In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

Risk Assessment of a Biometric Continuous Authentication Protocol for Internet Services

Enrico Schiavone, Andrea Ceccarelli, and Andrea Bondavalli
Department of Mathematics and Informatics,
University of Florence, Florence, Italy
{enrico.schiavone, andrea.ceccarelli, bondavalli}@unifi.it

Abstract

Distributed internet services involve multiple heterogeneous applications that communicate with each other. Guaranteeing their security is in general both mandatory and complex. Amongst the many security requirements that have to be guaranteed, secure user authentication is one of the most fundamental. Authentication is traditionally executed only at login phase, based on username and password. However, a single authentication point may not always guarantee a sufficient degree of security, especially in the context of critical systems. In a previous work we proposed a *continuous* authentication protocol that applies multiple biometric traits to continuously compute its trust in the user. This paper analyzes the security provided by such solution through a qualitative risk assessment, focusing on both threats related to transmission and specific of the biometric system level. Applying a NIST-compliant threat analysis, we identify the main threats and we assess their impact. Finally, we define the required countermeasures which allow us improving the security of our authentication solution.

1 Introduction

Internet services have become extremely important and today expose functionalities in a huge variety of fields, from healthcare and education to business and government. These services should be properly protected from cyber-crimes, which can range from theft of confidential information to cyber terrorism. In fact, attacks conducted against Internet services may even have catastrophic consequences. However, guaranteeing their security is a very complex activity and it usually includes a broad set of requirements like authentication, authorization, confidentiality, privacy, and integrity.

In this paper, we especially focus on authentication, which is defined as *the provision of assurance in the claimed identity of an entity* [1]. The identity verification can be obtained exploiting a piece of information and/or a process called *authentication factor*. Traditionally, the factor employed is a password, a PIN (Personal Identification Number), or more generally something that the user knows.

Usually, such authentication factor is requested and checked only at login phase, and this may expose the system to attacks [2].

An interesting alternative is offered by biometric traits, being them physiological or behavioral characteristics (as fingerprint or keystroke). Unlike passwords and secrets, biometric traits can be acquired continuously through time, and in some cases without active participation of the user e.g., when a camera is used to collect a face image. In [2], the CASHMA protocol is presented specifically intended for continuously authenticating users of mobile devices through a transparent acquisition of their biometric traits. The protocol determines timeouts based on the quality, frequency and type of biometric data collected. However, an exhaustive security analysis of the CASHMA protocol with respect to cyber-physical attacks have not been performed yet, thus it is uncertain if additional security measures to complement the architectural design of [2] would be beneficial.

In this paper, we present a NIST-compliant [3] qualitative risk assessment of the CASHMA protocol [2], in order to identify relevant threats and determine the risks associated with its execution. The objective is to evaluate the protocol, analyzing its security guarantees and weaknesses, and identifying countermeasures that improve its security. We consider intentional non-physical threats, differentiating transport level threats as *spoofing, forgery, unauthorized access*, *eavesdropping*, *message corruption,* from (biometric) system level threats, like *brute force, sensor spoofing, reuse of residuals, database compromise* [4], [5], [6], and [7]. A considerable set of threats that we examined are not described here because not applicable to CASHMA architecture or because we assess their risk as already Very Low thanks to the security and the countermeasures provided by protocol as it is.

We consider a set of modifications to the protocol that minimize the risk for all the analyzed threats whose risk is relevant (Moderate or higher), as shown in Appendix A and Appendix B. Those countermeasures, or a subset of them where some are alternative each other, are really recommended to be included.

2 Background and Related Work

2.1 Internet Services Security

A Web service relies on some of the same underlying HTTP and Web-based architecture as common Web applications; it is susceptible to similar threats and vulnerabilities. Web services security is based on several important concepts, including authentication, authorization, integrity, non-repudiation, confidentiality, privacy [8]. At the transport level, Secure Socket Layer (SSL), whose standardized version is known as Transport Layer Security (TLS), is the most widely used communication protocol providing authentication of the communicating parties, confidentiality and integrity of the exchanged data, which is encrypted and checked for corruption, and also providing secure key exchange between client and server. SSL provides a secure communication channel; however, when the data is not "in transit," it is not protected. This makes the environment vulnerable to attacks in multi-step transactions [9].

