytes** long

  → replay attacks not possible
- Physical attacker needs a possibility to **extract the private key** from the MFi chip



Confidentiality

- Most of the private data stays on the iPhone
  - No interesting meta-data
  - Only the video stream is leaving the iPhone



- Chacha20Poly1305 encrypted with AirPlay session key
- not possible for an attacker to get the shared secret without having physical access to the head unit

Future Work

- Look into the Apple MFi chip to extract private keys
- Fuzzing iAPv2
- Fuzzing AirPlay touch-stream

26. Jun 2024: “CarPlay 2.0 for classic cars: designers show what's possible”
https://www.iphone-ticker.de/carplay-2-0-fuer-klassiker-designer-zeigen-was-moeglich-ist-237262/

Contributions

- Identification of CarPlay Protocols (iAPv2 and AirPlay)
- Reverse Engineering of iAPv2
- Overview of AirPlay Usage in CarPlay
- Security Analysis of CarPlay emphasizing authenticity, availability, and confidentiality

Image Sources

Slide 1
- title image: https://www.igyaan.in/187582/apple-carplay-update/

Slide 3
- iPhone: http://www.nwsoundwaves.com/services/smartphone
- Lightning: http://maconline.com/products/cable-lightning-a-usb-c-apple
- Siri: https://www.appletips.nl/siri-mogelijkheden/
- instrument cluster: https://breeves002.net/product/cluster/
- head unit: https://www.cnet.com/roadshow/news/best-apple-carplay-head-unit/
- loudspeakers: https://axton.de/
- apps:
- https://support.apple.com/de-de/guide/maps/welcome/mac
- https://www.appletips.nl/siri-mogelijkheden/
- https://play.google.com/store/apps/
- http://support.apple.com/kb/ht4873
- https://iaccessibility.net/quick-tip-want-know-whos-calling-without-looking-phone/
- https://www.totalbug.com/imessage

Slide 8, 10
- Ford: https://www.meinauto.de/ford/neuwagen/498-focus/angebote/focus-turnier-neues-modell
- CarlinKit: https://www.carlinkit.ru/products/carlinkit-cp2a-40

Slide 29
- icons: https://www.apple.com/de/airplay/

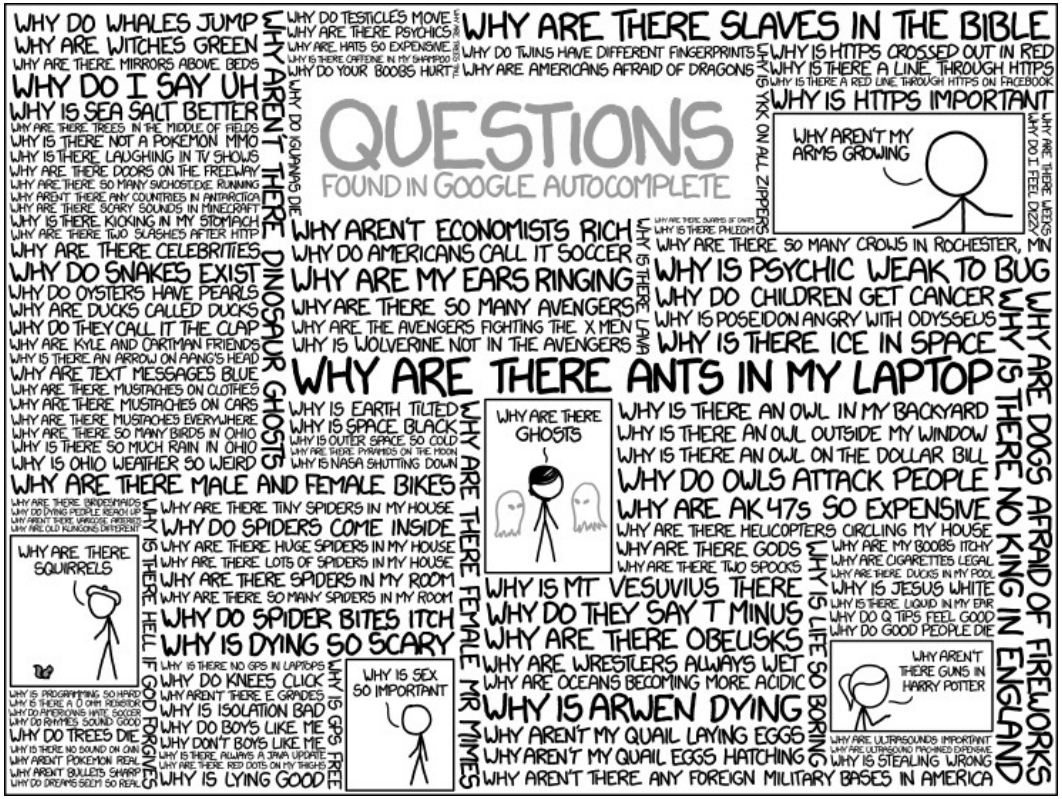
Slide 33
- Book cover: https://www.barnesandnoble.com/w/threat-modeling-adam-shostack/1124318153;jsessionid=2A4AC659118188D33DCAF8E729F312A6.prodny_store01-atgap14?ean=9781118809990

Slide 34
- Attacker1: https://vmag.pk/is-car-hacking-the-new-car-jacking/
- Attacker2: https://youprogrammer.com/how-to-hack-wifi/

Slide 38
- Apple Mfi: https://ventiontech.com/blogs/technology-overview/what-is-apple-mfi-certification

Slide 45
- MFi chip: https://wiomoc.de/misc/posts/mfi_iap.html

Questions?



Source: https://imgs.xkcd.com/comics/questions.png

hnoettgen@seemo.tu-darmstadt.de