Updating Location Based Services using Privacy Protection over Web based Content

Najeema Afrin[*1] **K. Pravallika**[*2]

[*1,2]Assistant Professor, CMR Technical Campus, Medchal,Hyderabad.

Abstract **– Security of the web based services is become serious concern now a days. Secure user authentication is very important and fundamental in most of the systems User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at login phase. No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user. Emerging biometric solutions provides substituting username and password with biometric data during session establishment, but in such an approach still a single shot verification is less sufficient, and the identity of a user is considered permanent during the entire session. A basic solution is to use very short session timeouts and periodically request the user to input his credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users. This paper explores promising alternatives offered by applying biometrics in the management of sessions. A secure protocol is defined for perpetual authentication through continuous user verification. Finally, the use of biometric authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user or requiring his interaction, which is essential to guarantee better service usability.**

Keywords – Security, Web Servers, Mobile Environments, Authentication

I. INTRODUCTION

In this technology era security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks, biometric techniques offer emerging solution for secure and trusted user identity verification, where username and password are replaced by bio-metric traits. Biometrics is the science and technology of determining identity based on physiological and behavioural traits. Biometrics includes retinal scans, finger and handprint recognition, and face recognition, handwriting analysis, voice recognition and Keyboard biometrics. Also, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially in the financial and banking sectors. In fact, similarly to traditional authentication processes which rely on username and password, biometric user authentication is typically formulated as a single shot,. providing user verification only during login time when one or more biometric traits may be required. Once the user's identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user. This approach is also susceptible for attack because the identity of the user is constant during the whole session. Suppose, here we consider this simple scenario: a user has al-ready logged into a security-critical service, and then the user leaves the PC unattended in the work area for a while the user session is active, allowing impostors to impersonate the user and access strictly personal data. In these scenarios, the services where the users are authenticated can be misused easily. The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this is not a satisfactory solution. So, to timely identify misuses of computer resources and prevent that, solutions based on bio-metric continuous authentication are proposed, that means turning user verification into a continuous process rather than a onetime authentication. Biometrics authentication can depend on multiple biometrics traits.

Secure user authentication is fundamental in most of modern ICT systems. User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at login phase. No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user. Security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks; biometric techniques offer emerging solution for secure and trusted authentication, where username and password are replaced by biometric data. However, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially considering their possible application in the financial and banking sectors. Such observations lead to arguing that a single authentication point and a single biometric data cannot guarantee a sufficient degree of security. In fact, similarly to traditional authentication processes which rely on username and password, biometric user authentication is typically formulated as a "single shot" providing user verification only during login phase when one or more biometric traits may be required. Once the user's identity has been verified, the system resources are available for a fixed period of time or until explicit logout from the user. This approach assumes that a single verification (at the beginning of the session) is sufficient, and that the identity of the user is constant during the whole session. For instance, we consider this simple scenario: a user has already logged into a security-critical service, and then the user leaves the PC unattended in the work area for a while. This problem is even trickier in the context of mobile devices, often used in public and crowded environments, where the device itself can be lost or forcibly stolen while the user session is active, allowing impostors to impersonate the user and access strictly personal data. In these scenarios, the services where the users are authenticated can be misused easily. A basic solution is to use very short session timeouts and periodically request the user to input his/her credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users

II. LITERETURE SURVEY

Security systems and methods are often described as strong or weak as shown in Fig.1. A strong system is one in which the cost of attack is greater than the potential gain to the attacker. Conversely, a weak system is one where the cost of attack is less than the potential gain. Authentication factors are grouped into these three categories: 1) what you know (e.g., password), 2) what you have (e.g., token), and 3) who you are (e.g., biometric). A. Knowledge-Based ("What You Know") These are characterized by secrecy and includes password. The term password includes single words, phrases, and PINs (personal identification numbers) that are closely kept secrets used for authentication. But there are various vulnerabilities of password-based authentication schemes. The basic drawback of passwords is that memorable password can often be guessed or searched by an attacker and a long, random, changing password is difficult to remember. Also, each time it is shared for authentication, so it becomes less secret. They do not provide good compromise detection, and they do not offer much defense against repudiation. B. Object-Based ("What You Have") They are characterized by physical possession or token.

An identity token, security token, access token, or simply token, is a physical device provides authentication. This can be a secure storage device containing passwords, such as a bankcard, smart card.