At application level, many challenges are traditionally met with existing standards relying on XML frameworks [8]. In addition to typical challenges of web applications, we also have to consider the threats to our specific system domain: there are a number of points where a biometric system can be attacked. Several, complementary, defensive measures can be taken to minimize the risk [6].

2.2 The CASHMA Approach for Continuous Authentication

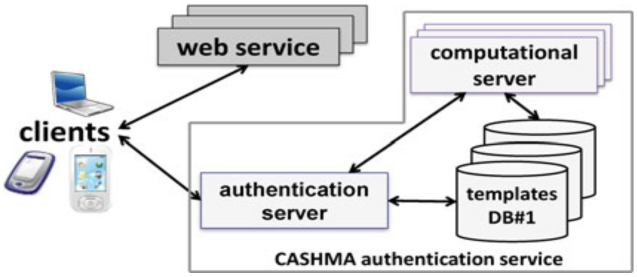

Figure 1 Overall view of the CASHMA architecture

The continuous authentication protocol proposed in [2] improves security and usability of user session. The protocol computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of biometric data transparently acquired during their activity. The overall system, shown in Figure 1, is composed of the CASHMA authentication service, the clients and the web services, connected through secure communication channels [2].

The CASHMA authentication service includes: i) an authentication server, which interacts with the clients, ii) a set of high-performing computational servers that perform comparisons of biometric data for verification of the enrolled users, and iii) databases of templates that contain the biometric templates of the enrolled users (these are required for user authentication/verification). The web services are the various services that use the CASHMA authentication service and demand the authentication of enrolled users to the CASHMA authentication server. These services are potentially any kind of Internet service or application with requirements on user authenticity.

Finally, by clients we mean the users' devices that acquire the biometric raw data corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server as part of the authentication procedure towards the target web service.

The CASHMA authentication server is in charge to transmit a certificate to the client. The certificate is composed by the following information: i) *Timestamp* and *sequence number* useful to univocally identify each certificate, and to protect from replay attacks; ii) *ID* is the user ID, e.g., a number; iii) *Decision* represents the outcome of the verification procedure carried out on the server side; iv) the *expiration time* of the session - the absolute instant of time at which the session should expire-, dynamically assigned by the CASHMA authentication server.

The execution of the protocol is composed of two consecutive phases: the initial phase (Figure 2), and the maintenance phase.

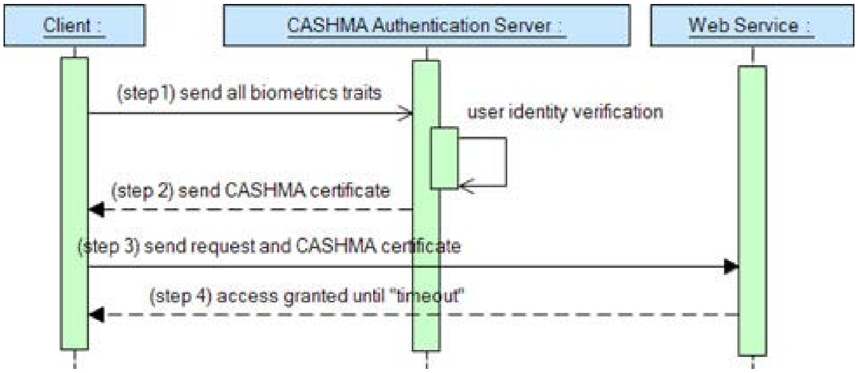
Client :
CASHMA Authentication Server :
Web Service :
(step1) send all biometrics traits
user identity verification
(step 2) send CASHMA certificate
(step 3) send request and CASHMA certificate
(step 4) access granted until "timeout"

Figure 2 Initial phase in case of successful user authentication

Initial phase. This phase is structured as follows:
Step 0 - The user (the client) contacts the web service for a service request; the web service replies that a valid certificate from the CASHMA authentication service is required for authentication.
Step 1 - Using the CASHMA application, the client contacts the CASHMA authentication server. The first step consists in acquiring and sending at time t_0 the data for the different biometric traits, specifically selected to perform a strong authentication procedure. The application explicitly indicates to the user the biometric traits to be provided and possible retries.
Step 2 - The CASHMA authentication server analyzes the biometric data received and performs an authentication procedure. Two different possibilities arise here. If the user identity is not verified (the global trust level is below the trust threshold g_{min}), new or additional biometric data are requested (back to step 1) until the minimum trust threshold g_{min} is reached. Instead if the user identity is successfully verified, the CASHMA authentication server authenticates the user, computes an initial timeout of length T_0 for the user session, set the expiration time at T_0+t_0, creates the CASHMA certificate and sends it to the client.
Step 3 - The client forwards the CASHMA certificate to the web service coupling it with its request.
Step 4 - The web service reads the certificate and authorizes the client to use the requested service until expiration time.

