IJDCST @ Dec-2017, Issue- V-5, I-8, SW-10
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Secure Internet Services with Continuous User Identity Verification for Using Biometrics

Raja sirigiri[1], P.V Hari Prasad [2]
[1]M.Tech (cse), Dhanekula Institute of Engineering & Technology, A.P., India.
[2]Associate Professor, Dept. of Computer Science & Engineering, Dhanekula Institute of Engineering & Technology, A.P., India.

Abstract —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. 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. Also, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially in the financial and banking sectors. Biometric user authentication is typically formulated as a "one-shot" process, providing verification of the user when a resource is requested (e.g., logging in to a computer system or accessing an ATM machine). Suppose, here 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 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. 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. 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 — ***Continuous user verification, biometric Authentication, Web Security.***

1. Introduction

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 behavioural 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 the legitimate user identity based on physiological and behavioural traits which includes face recognition, retinal scans, fingerprint, voice recognition and keystroke dynamics. 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 behavioural 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.

2. Security Methods

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.

1.Fingerprint Biometrics: Fingerprint identification is one of the most well-known and publicized biometrics. Because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration.

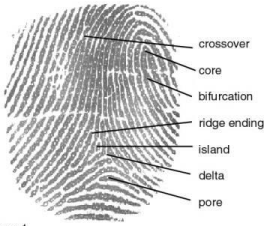


Figure 1

2.Face Biometrics: A general face recognition system includes many steps 1. Face detection, 2. Feature extraction, and 3.face recognition.Face detection and recognition includes many complementary parts, each part is a complement to the other.

3.Voice Biometrics: Speech recognition is the process by which a computer identifies spoken words. Basically, it means talking to your computer, and having it correctly recognized what you are saying. Voice or speech recognition is the ability of a machine or program to receive and interpret dictation, or to understand and carry out spoken commands.. For the voice recognition part the following steps have to be followed[5]. I) At first, we have to provide the user details as input in the form of voice asked by system. II) The system will then generate a ".wav" file and the generated file will be saved in the database for future references. III) At the time of log in by the user, user needs to provide the same information given at the time of registration and the system compares the recorded voice with the one saved in database. If both match, user logs in successfully, otherwise not.

3. Related Work

A. Continuous Authentication (CA) System: Most existing computer systems authenticate a user only at the initial log-in session. As a result, it is possible for another user, authorized or unauthorized, to access the system resources, with or without the permission of the signed-on user, until the initial user logs out. This can be a critical security flaw not only for high-security systems (e.g., the intellectual property office of a corporation) but also for lowsecurity access control systems (e.g., personal computers in a general office environment). To deal with this problem, systems need methods for continuous user authentication where the signed-on user is continuously monitored and authenticated. Biometric authentication is useful for continuous authentication. For a continuous user authentication to be user friendly, passive authentication is desirable because the system should not require user active cooperation to authenticate users continuously [11]. In addition, a single biometric trait (unimodal technique) is not sufficient to authenticate a user continuously because the system sometimes cannot observe the biometric information. For example, the system will not be able to capture a user face image if he turns his head away from the monitor. In general, to address the limitations of single biometrics, using multimodal biometrics (combining two or more single biometrics, (e.g., face and finger print) is a good solution.

B. 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

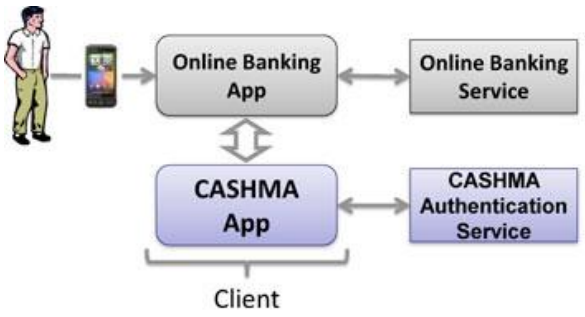
the decision of non-match when comparing biometric samples which are in the form of same biometric source. It is the probability that the unimodal system Sk wrongly rejects a valid user. Oppositely, the False Match Rate, FMRk , is the probability that the unimodal subsystem Sk makes a false match error, 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.

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 ti> t0forany 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). **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.

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.

C. CASHMA-(Context Aware Security by Hierarchical Multilevel Architecture):

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.



Conclusion &Future Work

In this paper, Continuous authentication verification with multimodal biometrics improves security and usability of 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. In future research user satisfaction, security level, cost and maintenance, I think this is the important and main challenges. The next step would be to put more attention to the check level of security, also to do more testing in order to get more accurate results.

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.Sudarvizhi, S.Sumathi, "Review on continuous authentication using multi modal biometrics, International Journal of Emerging Technology and Advanced Engineering", Volume 3, Special Issue 1, January 2013.

[7] D. M. Nicol, W. H. Sanders, K. S. Trivedi, "Model-based evaluation: from dependability to security", IEEE Trans. Dependable and Secure Computing, vol. 1 no. 1, pp. 4865, 2004.

[8] N. Mendes, A.A. Neto, J. Duraes, M. Vieira, H. Madeira, "Assessing and comparing security of web servers", IEEE International Symposiumon Dependable Computing (PRDC), pp. 313-322, 2008. [9] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, "Biometrics: a grand challenge, Proceedings of International Conference on Pattern Recognition", Cambridge, UK, Aug.2004.

[10] Sneha K. Patel, Dr. D. C. Joshi, "Mathematical Model Based Total Security System with Qualitative and Quantitative Data of Human", IntJr. of Mathematics Sciences Applications, Vol.3, No.1, January-June2013.

About authors:

Mr. RAJA SIRIGIRI is a student of Dhanekula Institute of Engineering & Technology, Ganguru , VIJAYAWADA. He is presently pursuing his M.Tech degree from JNTU,Kakinada.

Mr. P.V.HARI PRASAD is presently working as Associate professor in CSE department, Dhanekula Institute of Engineering &Technology, Ganguru ,Vijayawada.