A token can provide three advantages when combined with a password. One is that it can store or generate multiple passwords. Second advantage is that it provides compromise detection since its absence is observable. Third advantage is that it provides added protection against denial of service attacks. The two main disadvantages of a token are inconvenience and cost. There are also chances of lost or stolen token. But, there is a distinct advantage of a physical object used as an authenticator; if lost, the owner sees evidence of this and can act accordingly. C. ID-Based ("Who You Are")

They are characterized by uniqueness to one person. A driver's license, passport, etc., all belong in this category. So does a biometric, such as a fingerprint, face, voiceprint, eye scan, or signature. One advantage of a biometric is that it is less easily stolen than the other authenticators, so it provides a stronger defense against repudiation. For both ID documents and biometrics, the dominant security defense is that they are difficult to copy. However, if a biometric is compromised or a document is lost, they are not as easily replaceable as passwords or tokens.To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multi-modal biometric continuous authentication are proposed, turning user verification into a continuous process rather than a onetime occurrence. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple biometrics traits. Finally, the use of biometric authentication allows credentials to be acquired transparently, i.e., without explicitly notifying the user or requiring his/her interaction, which is essential to guarantee better service usability. We present some examples of transparent acquisition of biometric data.

Face can be acquired while the user is located in front of the camera, but not purposely for the acquisition ofthebiometric data; e.g., the user may be reading a textual SMS or watching a movie on the mobile phone. Voice can be acquired when the user speaks on the phone, or with other people nearby if the microphone always captures background. Keystroke data can be acquired whenever the user types on the keyboard, for example, when writing an SMS, chatting, or browsing on the Internet. This approach differentiates from traditional authentication processes, where username/password are requested only once at login time or explicitly required at confirmation steps; such traditional authentication approaches impair usability for enhanced security, and offer no solutions against forgery or stealing of passwords. This paper presents a new approach for user verification and session management that is applied in the context aware security by hierarchical multilevel architectures (CASHMA) [1]) system for secure biometric authentication on the Internet. CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services, and it is intended to be used from different client devices, e.g., smartphones, Desktop PCs or even biometric kiosks placed at the entrance of secure areas. Depending on the preferences and requirements of the owner of the web service, the CASHMA authentication service can complement a traditional authentication service, or can replace it. The approach we introduced in CASHMA for usable and highly secure user sessions is a continuous sequential (a single biometric modality at once is presented to the system [22]) multi-modal biometric authentication protocol, which adaptively computes and refreshes session timeouts on the basis of the trust put in the client. Such global trust is evaluated as a numeric value, computed by continuously evaluating the trust both in the user and the (biometric) subsystems used for acquiring biometric data. In the CASHMA context, each subsystem comprises all the hardware/software elements necessary to acquire and verify the authenticity of one biometric trait, including sensors, comparison algorithms and all the facilities for data transmission and management. Trust in the user is determined on the basis of frequency of updates of fresh biometric samples, while trust in each subsystem is computed on the basis of the quality and variety of sensors used for the acquisition of biometric samples, and on the risk of the subsystem to be intruded. Exemplary runs carried out using Matlab are reported, and a quantitative model-based security analysis of the protocol is performed combining the stochastic activity networks (SANs [16]) and ADversaryVIew Security Evaluation (ADVISE [12]) formalisms. The driving principles behind our protocol were briefly discussed in the short paper [18], together with minor qualitative evaluations. This paper extends [18] both in the design and the evaluation parts, by providing an in-depth description of the protocol and presenting extensive qualitative and quantitative analysis.

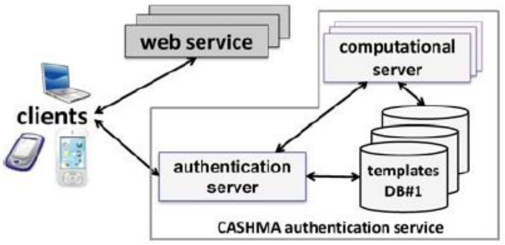
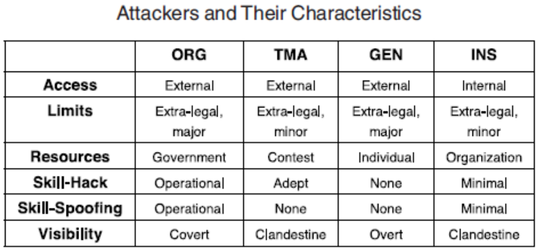