The *maintenance phase* is composed of three steps, analogous to Step 1, Step 2 and Step 3, repeated iteratively [2].

2.3 Security solutions in place and assumptions

We identify the following initial set of security solutions and assumptions for our security analysis. First, all communications between the components of CASHMA architecture are through encrypted communication channels, using Secure Sockets Layer (SSL). With SSL, the channel is protected against replay attacks using the MAC (Message Authentication Code) computed from the MAC secret, the sequence number, the message length, the message contents, and two fixed character strings [8]. Further, biometric data is transmitted in raw format from client to the CASHMA authentication service, and this has been a design decision applied to reduce the dimension, intrusiveness and complexity of the application installed on the client device [2]. However, biometric data in not stored on the client: the templates are stored on the CASHMA authentication service side.

3 Risk Assessment of the CASHMA Protocol

In this section we perform a qualitative risk assessment of the CASHMA protocol, based on the methodology of NIST SP-800-30 [3]. The purpose of the assessment is to establish if some of the steps of the protocol and of the entities involved may be exposed to relevant security risks; this activity supports decisions related to protocol modifications and improvements, where needed.

3.1 Definitions

In order to describe the details of the risk assessment, we first introduce some useful definitions from NIST SP-800-30 [3].

- A *threat* is any circumstance or event with the potential to adversely impact a system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. *Threat events* are caused by *threat sources*, i.e. hostile cyber or physical attacks; human errors of omission or commission; structural failures of organization-controlled resources (e.g., hardware, software, environmental controls); and natural and man-made disasters, accidents, and failures beyond the control of the organization.

- *Vulnerability* is a weakness in the system security procedures, internal controls, or implementation that can be exploited by a threat source.
- The *likelihood of occurrence* is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts). For adversarial threats, an assessment of likelihood of occurrence is typically based on: (i) adversary *intent*; (ii) adversary *capability*; and (iii) adversary *targeting*.
- The level of *impact* from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized behavior.
- *Risk* is a function of the likelihood of a threat event's occurrence and potential adverse impact should the event occur.

3.2 Assessment Methodology

We first determine which types of threat sources are to be considered during risk assessment. We consider adversarial threat sources only, as opposed to non-adversarial like human errors, structural failures or natural disasters. The characteristics of the identified attackers are summarized in Table 1 and are adapted from the quantitative security evaluation of [2].

A Hacker (Hk) represents an external individual having high technological capabilities but moderate resources. An Insider (Is) is an internal attacker, having minimal capabilities and organization-level resources.

The threat events that we consider can be divided in transport level threats: *spoofing, forgery, unauthorized access, eavesdropping, message corruption*; and system level threats: *brute force attack, reuse of residuals, insertion of imposter data, component replacement, database compromise,* [4], [5], [6], and [7].

In the following sections, we will rate the likelihood of occurrence as a combination of i) the likelihood that a threat is initiated, possibly related to the attack gain, and ii) the likelihood that a threat event, once initiated, will result in adverse impact. The likelihood of occurrence determination is based on authors' experience and confirmed by the CVSS framework [12].

The overall likelihood is expressed in a qualitative scale: *Very Low (VL),* if the threat event is highly unlikely to occur and have adverse impact, *Low (L)* if it is unlikely, *Moderate (M)* if it is somewhat likely, *High (H)* if it is highly likely, *and Very High (VH)* if it is almost certain.

As discussed in [3], impacts from threat events are determined considering (i) the characteristics of the threat sources that can initiate the events; (ii) the vulnerabilities/predisposing conditions identified, and (iii) the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events. The assessment scale is Very Low (VL); meaning that the adverse effect is negligible; Low (L), if the impact is expected to be limited; Moderate (M), if the threat event is expected to have a serious adverse effect; High (H), in case of severe or catastrophic impact; and Very High (VH), if the threat event is expected to have multiple severe or catastrophic adverse effect.

