IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 40-44
www.iosrjournals.org

Continuous Biometric Verification to Protect Interactive Login Sessions for Secure Internet Services

Waghmare. S. D[1], More. A. B[2], Jahaurkar. S. A[3], Kasture. S.V[4], Dahane. G.M. [5,]
[1,2,3,4,5]*(Dept. of Information Technology, P.D.V.V.P.COE, SPPU, MS, India)*

Abstract *: Nowadays, it becomes serious concern to provide more security to web services. So, secure user authentication is the fundamental task in security systems. Traditionally, most of the systems are based on pairs of username and password which verifies the identity of user only at login phase. Once the user is identified with username and password, no checks are performed further during working sessions We explore the continuous user verification for the secure internet services using biometrics in the session management No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user However a single verification step is still deemed sufficient, and the identity of a user is considered immutable during the entire session. Additionally, the static length of the session timeout may impact on the usability of the service and consequent client satisfaction. 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 : *Web Security, Authentication, Continuous user verification, biometric Authentication.*

I. Introduction

Day by day the usage of web based applications and technologies are growing. Therefore security of such web-based applications is becoming important and necessary issue or 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 and identity verification. By using continuous verification the identity of the human operating the computer is continually verified. Username and password of traditional authentication system is get replace by biometric trait in case of biometric technique. Biometrics are the science and technology of determining and identifying the correct user identity based on physiological and behavioral traits which includes face recognition, retinal scans, fingerprint voice recognition and keystroke dynamics. Biometric user authentication is formulated as a single shot verification .Single shot verification provides user verification only at the login time. If the identity of user is verified once, then resources of the system are available to user for fixed period of time and the identity of user is permanent for whole session.

A basic solution is to use very short session timeouts and periodically request the user to input his/her credentials again and again. To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multi-modal bio-metric continuous authentication are proposed, turning user verification into a continuous process instead of onetime occurrence. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple biometrics traits .new approach for users verification and session management are discussed in this paper that is defined and implemented in the context of the multi-modal biometric authentication system CASHMA-(Context Aware Security by Hierarchical Multilevel Architecture). The CASHMA system realizes a secure biometric authentication service on the Internet, in this users need to remember only one username and use their biometric data rather than passwords to authenticate in multiple web services. CASHMA operate securely with any kind of web service for example online banking, military zones, and airport zone which require high security services.

II. Continuous Authentication

Authorization is the module that determines whether a user is allowed to access a specific resource. Moreover, the authorization model could provide complex access controls based on data or information or policies including user attributes, user roles / groups, actions taken, access channels, time, resources requested, external data and business rules.

A important problem that continuous authentication aims to solve the possibility that the user device like laptop is get used, stolen or forcibly taken after the user has already logged, or that the communication channels or the biometric sensors may get hacked. Users logged to a PCs are get verified through the continuous authentication .Our approach moves forward from the state of the art because it targets Internet web services. Physical presence of the user after logged in a computer are get detected by using multi-modal biometric verification system .Multi-model biometric get design and develop for that purpose only. The proposed approach assumes that first the user logs in using a strong authentication procedure, and then a continuous verification process is started based on multi- modal biometric. Verification failure together with a conservative estimate of the time required to religious the computer can automatically lock it up .In same way in a multi-modal biometric verification system is presented, continuously which verifies the presence of a user working with a computer. If in case the verification of user fails, the system reacts by locking the computer and by delaying the user's processes. or by freezing them. Authorization is the essential module that implements role-based access control.

All the above methods provide high level of security by providing continuous monitoring and verification, but all these systems requires some sort of users co-operation to authenticate the user. The objective of the proposed framework is to authenticate the user without their co-operation, i.e., irrespective of user's posture in front of the system.

2.1 Biometrics

Biometrics is generally used by means the measurement of some physical characteristic of the human body for the purpose of identifying the person. Biometrics traits include fingerprint, face image, and iris, retina pattern .A more inclusive idea of biometrics also includes the behavioral characteristics, such as gait, speech pattern, and keyboard typing dynamics .A strong link is provided between a physical person and his or her digital identities by biometric traits. Human characteristics such as face, iris and voice can't be forged, lost, shared, or stolen .They are unique because the individual is unique.