Fig 1: Overall view of the CASHMA architecture

Quantitative Security Evaluation: Scenario and Measures of Interest For the quantitative security evaluation of the proposed protocol we consider a mobile scenario, where a registered user uses the CASHMA service through a client installed on a mobile device like a laptop, a smartphone or a similar device. The user may therefore lose the device, or equivalently leave it unattended for a time long enough for attackers to compromise it and obtain authentication. Moreover, the user may lose the control of the device (e.g., he/she may be forced to hand over it) while a session has already been established, thus reducing the effort needed by the attacker. In the considered scenario the system works with three biometric traits: voice, face, and fingerprint. A security analysis on the first authentication performed to acquire the first certificate and open a secure session has been provided in [6]. We assume here that the attacker has already been able to perform the initial authentication (or to access to an already established session), and we aim to evaluate how long he is able to keep the session alive, at varying of the parameters of the continuous authentication algorithm and the characteristics of the attacker. The measures of interest that we evaluate in this paper are the following: i) PkðtÞ: Probability that the attacker is able to keep the session alive until the instant t, given that the session has been established at the instant t ¼ 0; ii) Tk: Mean time for which the attacker is able to keep the session alive. Since most of the computation is performed server-side, we focus on attacks targeting the mobile device.

In order to provide fresh biometric data, the attacker has to compromise one of the three biometric modalities. This can be accomplished in several ways; for example, by spoofing the biometric sensors (e.g., by submitting a recorded audio sample, or a picture of the accounted user), or by exploiting cyber-vulnerabilities of the device (e.g., through a “reuse of residuals” attack [9]). We consider three kind of abilities for attackers: spoofing, as the ability to perform sensor spoofing attacks, hacking as the ability to perform cyber attacks, and lawfulness, as the degree to which the attacker is prepared to break the law. The actual skills of the attacker influence the chance of a successful attack, and the time required to perform it. For example, having a high hacking skill reduces the time required to perform the attack, and also increases the success probability: an attacker having high technological skills may able to compromise the system is such a way that the effort required to spoof sensors is reduced (e.g., by altering the data transmitted by the client device).

The ADVISE Formalism The analysis method supported by ADVISE relies on creating executable security models that can be solved using discrete-event simulation to provide quantitative metrics. One of the most significant features introduced by this formalism is the precise characterization of the attacker (the “adversary”) and the influence of its decisions on the final measures of interest. The specification of an ADVISE model is composed of two parts: an Attack Execution Graph (AEG), describing how the adversary can attack the system, and an adversary profile, describing the characteristics of the attacker. An AEG is a particular kind of attack graph comprising different kinds of nodes: attack steps, access domains, knowledge items, attack skills, and attack goals. Attack steps describe the possible attacks that the adversary may attempt, while the other elements describe items that can be owned by attackers (e.g., intranet access). Each attack step requires a certain combination of such items to be held by the adversary; the set of what have been achieved by the adversary defines the current state of the model. ADVISE attack steps have also additional properties, which allow creating executable models for quantitative analysis. The adversary pro- file defines the set of items that are initially owned by the adversary, as well as his proficiency in attack skills. The adversary starts without having reached any goal, and works towards them. To each attack goal it is assigned a payoff value, which specifies the value that the adversary assigns to reaching that goal. Three weights define the relative preference of the adversary in: i) maximizing the payoff, ii) minimizing costs, or iii) minimizing the probability



Attackers and Their Characteristics

	ORG	TMA	GEN	INS
Access	External	External	External	Internal
Limits	Extra-legal, major	Extra-legal, minor	Extra-legal, major	Extra-legal, minor
Resources	Government	Contest	Individual	Organization
Skill-Hack	Operational	Adept	None	Minimal
Skill-Spoofing	Operational	None	None	Minimal
Visibility	Covert	Clandestine	Overt	Clandestine

Architecture:

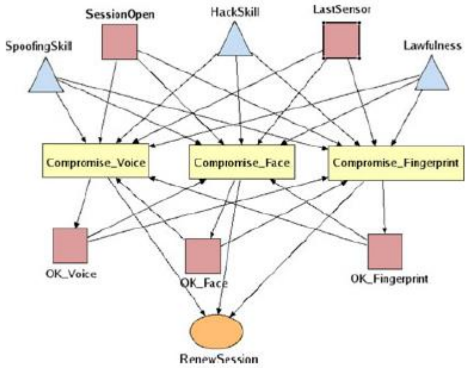


Fig 2: AEG of the ADVISE model used for security evaluations

The model that is used for the analysis combines an ADVISE model, which takes into account the attackers’ behaviour, and a SAN model, which models the evolution of trust over time due to the continuous authentication protocol. Both models include a set of parameters, which allow evaluating metrics under different conditions and performing sensitivity analysis. Protocol parameters used for the analysis are reported in the upper labels of Figs. 13 and 14; parameters describing attackers are shown in Table 1 and their values are discussed in Section 6.2.4. ADVISE model. The AEG of the ADVISE model is composed of one attack goal, three attack steps, three attack skills, and five access domains. Its graphical representation is shown in Fig. 11, using the notation introduced in [12]. The only attack goal present in the model, "RenewSession" represents the renewal of the session timeout by submitting fresh biometric data to the CASHMA server. To reach its goal, the attacker has at its disposal three attack steps, each one representing the compromise of one of the three biometric traits: "Compromise_Voice", "Compromise_Face",and"Compromise_Fingerprint". Each of them requires the "SessionOpen" access domain, which represents an already established session.

The three abilities of attackers are represented by three attack skills: "SpoofingSkill", "HackSkill" and "Lawfulness". The success probability of such attack steps is a combination of the spoofing skills of the attacker and the false nonmatch rate (FNMR) of the involved biometric subsystem. In fact, even if the attacker was able to perfectly mimic the user's biometric trait, reject would still be possible in case of a false non-match of the subsystem. For example, the success probability of the "Compromise_Voice" attack step is obtained as: FNMR VoiceðSpoofingSkill ->MarkðÞ=1; 000:0Þ; where "FNMR_Voice" is the false non-match rate of the voice subsystem, and SpoofingSkill ranges from a minimum of 0 to a maximum of 1,000. It should be noted that the actual value assigned to the spoofing skill is a relative value, which also depends on the technological measures implemented to contrast such attack. Based on the skill value, the success probability ranges from 0 (spoofing is not possible) to the FNMR of the subsystem (the same probability of a non-match for a "genuine" user). The time required to perform the attack is exponentially distributed, and its rate also depends on attacker' skills. When one of the three attack step succeeds, the corresponding "OK_X" access domain is granted to the attacker. Owning one of such access domains means that the system has correctly recognized the biometric data, and that it is updating the global trust level; in this state all the attack steps are disabled. A successful execution of the attack steps also grants the attackers the "RenewSession" goal. "LastSensor" access domain is used to record the last subsystem that has been used for authentication. SAN model. The SAN model in Fig. 12 models the management of session timeout and its extension through the continuous authentication mechanism. The evolution of trust level over time is modeled using the functions introduced in Section 4.2; it should be noted that the model introduced in this section can also be adapted to other functions that might be used for realizing the protocol.

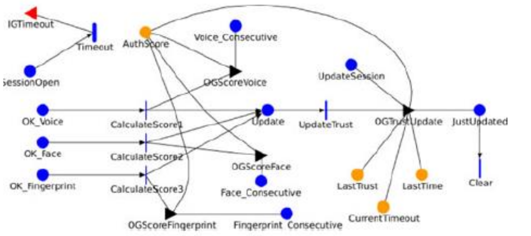


Fig 3: SAN model for the continuous authentication mechanism

III. PROTOTYPE IMPLEMENTATION

The implementation of the CASHMA prototype includes face, voice, iris, fingerprint and online dynamic handwritten signature as biometric traits for biometric kiosks and PCs/ laptops, relying on on-board devices when available or pluggable accessories if needed. On smartphones only face and voice recognition are applied: iris recognition was discarded due to the difficulties in acquiring high-quality iris scans using the camera of commercial devices, andhandwritten signature recognition is impractical on most of smartphones today available on market (larger displays are required). Finally, fingerprint recognition was discarded because few smartphones include a fingerprint reader. The selected biometric traits (face and voice) suit the need to be acquired transparently for the continuous authentication protocol described. A prototype of the CASHMA architecture is currently available, providing mobile components to access a secured web-application. The client is based on the Adobe Flash [19] technology: it is a specific client, written in Adobe Actions Script 3, able to access and control the on-board devices in order to acquire the raw data needed for biometric authentication. In case of smartphones, the CASHMA client component is realized as a native Android application (using the Android SDK API 12). Tests were conducted on smartphones Samsung Galaxy S II, HTC Desire, HTC Desire HD and HTC Sensation with OS Android 4.0.x. On average from the executed tests, for the smartphones considered we achieved FMR ¼ 2.58% for face recognition and FMR ¼ 10% for voice. The dimensions of biometric data acquired using the considered smartphones and exchanged are approximately 500 KB. As expected from such limited dimension of the data, the acquisition, compression and transmission of these data using the mentioned smartphones did not raise issues on performance or communication bandwidth.