The level of risk is determined as a combination of: (i) the impact resulting from the events; and (ii) the likelihood of the events occurring, as summarized in Table 2.

	Hacker (Hk)	**Insider (Is)**
Access	External	Internal
Resources	Moderate	Organization
Capabilities	High	Minimal

Table 1: Attackers and their characteristics.

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Table 2: Level of risk determination, from NIST SP-800-30 [3].

In the following, we call: *Hk*, and *Is* the attackers, being a *Hacker* or *Insider*, respectively, *C* the legitimate client, *AS* the Authentication Server, *WS*: the Web Service.

For space constraints and in order to not being too redundant, the assessment is performed only for the initial phase of the protocol, but it can be easily extended to the maintenance phase too, that is analogous.

3.3 Transport Level Threats Analysis

Spoofing. The spoofing threat (*masquerade*) is a communication level threat that happens when an entity pretend to be recognized as a different entity, possibly laying the foundation for other threats like forgery or unauthorized access [4]. For instance, it can be accomplished using stolen user credentials. Traditional countermeasures are: the usage of strong authentication, avoiding the storage of secretes (e.g. passwords) in plaintext, avoiding transfer of credentials in plaintext over the wire, and protecting communication with SSL [5]. Based on the protocol description and assumptions, CASHMA is integrating most of the countermeasures to this threat. However, we identified four different points of vulnerability, and the related threats are referred as S1, S2, S3 and S4, shown in Appendix A Table 3.

The threat *Spoofing S1* specifically refers to step 1 of the CASHMA protocol (Figure 2): the adversary injects believable biometric raw data into a message, claiming to be C, and obtains a valid certificate from the AS. Noteworthy, the attacker needs previous possession of the biometric raw data of the legitimate user. An Insider may be somehow capable of acquiring the biometrics needed, helped by the proximity and knowledge of C habits. In order to perform step 1 of the protocol and act as being C, it should send the data to the AS. This may be harder for Is because we consider that high skills are needed to circumvent the SSL protocol. We consider as Moderate the overall likelihood. On the contrary, if the threat agent is a Hk, it may be hard to obtain access to the set of biometric raw data remotely. If the data are obtained, the Hk may possess enough capabilities to circumvent SSL protocol. The overall likelihood is Moderate also for Hk.

If the attacker is able to accomplish the spoofing attack, it may lay foundations for subsequent threat events: being recognized as C, and obtained a valid certificate, X may send a valid request to the Web Service. For this reason, we determine as High the *Impact* of this threat. As shown in Appendix A Table 3, the resulting *Risk* is Moderate for both the attackers.

The threat *Spoofing S2* refers both to steps 1 and 2 of the protocol. On step 1, the attacker spoofs the AS, receives the biometric traits of C, with detrimental effects on C’s privacy. In addition it can be used in step 1 of a subsequent iteration of the protocol to act as being C towards AS (*Spoofing S1*). As a result, we consider High the *Impact* of this threat. On step 2, instead, if X can corrupt a certificate and claim to be the AS, the corruption probably provides a fake and useless certificate to C. We consider unlikely to spoof the AS for the Insider and Moderate the likelihood of occurrence of S2 for the Hacker.

The threat *Spoofing S3* applies to step 3 of the protocol. The attacker spoofs the WS, receiving the request and a valid certificate from C. These data can be useful in step 1 to spoof C (see *Spoofing S1*). However, a CASHMA certificate integrates information like timestamp and user ID that protect from replay attacks (see also *Message corruption M1*). For this reason the impact can be considered Moderate: the gain is not so relevant if the obtained data is not useful for the attacker.

The threat *Spoofing S4* applies to step 3 of the protocol. The attacker sends a request with a valid certificate, obtaining the access to the service provided by WS. The impact is High, but we consider the successful reuse of a valid certificate unlikely, because it is univocally identified by *Timestamp* and *sequence number.*

Possible countermeasures for threats S1-S4 range from sending the message coupled with its digital signature (measure useful for auditing and as a deterrent), adding a further level of encryption using AS's public key or avoid passing the raw biometric data over the wire.

