International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 6 (Nov-Dec 2016), PP.125-128

Continuous and Transparent User Identity Verification for Secure Internet Services

[1] Sneha Dalvi , [2]Dr. M.Z. Shaikh
[1]Student, [2]Principal
[1,2,] Computer Department, Bharati Vidyapeeth College of Engineering, Kharghar, Navi Mumbai
[1] Snehasonule10@gmail.com

***Abstract*— Session management in distributed Internet services is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. Emerging biometric solutions allow substituting username and password with biometric data during session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session. Additionally, the 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. The protocol determines adaptive timeouts based on the quality, frequency and type of biometric data transparently acquired from the user. The functional behavior of the protocol is illustrated through Matlab simulations, while model-based quantitative analysis is carried out to assess the ability of the protocol to contrast security attacks exercised by different kinds of attackers. Finally, the current prototype for PCs and Android smartphones is discussed.**

***Keywords*— Security, web servers, mobile environments, authentication.**

I. INTRODUCTION

In almost every aspect of human life have computing devices (such as PC, smart phone, tablet, or smart watches) become important gadgets. The communication services, aviation and financial services are very much controlled by computer systems. People entrust with vital information such as medical and criminal records, manage transactions, pay bills and private documents. However, this increasing dependency on computer systems, coupled with a growing emphasis on global accessibility in cyberspace, has unveiled new threats to computer system security. In addition, crimes and imposters in cyberspace are almost everywhere. For most existing computer systems, once the user's identity is verified at login, the system resources are available to that user until he/she exits the system or locks the session. In fact, the system resources are available to any user during that period. This may be appropriate for low security environments, but can lead to session hijacking, in which an attacker targets an open session, e.g. when people leave the computer unattended for shorter or longer periods when it is unlocked, for example to get a cup of coffee, to go and talk to a colleague, or simply because they do not have the habit of locking a computer because of the inconvenience. In high risk environments or where the cost of unauthorized use of a computer is high, a continuous check of the user's identity is extremely important.

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. THE CASHMA ARCHITECTURE

CASHMA means Context-Aware Security by Hierarchical Multilevel Architectures. This system is used 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. Depending on Preferences and requirements of the owner of the web service the CASHMA authentication service replace the traditional authentication service.

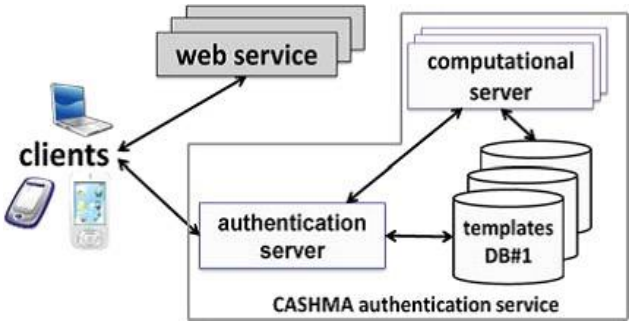

Fig.1. overall view of the CASHMA architecture

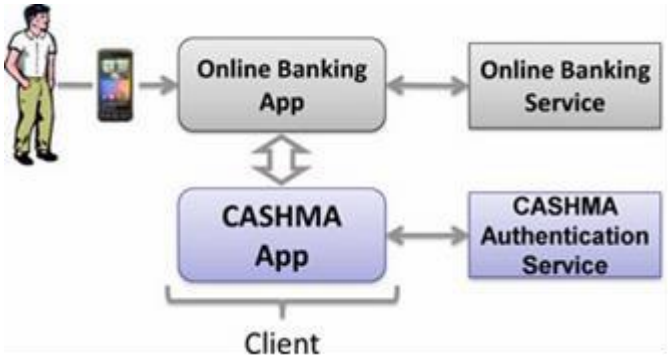

Fig2. Online Banking services using CASHMA

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). 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.

Consider online banking where a user wants to log into an online banking service using a smart phone. Here user and web services must be enrolled to CASHMA authentication service and user must be installed CASHMA application on his smart phone. The smartphone contacts the online banking service, which replies requesting the client to contact the CASHMA authentication server and get an authentication certificate. Using the CASHMA application, the smartphone sends its unique identifier and biometric data to the authentication server for verification. The authentication server verifies the user identity, and grants the access if: i) it is enrolled in the CASHMA authentication service, ii) it has rights to access the online banking service and, iii) the acquired biometric data match those stored in the templates database associated to the provided identifier. In case of successful user verification, the CASHMA authentication server releases an authentication certificate to the client, proving its identity to third parties, and includes a timeout that sets the maximum duration of the user session. The client presents this certificate to the web service, which verifies it and grants access to the client. The CASHMA application operates to continuously maintain the session open: it transparently acquires biometric data from the user, and sends them to the CASHMA authentication server to get a new certificate. Such certificate, which includes a new timeout, is forwarded to the web service to further extend the user session.