III. The Cashma Architecture

The system architecture is consisting of the CASHMA authentication service, the clients and the web services and they are connected through communication channels. Fig. 1 describes the continuous authentication system to a web service. The authentication server, which interacts with the clients, computational servers that perform comparisons of biometric data for verification of the users, and databases of templates contains the biometric templates of the users (that are required for user authentication or verification purpose).

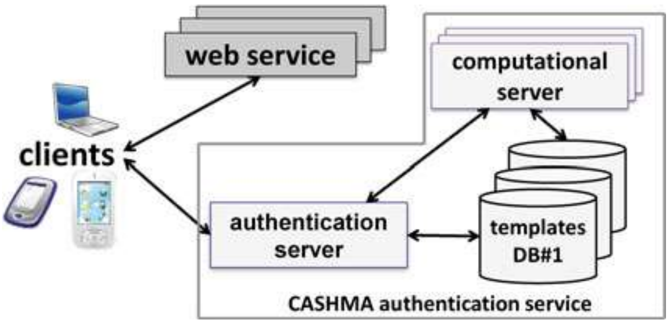

Fig 3. Architecture of CASHMA authentication system

The web service demands the authentication of users to the CASHMA authentication server. These services are any kind of Internet service. Finally, by clients we mean the users' devices like (laptops, Desktop PCs, tablets, etc.) which acquire the biometric data corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server towards a target web service. A client contains .i) sensors - acquire the raw data, ii) the CASHMA application - transmits the raw data to the authentication server. The CASHMA authentication server applies user authentication and verification procedures that compare the raw data with the biometric templates stored.

3.1 The CASHMA Certificate

In the following we have given the information contained in the body of the CASHMA certificate transmitted to the client by the CASHMA authentication server, which is necessary to understand details of the protocol. Time stamp and sequence number identify each certificate, and protect from replay attacks. the outcome of the verification is decision ,carried out on the server side. It consists of the expiration time of the session that is assigned by the CASHMA authentication server. The global trust level and the session timeout are usually computed considering the time instant in which the CASHMA application acquires the biometric data.

IV. The Continuous Authentication Protocol

The continuous authentication protocol allows providing adaptive session timeouts to a web service to set up and maintain a secure session with a client. The timeout is adapted on the basis of the trust that the CASHMA authentication system that trust puts in the biometric subsystems and in the user.

4.1 Initial phase.

In this phase: - The user (the client) communicates with the web service for a service request; the web service replies a valid certificate from the CASHMA authentication service is required for authentication. The first step is sending the data for the different biometric traits, specifically selected to perform a strong authentication procedure. The CASHMA authentication server checks the biometric data received and performs an authentication procedure.

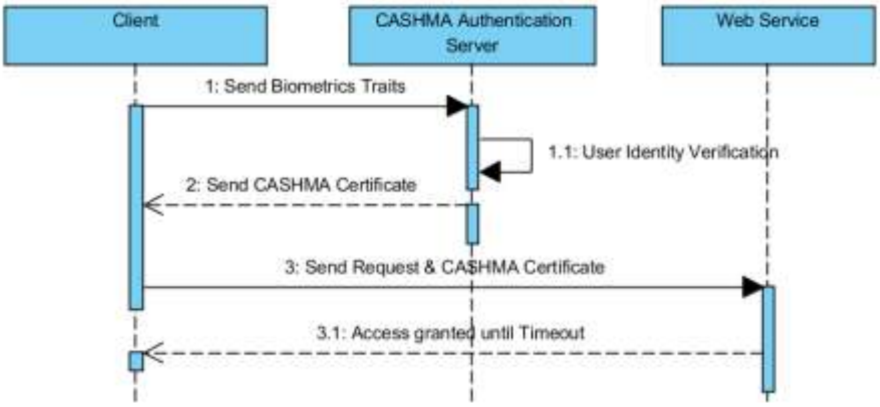
Client
CASHMA Authentication Server
Web Service
1: Send Biometrics Traits
1.1: User Identity Verification
2: Send CASHMA Certificate
3: Send Request & CASHMA Certificate
3.1: Access granted until Timeout

Fig 2. Initial phase of authentication server

There are two different possibilities arises. If the user identity is not verified (step 1:1), new or additional biometric information are requested (back to step 1); this process is repeated until the minimum trust threshold $g_{min}$is reached. If the user identity is successfully verified (step 1:1), the CASHMA authentication server authenticates the user, computes an initial timeout of length T_1 at time instant $timestamp_1$ for the user session. Creates the CASHMA certificate and sends it to the client. - The client forwards the CASHMA certificate to the web service (step 2). The certificate is read by web server and authorizes the client to use the requested service (step 3) until time timestamp.