Forgery. The forgery happens when an entity fabricates information and claims that such information was received from another entity or sent to another entity [4]. For the CASHMA protocol, we discuss two main forgery threats, F1 and F2, shown in Appendix A Table 4.

For threat *Forgery F1*, the attacker fabricates one or more biometric traits in order to spoof C's identity. The occurrence likelihood depends on the kind of biometric traits necessary for the authentication, on their FRR (False Rejection Rate) and on the FRR of the system. However, as discussed for threat S1, we consider unlikely to forge a set of traits and provide them continuously for the remote Hk, and moderately likely for the Is. For this reason, even if the threat has a High impact (especially if the application protected is critical), the risk can be considered low for Hk. Instead, we consider a Moderate risk for the Is. An additional countermeasure useful to reduce this risk is to not transmit raw biometric over the wire. This threat is related to Sensor Spoofing (Appendix B Table 8).

The threat *Forgery F2* refers to the forgery of a CASHMA certificate. We can consider Unlikely for the Insider attacker to forge a certificate and Moderate the likelihood of occurrence if the threat source is Hk. The impact is High. As a countermeasure, the message containing the certificate sent on step 3 to the WS, should be digitally signed by the sender.

Unauthorized Access. When an entity accesses data in violation to the security policy in force [4] we have the so called unauthorized access threat event. We comment the two threats U1 and U2, Appendix A Table 5. With the threat *Unauthorized access U1*, we refer to the event of getting (physically or remotely) possession of C's device or workstation, but not the critical functions only provided through continuous authentication. We consider the likelihood for a remote attacker (Hk) as Moderate, and High for the Is. However, the resulting impact and risk are Low, because as we defined in Section 2.3, no biometric data is stored on the device.

The threat *Unauthorized access U2* refers instead to the access to the critical functions/services protected with the continuous authentication. Proper configuration of security permission is able to mitigate this threat. No modifications to the protocol are required in this case. We rate the likelihood and the related risk as Low. No additional countermeasures are proposed for these two threats.

Eavesdropping. Eavesdropping (or *Sniffing*) is a breach of confidentiality by unauthorized monitoring of communications [4]. We detect the threats E1, E2, and E3 for CASHMA, shown in Appendix A Table 6. A sniffing happens when an attacker captures packets from the network and reads the data content in search of sensitive information like biometric data, secret keys, certificates or any kind of confidential information. Traditionally, the full encryption of communication, including credentials, prevents sniffed packets from being usable to an attacker. SSL is an example of encryption solution [5].

The threat *Eavesdropping E1* refers to the sniffing of the message on step 1, containing the biometric raw data of C. Referring to Section 2.3, the message on step 1 is transmitted through an SSL channel, thus it is encrypted with a session key that only C and AS know. We consider Moderate the likelihood of occurrence for E1 if the attacker possesses high capabilities, as the Hk, and Low if is Is. The impact is High, because obtaining the biometrics may cause identity theft. Possible countermeasures are a subset of what proposed for the Spoofing threats: adding a further level of encryption using AS's public key or avoid passing the raw biometric data over the wire.

The threat *Eavesdropping E2* refers to the sniffing of the message on step 2 or step 3, containing the CAHSMA certificate. Again, we assess the likelihood as Moderate for Hk and Low for Is. The impact can be considered Moderate, as discussed for Spoofing S3 threat, being that the CASHMA certificate contains ID and timestamp that protect from replay attacks.

Message Corruption. The message corruption threats refer to the situation in which the integrity of transferred data is compromised by unauthorized copying, deletion, insertion, modification, reordering, replay or delay [4]. For the CASHMA protocol, we detect the set of message corruption threats shown in Appendix A Table 7. Referring to Section 2.3, the SSL encryption and the MAC address protect the protocol from this threat.

The threat *Message corruption M1* happens when the attacker copies and replays one of the messages, for instance the message sent on step 1 containing the biometrics of C. We consider as Low the impact of the simple replaying of a message (without modification) thanks to the SSL encryption already available as discussed above.