III. The CASHMA Certificate

The information contained in the body of the CASHMA certificate transmitted to the user by using the CASHMA authentication server, imperative to recognize important points of the protocol.

The CASHMA certificates consist of Time stamp and sequence number univocally identify each certificate, and it look after from replay attacks. Id is the person id, e.g., a number. Choice represents the final result of the verification process carried out on the server side. It includes the expiration time of the session, dynamically assigned by the CASHMA authentication server. Typically ,the global trust stage and the session timeout are at all times computed by way of considering the time immediate in which the CASHMA application acquires the biometric data, to restrict potential issues concerning unknown delays in conversation and computation. Due to the fact such delays will not be predicable in prior, simply supplying a relative timeout value to the user will not be viable, so the CASHMA server thus provides the absolute immediate of time at which the session must expire. The CASHMA certificates will probably be expired when the expiration timeout attain zero.

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 puts in the biometric subsystems and in the user.

The execution of the protocol is composed of two consecutive phases: the initial phase and the maintenance phase. The initial phase aims to authenticate the user into the system and establish the session with the web service. During the maintenance phase, the session timeout is adaptively updated when user identity verification is performed using fresh raw data provided by the client to the CASHMA authentication server. 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.

A. Initial phase:

Using the CASHMA application, the client contacts the CASHMA authentication server. The first step consists in acquiring and sending at time t0 the data for the different biometric traits, specifically selected to perform a strong authentication procedure (step 1). The application explicitly indicates to the user the biometric traits to be provided and possible retries. 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 gmin), new or additional biometric data are requested (back to step 1) until the minimum trust threshold gmin is reached. Instead if the user identity is successfully verified, the CASHMA authentication server authenticates the user, computes an initial timeout of length T0 for the user session, set the expiration time at T0 + t0, creates the CASHMA certificate and sends it to the client (step 2). The client forwards the CASHMA certificate to the web service (step 3) coupling it with its request. The web service reads the certificate and authorizes the client to use the requested service (step 4) until time t0 +T0.

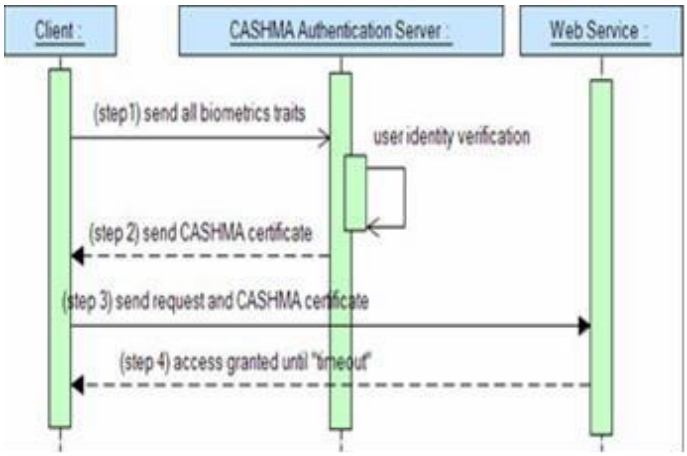

Fig.3.Initial Phase

B. Maintenance Phase

When some time the user software get fresh (new) raw data (corresponding to one biometric trait), it communicates them to the CASHMA authentication server [3] (step 5). The biometric data can also be bought transparently to the user; The CASHMA authentication server receives the biometric data from the user and verifies the identity of the person. If verification shouldn't be triumphant, then the user is marked as not professional, and thus the CASHMA authentication server does not perform. If verification is successful, the CASHMA authentication server applies the algorithm to adaptively estimate a brand new timeout of period Ti , the expiration time of the session at time Ti+ ti and then it makes and sends a new certificate to the client. The user gets a new certificate and forwards it to the web service; the online service reads the certificates and sets the session timeout to expire at time ti+ Ti. For readability, steps 1-4 are represented in Fig. 4for the case of positive user verification best [1]. Maintenance phase [1]. It is composed of three steps repeated iteratively: When at time ti the client application acquires recent (new) raw data (corresponding to one biometric trait), it communicates them to the CASHMA authentication server (step 5). The biometric data can also be received transparently to the user; the user may nevertheless make a decision to provide biometric data which are unlikely bought in a obvious approach (e.g., fingerprint). Ultimately when the session timeout goes to expire, the client could explicitly notify to the user that fresh biometric data are wanted.

