IJCRT Publish Paper record is available at DOI: http://doi.one/10.1727/IJCRT.17187

Continuous User Identity Verification Using Biometric

Priyanka L. Patil
Department of Computer Engineering
SSBT COET Bambhori, NMU

Prof. Dr. Girish K. Patnaik
Department of Computer Engineering,
SSBT COET Bambhori, NMU

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. And, 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. 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, because the identity of user is permanent during whole session. Hence, a basic solution is to use very short period of timeouts for each session and periodically request the user credentials over and over. However it heavily affects the service usability and ultimately the satisfaction of users. The paper explores the system for continuous authentication of user using credentials such as biometric traits. The use of continuous biometric authentication system acquires credentials without explicitly notifying the user or requiring user interaction that is, transparently which is necessary to provide better service usability. Also, paper overcomes the problem of network traffic by making use of OTK for authentication purpose as transferring biometric data over low capacity network is not feasible.**

Keywords— **session management, continuous verification, multimodal biometric, transparent authentication, OTK**

I. Introduction

In current 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.

Currently used approach is also susceptible for attack because the identity of the user is constant during the whole session. Suppose, here we consider 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. Hence the need of new system to tackle this problem has arises.

To deal with the problem use very short session timeouts and request the user to input his login data again and again which 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. The use of biometric authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user to enter data over and over, which provides guarantee of more security of system than traditional one.

In a multi-modal biometric verification system designed and developed to detect the physical presence of the user logged in a computer. The proposed approach assumes that first the user logs in using a strong authentication procedure, then a continuous verification process is started based on multi- modal biometric. Verification failure together with a conservative estimate of the time required to subvert the computer can automatically lock it up. Similarly, in a verification system presented, which continuously verifies the presence of a user working with a computer. If the verification fails, the system reacts by locking the computer and by delaying or freezing the user’s processes.

The rest of the paper is organized as follows. Section II gives us the basic background about the topic along with the related research done by other people. Section III introduces the existing system. And section IV gives idea about the proposed solution to deal with current problem, while conclusion is in section V.

II. Literature Survey

A. Preliminaries

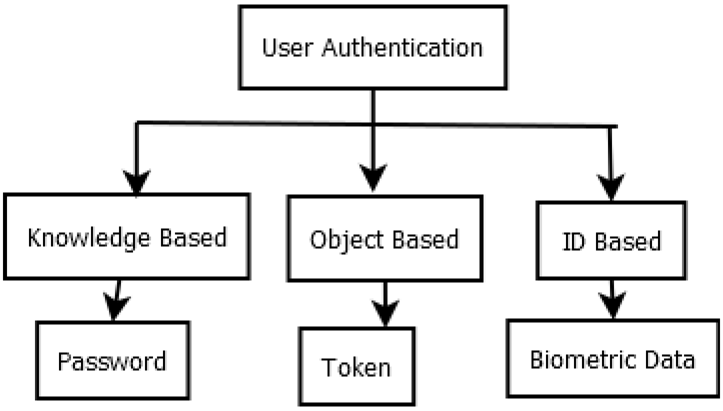

Fig. 1 User Authentication approaches

CASHMA [9], gives three approaches for user identification as shown in Fig.1. The approaches are as follow.

Primary approach is knowledge based identity for authentication of user involves is password that is what you know; Password contains single word, PIN (Personal Identification Number), Phrases that can be reserved secret for authentication. However, knowledge based identity does not offer good solution it can be searched or guess by an attacker and they do not present security against repudiation.

Secondary approach is object based identity for authentication of user involves what you have is token; Token means a physical device which provides authentication that can be security tokens, access token, storage devices including passwords such as smart card or bank cards. The main disadvantage is identity token can be lost or stolen and inconvenience and cost.

Last approach is ID based authentication for authentication of user it considers who you are. That is simply biometric such as voice recognition, figure print identification, face recognition and signature or eye scan give stronger defence against attack. Comparing with Knowledge based and object/entity based ID based authentication provides privileged level of security.

To achieve computer security with biometric four ways are presented as follow.

1) Keystroke Biometric

It is a type of behavioural biometric; it's an easy method for authenticating users where the users typing behaviour for validating identity is considered. Keystroke dynamics is simply "how you type not what you type" [10]. It uses raw keystroke data to obtain timing features.

2) Voice Biometric

A voice biometric is unique for each individual like fingerprint. Voice biometric called numerical modelling consist sound pattern or rhythm of a user's voice, sound. Voice biometric uses dissimilar characteristics of individual to distinguish between two speakers. This biometric is an interaction tool to user for verification [11].