The threat *Message corruption M2* applies to the deletion of a message sent on steps 1 to 4. If the message on step 1 with biometric traits is deleted, no verification is done. However, it does not have any relevant consequence in terms of security. If the message on step 2 containing the certificate is deleted, the client has to restart from the first step of the protocol. If the message sent on step 3 with the certificate is deleted, the client has to send the same message again, or if the session is expired, restart from step 1. Finally, if the "access granted until timeout" message (step 4) is deleted, C waits for the message until the session expiration. We can consider all these threats together having a Low impact and a resulting Low risk.

The threat *Message corruption M3* refers to the insertion of a message in between the information flow from sender and receiver (from C to AS, from AS to C, from C to WS or from WS to C). The impact is Moderate, being that the insertion of a message can be used for instance to conduct a spoofing threat. However, in CASHMA messages from one party cannot be inserted into the other's output, since they use independent MAC secrets [10]. Consequently, the likelihood for this threat is set to Low. The resulting risk is set to Moderate if the attacker is Hk, and to Low for the Is.

The threat *Message corruption M4* represents a resequencing attack conducted against AS. Again, it is not likely due to the encryption obtained with SSL. Moreover, the impact is limited. For instance, inverting messages in step 2 and 4 would make C thinking to be able to access the WS, when actually it is not. So it just results in unsatisfied user due to unavailable or delayed service.

For threat *Message corruption M5*, we can distinguish four events, one for each step from 1 to 4. *Step 1*: The attacker corrupts the message with the biometric traits of C, but cannot act as C. The corruption makes the verification procedure to reject C, causing a DoS. *Step 2*: The attacker corrupts the message containing the certificate, alters the timestamp, the sequence number, the expiration time, the decision, with remarkable consequences for the subsequent steps. *Step 3*: The attacker alters a valid certificate, generated for C when it is being sent to the WS. This impacts the next step. *Step 4*: if messages are corrupted by X, the WS denies the access for C or grant it for a time window lower than normal, thus provoking a Denial of Service.

3.4 System Level Threats Analysis

In this section we analyze a set of system level threats, shown in Appendix B Table 4, which are typical of a biometric system [6].

Brute force. Brute force attacks in general rely on computational power to crack secrets secured with hashing and encryption. The *Brute Force B1* threat refers to the submission of a huge set of biometric traits to the sensors embedded or connected to the client workstation with the objective of finding a trait (or a set of traits) that let the attacker to be authenticated. However, the CASHMA protocol as it is should maintain Low the impact of this threat, because the number of retries is limited, as discussed in Section 0. As a result, also the risk is Low for both the attackers.

Sensor Spoofing. An attacker provides a set of fake physical or digital biometric traits designed to circumvent the biometric system. The CASHMA system integrates a multi-modal biometric system: the user has to provide a set of traits in order to be authenticated. The multi-modality itself can be considered a first defensive measure to this threat [6]. The impact of this threat is High. We assess a Moderate risk for the Insider attacker, which may have direct access to the device and the biometric sensors. An additional countermeasure that can reduce the risk is the liveness detection to ensure the biometric sample presented to the reader is from a live person.

Reuse of residuals. An attacker gains somehow access to valid biometric data and reuses it. As discussed in the assumptions, no biometric data is saved on client's device. However, is important to defend from this threat, because the attacker may obtain data in other ways (i.e. through Eavesdropping). The risk is Moderate and the Impact is considered High for the Hk attacker. An effective defensive measure is prohibiting identical samples being used consecutively.

Database compromise. An attacker obtains access to template repository and is able to read, modify or substitute templates. We consider Low the likelihood of this threat: we assume that the CASHMA authentication server implements a very efficient and complete set of access control mechanisms. However, the impact of this threat is very high for template security and users' privacy, and, as a consequence, the risk for Hk is Moderate. To reduce the risk, may be necessary to introduce additional defensive measures as biometric cryptosystems or cancellable biometrics. With cancellable biometrics, only the transformed data are stored and if these data are compromised, a new transform can be applied, thus replacing the original template [6]. Biometric cryptosystems, instead, are designed to securely bind a digital key to a biometric or generate a digital key from a biometric, offering solutions to and biometric template protection, together with biometric-dependent key-release [11]. With the integration of one of these countermeasures, we imagine a reduction of the Impact due to database compromise from Very High to High, which together with a Low likelihood determines a Low risk.