4.2 Maintenance phase.

The aim of the maintenance phase is to reduce the risks. It includes the steps repeated iteratively: - When the client application acquires fresh raw data that corresponding to one biometric trait, it interact them with CASHMA authentication server (step 5). The biometric data can be acquired transparently to the user. When the session timeout is going to expire, the client may explicitly indicate to its user that fresh biometric data are needed. - The CASHMA authentication server verifies the identity of the user. If verification is not successful (step 5:1) the user is considered as not correct and consequently the CASHMA authentication server does not operate to refresh the session timeout. This does not show that the current session is terminated suddenly if another biometric data are provided before the timeout expires, though it is possible to get a new certificate and refresh the timeout. If verification is successful (step 6) the client receives and forwards certificate to the web service, which reads the certificate. Sets the session timeout to expire at time timestamp+ T_i(step 7).

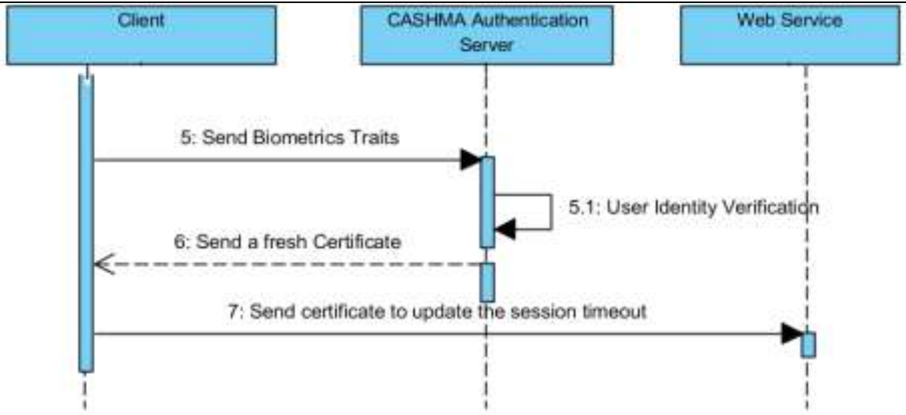
Client
CASHMA Authentication Server
Web Service
5: Send Biometrics Traits
5.1: User Identity Verification
6: Send a fresh Certificate
7: Send certificate to update the session timeout

Fig 3. Maintenance phase of authentication server

V. Trust Levels And Timeout Computation

In this section the basic definitions are introduce that are adopted in this paper. Given an unimodal biometric subsystems S_k with *k = 1, 2,..,n* that are able to deciding dependently on the authenticity of a user, the False Non-Match Rate, $FNMR_k$, is the proportion of genuine comparisons which result in false which does not matches. False non-match is the decision of non-match when comparing biometric samples which are in the form of same biometric source. It is the probability that the unimodal system S_k wrongly rejects a valid user. Oppositely, the False Match Rate, FMR_k, is the probability that the unimodal subsystem S_k makes a false match error, it wrongly decides that a invalid user is rather than valid one. A false match error in a unimodal system would lead to authenticate a invalid user. To make easy the discussion but by not losing the general applicability of the approach, we suppose that each sensor allows only one biometric trait.

5.1 Trust Levels and Timeout Computation

The algorithm to express the expiration time of the session that executes iteratively on the CASHMA authentication server it takes a new timeout and equally the expiration time each time the CASHMA authentication server receives fresh biometric data from a user. Let us consider that the initial phase happens at time $t0$ when biometric data is acquiredand transmitted by the CASHMA application of the user and that during the maintenance phase at time $t_i > t_0$forany *i=1,…, m.* new biometric data is acquired by the CASHMA application of the user u (we assume these data are transmitted to the CASHMA authentication server and lead to successful verification. The steps of the algorithm described hereafter are executed .To ease the readability of the notation, in the following the user u is often omitted; for example, $g(t_i)=g(u,t_i)$.