In particular, the time required to establish a secure session and transmit the biometric data was deemed sufficiently short to not compromise usability of the mobile device. Regarding the authentication service, it runs on Apache Tomcat 6 servers and Postgres 8.4 databases. The web services are, instead, realized using the Jersey library (i.e., a JAX-RS/JSR311 Reference Implementation) for building RESTful web services. Finally, the example application is a custom portal developed as a Rich Internet Application using SenchaExtJS 4 JavaScript framework, integrating different external online services (e.g., Gmail, Youtube, Twitter, Flickr) made accessible dynamically following the current trust value of the continuous authentication protocol.

IV. CONCLUSION

We exploited the novel possibility introduced by biometrics to define a protocol for continuous authentication that 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 acquired transparently through monitoring in background the user's actions. Some architectural design decisions of CASHMA are here discussed. First, the system exchanges raw data and not the features extracted from them or templates, while crypto-token approaches are not considered; as debated in Section 3.1, this is due to architectural decisions where the client is kept very simple. We remark that our proposed protocol works with no changes using features, templates or raw data. Second, privacy concerns should be addressed considering National legislations. At present, our prototype only performs some checks on face recognition, where only one face (the biggest one rusting from the face detectionphase directly on the client device) is considered for identity verification and the others deleted. Third, when data is acquired in an uncontrolled environment, the quality of biometric data could strongly depend on the surroundings. While performing a client-side quality analysis of the data acquired would be a reasonable approach to reduce computational burden on the server, and it is compatible with our objective of designing a protocol independent from quality ratings of images (we just consider a sensor trust), this goes against the CASHMA requirement of having a light client. We discuss on usability of our proposed protocol. In our approach, the client device uses part of its sensors extensively through time, and transmits data on the Internet. This introduces problematic of battery consumption, which has not been quantified in this paper: as discussed in Section 7, we developed and exercised a prototype to verify the feasibility of the approach but a complete assessment of the solution through experimental evaluation is not reported. Also, the frequency of the acquisition of biometric data is fundamental for the protocol usage; if biometric data are acquired too much sparingly, the protocol would be basically useless. This mostly depends on the profile of the client and consequently on his usage of the device. Summarizing, battery consumption and user pro- file may constitute limitations to our approach, which in the worst case may require to narrow the applicability of the solution to specific cases, for example, only when accessing specific websites and for a limited time window, or to grant access to restricted areas (see also the examples in Section 3.2). This characterization has not been investigated in this paper and constitute part of our future work. It has to be noticed that the functions proposed for the evaluation of the session timeout are selected amongst a very large set of possible alternatives. Although in literature we could not identify comparable functions used in very similar contexts, we acknowledge that different functions may be identified, compared and preferred under specific conditions or users requirements; this analysis is left out as goes beyond the scope of the paper, which is the introduction of the continuous authentication approach for Internet services

REFERENCES

[1] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, Andrea Bondavalli, Member, IEEE, “Continuous and Transparent User Identity Verification for Secure Internet Services”, IEEE Transactions on Dependable and Secure Computing, Manuscript Id, December 2013.

[2] CASHMA - Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB 2005.

[3] L. Hong, A. Jain, and S. Pankanti, “Can Multi-biometrics Improve Performance?,” Proc. AutoID’99, Summit, NJ, pp. 59–64, 1999.

[4] S. Ojala, J. Keinanen, J. Skytta, “Wearable authentication device for transparent login in nomadic applications environment,” Proc. 2nd International Conference on Signals, Circuits and Systems (SCS 2008), pp. 1-6, 7-9 Nov. 2008.

[5] BioID, “Biometric Authentication as a Service (BaaS), “BioID press release, 3 March 2011, https://www.bioid.com [online].

[6] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, “Continuous Verification Using Multimodal Biometrics,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, April 2007.

[7] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, “Quantitative Security Evaluation of a MultiBiometric Authentication System,” Computer Safety, Reliability and Security, F. Ortmeier and P. Daniel (eds.), Lecture Notes in Computer Science, Springer, vol. 7613, pp. 209-221, 2012.

[8] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, “Using Continuous Biometric Verification to Protect Interactive Login Sessions,” Proc. 21st Annual Computer Security Applications Conference (ACSAC '05), pp. 441- 450, 2005. IEEE Computer Society, Washington, DC, USA.