4 Conclusions and Future work

This paper presents a qualitative risk assessment of a biometric continuous authentication protocol. The CASHMA protocol guarantees high security of user session, monitoring in background the user's actions, through a continuous and transparent acquisition of multiple biometric traits, and computing an adaptive, trust-based, timeout. Nevertheless, we show that the introduction of some additional defense measures would considerably increase system's security.

Our assessment complies with NIST methodology: we identify the main threats both for the transmission and the biometric system level; we assess the likelihood of occurrence and the impact for each threat, distinguishing two different attackers' profiles. Then, we determined the risk related to each threat occurrence. The assessment highlighted a set of threats whose risk is considerate Moderate and for which we discussed further security countermeasures as additional encryption layers, or templates protection solutions. The modifications are capable of reducing the risk for all the threats considered and for this reason are recommended to be included in the protocol or in the architecture.

In future work, we plan to investigate the possibility to introduce modifications to the CASHMA protocol in order to provide additional security requirements as, for instance, the non-repudiation of user actions.

Acknowledgment

This work has been partially supported by the project DEVASSES, funded by the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no PIRSES-GA-2013-612569, and by the Joint Program Initiative (JPI) Urban Europe via the IRENE project.

References

[1] ISO/IEC 18014 (2009). *Information technology - Security techniques - Time-stamping services - Part 2: Mechanisms producing independent tokens*.

[2] Ceccarelli, A., Montecchi, L., Brancati, F., Lollini, P., Marguglio, A., & Bondavalli, A. (2015). Continuous and transparent user identity verification for secure internet services. *IEEE Transactions on Dependable and Secure Computing*, *12*(3), 270-283.

[3] NIST. *Guide for Conducting Risk Assessments*. NIST SP-800-30, Rev.1, 2012

[4] ETSI TS 102 165-1 V4.1.1 (2003). *Telecommunications and internet protocol harmonization over networks (TIPHON) release 4; protocol framework definition; methods and protocols for security; part 1: Threat analysis. Technical Specification*.

[5] Nostro, N., Bondavalli, A., & Silva, N. (2014, November). Adding Security Concerns to Safety Critical Certification. In *Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on* (pp. 521-526). IEEE.

[6] Chris, R. (2007). Biometric attack vectors and defenses. *Computers & Security*, *26*, 14-25.

[7] Li, S. Z. (2009). *Encyclopedia of Biometrics: I-Z* (Vol. 1). Springer Science & Business Media.

[8] Singhal, A., Winograd, T., & Scarfone, K. (2007). Guide to secure web services. *NIST Special Publication*, *800*(95), 4.

[9] Oracle Fusion Middleware Security and Administrator's Guide for Web Services. https://docs.oracle.com/cd/E28280_01/web.1111/b32511/standards.htm#WSSEC1358

[10] Dierks, T. (2008). The transport layer security (TLS) protocol version 1.2.

[11] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 1-25, 2011.

[12] Mell, P., Scarfone, K., & Romanosky, S. (2006). Common vulnerability scoring system. IEEE Security & Privacy, 4(6), 85-89.

Appendix A. Risk Assessment and Countermeasures for Transport Level Threats

Threat	Description	Attacker	Risk Assessment			Countermeasures	New Risk Assessment		
			Likelihood	Impact	Risk		Likelihood	Impact	Risk
Spoofing S1	The attacker pretends towards AS to be C	Hk	M	H	**M**	1) Digital signature of the message. 2) Additional encryption of the message with receiver's public key. 3) Do not transmit raw biometric data over the wire: encrypt biometric data on client-side	L	H	**L**
		Is	M	H	**M**		L	H	**L**
Spoofing S2	X pretends towards C to be AS (step 1 and 2)	Hk	M	H	**M**		L	H	**L**
		Is	L	H	L		VL	H	L
Spoofing S3	X pretends towards C to be WS (step 3)	Hk	M	M	**M**		L	M	**L**
		Is	L	M	L		L	M	L
Spoofing S4	X pretends towards WS to be C (step 3)	Hk	L	H	L		L	H	L
		Is	L	H	L		VL	H	L