The CASHMA authentication server receives the biometric data from the user and verifies the identification of the client. If verification shouldn't be successful, the client is marked as not legit, and as a result the CASHMA authentication server does not function to refresh the session timeout. This doesn't indicate that the user is cutoff from the present session: if other biometric data are provided earlier than the timeout expires, it is nonetheless feasible to get a new certificate and refresh the timeout. If verification is successful, the CASHMA authentication server applies the algorithm[1] to adaptively compute a brand new timeout of length Ti , the expiration time of the session at time Ti + ti and then it creates and sends a brand new certificate to the purchaser (step 6). The client gets the certification and supplies it to the online provider; the web carrier reads the certificates.

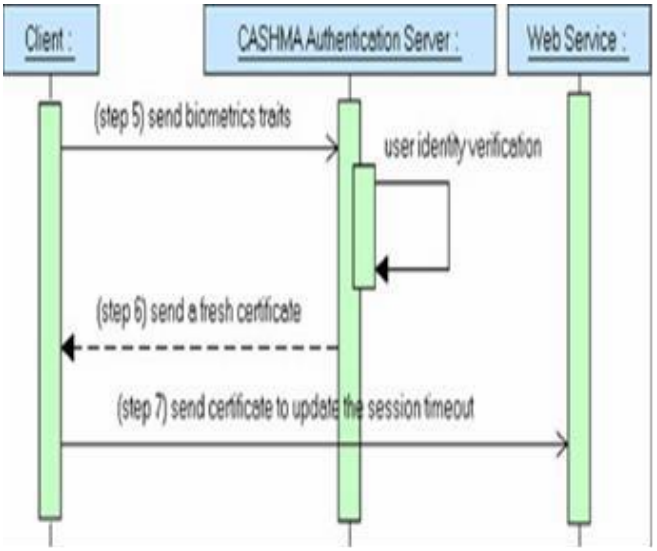

Fig. 4 Maintenance Phase

C. Trust Levels And Timeout Computation

In this section the basic definitions are introduce that are adopted in this paper. Given an unimodal biometric subsystems Sk with k = 1, 2,..,n that are able to deciding dependently on the authenticity of a user, the False Non-Match Rate, FNMRk, 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 Sk wrongly rejects a valid user. Oppositely, the False Match Rate, FMRk, is the probability that the unimodal subsystem Sk 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.

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 acquired and transmitted by the CASHMA application of the user and that during the maintenance phase at time ti> t0 for any 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(ti)=g(u,ti)

.

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(Sk,t)=1 - FMR(Sk).for each unimodal subsystem Sk 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.

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 Δti=0and 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.

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. Methods used for continuous authentication using different biometrics. Initial one time login verification is inadequate to address the risk involved in post logged in session. 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. Continuous authentication verification with multi -modal biometrics improves security and usability of user session. The functions proposed for the evaluation of the session timeout are selected amongst a very large set of possible alternatives.

REFERENCES

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

[2] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, Andrea Bondavalli "Continuous and Transparent User Identity Verification for Secure Internet Services" IEEE Transaction on De-pendable and Secure Computing, VOL. 12,NO. 3,JUNE 2015

[3] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, "Biometrics: A Grand Challenge" International Conference on Pattern Recognition , Aug 2004.

[4] 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.

[5] T.F. Dapp, "Growing Need for Security in Online Banking: Biometrics Enjoy Remarkable Degree of Acceptance,," Banking & Technology Snapshot, DB Research, Feb. 2012.

[6] A. Ceccarelli, A. Bondavalli, F. Brancati, and E. La Mattina, "Improving Security of Internet Services through Continuous and Transparent User Identity Verification," Proc. Int'l Symp. Reliable Distributed Systems (SRDS), pp. 201-206, Oct. 2012.

[7] 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.

[8] 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.

[9] Biometric System Base Secure Authentication Service for Session Management Nilima Deore, Prof. C.R.Barde International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 12, December 2015.