International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

User Identity Verification for Secure Internet Services using CASHMA

Develapalli Shushma , Joshi Padma N, Dr.Suresh Akella
[1]M.Tech Computer Science Engineering
Sreyas Institute of Engineering and Technology, Beside INDU Aranya,Nagole, Hyderabad
[2]Associate Professor, Department of Computer Science And Engineering
Sreyas Institute of Engineering and Technology, Beside INDU Aranya,Nagole, Hyderabad
[3]Principal
Sreyas Institute of Engineering and Technology, Beside INDU Aranya,Nagole, Hyderabad

Abstract: *Now a day's security of the web based services has become serious concern. Traditional authentication processes rely on username and password, formulated as a "single shot", providing user verification only during login phase . 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.*

Index Terms—Security, web servers, mobile environments, authentication.

I. INTRODUCTION

The usage of web based applications and technologies are growing day by day rapidly. There are many world events that have been directed our attention toward safety and security. Therefore security of such webbased applications is becoming important and necessary part of today's technology world. Hence, now day's biometric techniques offer emerging secure and trusted user identity verification. Every biometrics refers that the identification of a person based on his or her physiological or behavioral characteristics. Now days there are many devices based on biometric characteristics that are unique for every person. In the biometric technique, username and password is replaced by biometric data. Biometrics are the science and technology of determining and identifying themlegitimate user identity based on physiological and behavioral traits which includes face recognition, retinal scans, fingerprint, voice recognition and keystroke dynamics [3]. Also many of the biometric devices are based on the capturing and matching of biometric characteristics in order to produce a properpositive identification. The spreading use of biometric security systems increases their misuse, especially in banking and financial sectors. Biometric user authentication is formulated as a single shot verification which provides user verification only during login time. Once the identity of user is verified, the system resources are available to user for fixed period of time and the identity of user is permanent for entire session. Hence, this approach is also susceptible to attack. Suppose, here we consider this simple scenario: a user has al-ready logged into a securitycritical 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.

II. RELATED WORKS

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")

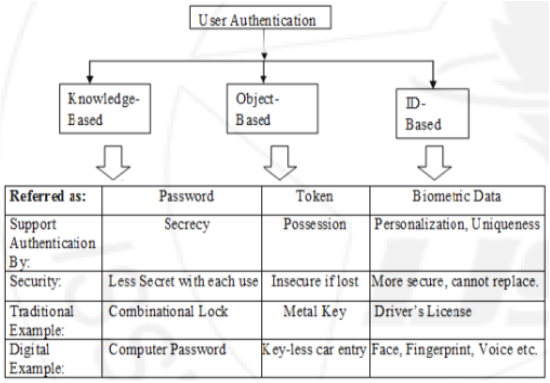
These are characterized by secrecy and includes password. The term password includes single words, phrases, and PINs (personal identification numbers) that are closely kept secrets used for authentication. But there are various vulnerabilities of password-based authentication schemes. The basic drawback 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.



Referred as:	Password	Token	Biometric Data
Support Authentication By:	Secrecy	Possession	Personalization, Uniqueness
Security:	Less Secret with each use	Insecure if lost	More secure, cannot replace.
Traditional Example:	Combinational Lock	Metal Key	Driver's License
Digital Example:	Computer Password	Key-less car entry	Face, Fingerprint, Voice etc.

Fig.1. Authenticator Categories

III. PROPOSED METHODS

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.

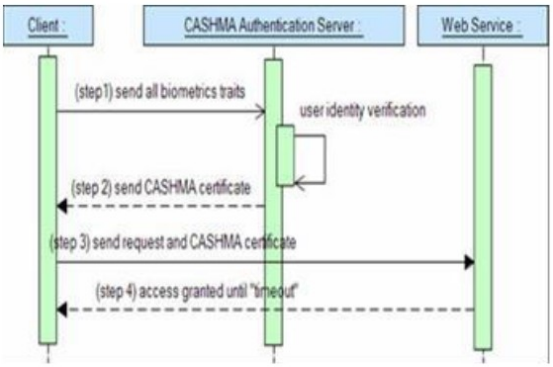


Fig.2.Initial Phase

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.

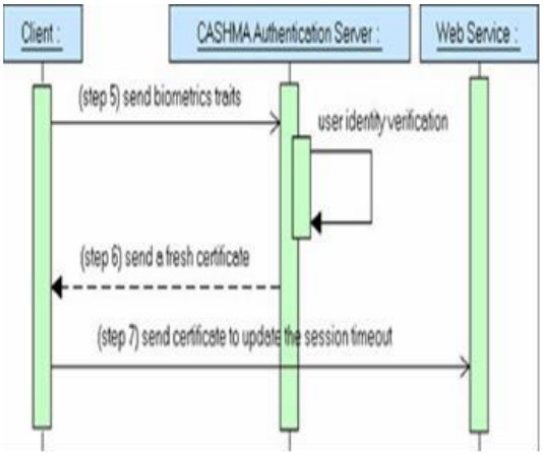


Fig. 3 Maintenance Phase

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.

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 0 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 (, t_i − 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.

IV. CONCLUSION

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.

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.

[10] C. Roberts, "Biometric attack vectors and defenses," Computers & Security, vol. 26, Issue 1, pp. 14-25, 2007.

[11] S.Z. Li, and A.K. Jain, Encyclopedia of Biometrics, First Edition, Springer Publishing Company, Incorporated, 2009.

[12] U. Uludag, and A. K. Jain, "Attacks on Biometric Systems: a Case Study in Fingerprints," Proc. SPIE-EI 2004, Security, Steganography and Water-marking of Multimedia Contents VI, pp. 622-633, 2004.