Table 3: Spoofing Threats in CASHMA

Threat	Description	Attacker	Risk Assessment			Countermeasures	New Risk Assessment		
			Likelihood	Impact	Risk		Likelihood	Impact	Risk
Forgery F1	The attacker fabricates one or more biometric traits in order to spoof C's identity	Hk	L	H	L	Do not transmit raw biometric data over the wire: encrypt biometric data on client-side	L	H	L
		Is	M	H	**M**		L	H	**L**
Forgery F2	X fabricates a fake certificate, claiming that was received from AS	Hk	M	H	**M**	Digital signature of the message.	L	H	**L**
		Is	L	H	L		L	H	L

Table 4: Forgery Threats in CASHMA

Threat	Description	Attacker	Risk Assessment		
			Likelihood	Impact	Risk
Unauthorized Access U1	The attacker gets possession of C's device or workstation	Hk	M	L	L
		Is	H	L	L
Unauthorized Access U2	The attacker obtains access to the data protected by the continuous authentication	Hk	L	H	L
		Is	L	H	L

Table 5: Unauthorized Access Threats in CASHMA

Threat	Description	Attacker	Risk Assessment			Countermeasures	New Risk Assessment		
			Likelihood	Impact	Risk		Likelihood	Impact	Risk
Eavesdropping E1	X sniffs the message on step 1 (see Figure 2), with the biometric traits of C	Hk	M	H	**M**	1) Additional encryption of the message with receiver's public key. 2) Do not pass raw biometric data over the wire: encrypt biometric data on client-side	L	H	**L**
		Is	L	H	L		L	H	L
Eavesdropping E2	X sniffs the message on step 2 or step 3 (see Figure 2), containing the certificate.	Hk	M	M	**M**	Additional encryption of the message with receiver's public key.	L	M	**L**
		Is	L	M	L		L	M	L

Table 6: Eavesdropping Threats in CASHMA

Threat	Description	Attacker	Risk Assessment			Countermeasures	New Risk Assessment		
			Likelihood	Impact	Risk		Likelihood	Impact	Risk
Message Corruption Threat M1	X copies a message (step 1 to 4) and replays it to the receiver.	Hk	M	L	L	Do not pass raw biometric data over the wire: encrypt biometric data on client-side	L	L	L
		Is	L	L	L		L	L	L
Message Corruption Threat M2	X deletes a message (steps 1 to 4)	Hk	M	L	L	n/a	n/a	n/a	n/a
		Is	L	L	L		n/a	n/a	n/a
Message Corruption Threat M3	X inserts a message in between the information flow from C to AS (and vice versa) or from C to WS (and vice versa).	Hk	M	M	**M**	1) Additional encryption of the message with receiver's public key. 2) Do not pass raw biometric data over the wire: encrypt biometric data on client-side	L	M	**L**
		Is	L	M	L		L	M	L
Message Corruption Threat M4	X changes the sequence of messages for AS	Hk	M	L	L	n/a	n/a	n/a	n/a
		Is	L	L	L		n/a	n/a	n/a
Message Corruption Threat M5	X alters a message in a plausible way so that C and/or AS and/or WS cannot detect the modification	Hk	M	M	**M**	1) Digital signature of the message 2) Additional encryption of the message with receiver's public key.	L	M	**L**
		Is	L	M	L		L	M	L

Table 7: Message Corruption Threats in CASHMA

Appendix B. Risk Assessment and Countermeasures for System Level Threats

Threat	Description	Attacker	Risk Assessment			Countermeasures	New Risk Assessment		
			Likelihood	Impact	Risk		Likelihood	Impact	Risk
Brute Force	The attacker submits a huge set of biometric traits to the sensors embedded or connected to the client workstation to find a trait (or a set of traits) that let him/her authenticate	Hk	L	L	L	n/a	n/a	n/a	n/a
		Is	M	L	L		n/a	n/a	n/a
Sensor Spoofing	An attacker provides a set of fake physical or digital biometric traits designed to circumvent the biometric system	Hk	L	H	L	Liveness detection	L	H	L
		Is	M	H	**M**		L	H	**L**
Reuse of residuals	An attacker gains somehow access to biometric data and reuses it.	Hk	M	H	**M**	Prohibiting identical samples being used consecutively.	L	H	**L**
		Is	L	H	L		L	H	L
Database Compromise	An attacker obtains access to template repository and is able to read, modify and substitute the templates.	Hk	L	VH	**M**	Biometric Encryption or Cancellable biometrics	L	H	**L**
		Is	VL	VH	L		VL	H	L

Table 8: System level Threats in CASHMA