5.2 Computation of Trust in the Subsystems

The algorithm starts computing the trust in the subsystems .Intuitively, the subsystem trust level could be simply set to the static value $m(S_{k,}t)=1 - FMR(S_k)$.for each unimodal subsystem S_k and any time t (we assume that information on the subsystems used, including their FMRs, is contain edam a repository accessible by the CASHMA authentication server). Instead we apply a penalty function to calibrate the trust in the subsystems on the basis of its usage. Basically, in our approach the more the subsystem is used, the less it is trusted: to avoid that a malicious user is required to manipulate only one biometric trait (e.g., through sensor spoofing) to keep authenticated to the online service, we decrease the trust in those subsystems which are repeatedly used to acquire the biometric data.

5.3 Computation of Trust in the User

As time passes from the most recent user identity verification the probability that an attacker substituted to the legitimate user increases i.e., the level of trust in the user decreases. This leads us to model the user trust level through time using a function which is asymptotically decreasing towards zero. Among the possible models we selected the function in (1), which: i) asymptotically decreases towards zero; ii) yields $trust(, ti - 1)$for $\Delta t_i=0$and iii) can be tuned with two parameters which control the delay *(s)*and the slope *(k)* with which the trust level decreases over time. Different functions maybe preferred under specific conditions or users requirements in this paper we focus on introducing the protocol, which can be realized also with other functions.

VI. 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 smart phones 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, and handwritten signature recognition is impractical on most of smart phones today available on market (larger displays are required). Finally, fingerprint recognition was discarded1because few Smartphone's include a fingerprint reader. The selected biometric traits (face and voice) suit the need to be acquired transparently for the continuous authentication protocol described.

VII. Data Protection In Cashma

Very shortly, we present the security solutions adopted to protect the communication channels. We assume the usage of mechanisms as firewall to protect data stored whenever required. Channel Client – CASHMA Authentication Server. The raw data acquired by the client sensors are tra1nsmitted to the CASHMA authentication server. This calls for guarantees of confidentiality; this channel is built using TLS/SSL, configured for asymmetric authentication (a secure channel is established starting from the public key of the CASHMA server). To provide authenticity and integrity to the client and the web service, the CASHMA server appends its digital signature to the certificate released to the client. Channel Client - Web Service. The client transmits its authentication certificate to the web service. We assume that the web service contains a pairs of public-private keys.

VIII. Conclusions

Session management system is fully based on username and password, and sessions are terminated by explicit logouts or by the expiration of session timeouts. One single verification point is applied but may be seem not sufficient or not satisfactory because the identity of a user is supposed immutable during the entire session. We exploit the major possibility introduced by biometrics to define a protocol for continuous authentication which improves security and usability of a user session. The protocol computes adaptive timeouts which is based on the trust put on the activity of user and in the quality as well as the kind of biometric data user is providing. The transparent acquisition of biometric data, realized through monitoring in background the user's actions, allows maintaining the session open without explicit interactions with the user, thus improving usability. A running prototype is available for PCs.

References

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

[2]. Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, PaoloLollini, Angelo Marguglio, Andrea Bondavalli,, "Continuous and

[3]. Transparent user identity verification for secure internet services", IEEE Transactions on Dependable and Secure Computing MAY/JUNE 2015.

[4]. L . Hong, A. Jain, and S. Pankanti, "Can Multibiometrics Improve Performance?" Proc. Workshop on Automatic Identification Advances Technologies (Auto ID '99) Summit, pp. 59-64, 1999.

[5]. [4] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina,"Quantitative Security Evaluation of a Multi-Biometric Authentication System", Proc. Int'l Conf. Computer Safety, Reliability and security, pp. 209-221, 2012.

[6]. S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions" Proc. 21st Ann. Computer Security Applications Conf. (ACSAC '05), pp. 441-450, 2005.

[7]. 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, Apr.2007.