3) Face Biometric

Face biometric includes detection and reorganization of human faces from digital image or video source. Facial database is required to distinguish certain feature from image. Face Identification and extraction includes many complementary parts. This type of authentication scheme is normally used in security systems [12].

D. Finger Print Scan Biometric

Fingerprint scan biometric recognition is well known identification due to its easiness of acquisition. Several sources (ten fingers) available for acquisition and because of such uniqueness and uniformity fingerprint recognition are very famous. S. Kumar [4] represented a Multimodal biometric scheme which is developed to discover physical existence of individual sign in a computer. Approach considers that primary user login using strong authentication, and then depends on multimodal biometric continuous verification started. In Ojala [3] wristband a wearable authentication device is offered for continuous authentication of user where by wearing device user can login and continuous authentication takes place.

B. Background

L. Montecchi et al, in [6], said biometrics is commonly perceived as a strong authentication method; in practice several well-known vulnerabilities exist, and security aspects should be carefully considered, especially when it is adopted to secure the access to applications controlling critical systems and infrastructures. System performs a quantitative security evaluation of the multi-biometric authentication system, assessing the security provided by different system configurations against attackers with different capabilities. The analysis is performed using the modeling formalism, a formalism for security evaluation that extends attack graphs; it allows to combine information on the system, the attacker, and the metrics of interest to produce quantitative results. The obtained results provide useful insight on the security offered by the different system configurations, and demonstrate the feasibility of the approach to model security threats and countermeasures in real scenarios.

L. Montecchi et al, in [7], said current infrastructures are characterized by increasing requirements of reliability, security, performance, availability, adaptability. A relevant issue is represented by the scalability of the system with respect to the increasing number of users and applications, thus requiring a careful dimensioning of resources. Furthermore, new security issues to be faced arise from exposing applications and data to the Internet, thus requiring an attentive analysis of potential threats and the identification of stronger security mechanisms to be implemented, which may produce a negative impact on system performance and scalability properties. The paper presents a model-based evaluation of scalability and security tradeoffs of a multi-service web-based platform, by evaluating how the introduction of security mechanisms may lead to a degradation of performance properties. The evaluation focuses on the openness platform, a web-based platform providing different kind of services, to different categories of users. The evaluation aims at identifying the bottlenecks of the system, under different configurations, and assess the impact of security countermeasures which were identified by a thorough threat analysis activity previously carried out on the target system. The modeling activity has been carried out using the Stochastic Activity Networks (SANs) formalism, making full use of its characteristics of modularity and reusability. The analysis model is realized through the composition of a set of predefined template models, which facilitates the construction of the overall system model, and the evaluation of different configuration by composing them in different ways.

U. Uludag et al, in [8], mentions despite numerous advantages of biometrics-based personal authentication systems over traditional security systems based on token or knowledge, they are vulnerable to attacks that can decrease their security considerably. Here analyzation of these attacks in the realm of a fingerprint biometric system is done. Author proposed an attack system that uses a hill climbing procedure to synthesize the target minutia templates and evaluate its feasibility with extensive experimental results conducted on a large fingerprint database. Several measures that can be utilized to decrease the probability of such attacks and their ramifications are also presented.

C. Related Work

S. Kumar et al, in [1], used the combination of digital camera-based face verification with a mouse-based fingerprint reader. The main objective is to build a multi-modal biometric feedback mechanism into the operating system so that verification failure can automatically lock up the computer. The user's biometric features are entered into the database during the enrollment phase. Then during the continuous verification, the user first presents the biometric data which is then pre-processed. In case of fingerprint, a matching algorithm is used to compute the similarity score between the input and the biometric already stored in the database. In case of face verification, the viola-jones face detector algorithm is used. Then the integration of biometric observations across modalities and time is done using Hidden Markov model. Finally, biometric feedback is integrated into the operating system. Problem with system is if the OS integrated feedback mechanism fails, it can make way for illegal user access. And verification using fingerprint-enabled mouse decreases the usability.

T. Sim et al,in [2], presented the use of two biometric modalities: face and fingerprint and it can be extended to use more modalities. Also, paper has proposed new metrics for measuring the performance of the system. The user logs in at the console using the kdm session manager, kdm authenticates the user using a password. Then it starts the face and fingerprint verification. Once the integrator has the user-id of the logged in user, it loads the biometric profile corresponding to the user and starts acquiring biometric observations using the video and fingerprint. The integrator is the central coordinating entity that combines verification results and communicates the value of Psafe to the kernel. The viola-jones face detector algorithm is used for face verification. Finally, the continuous verification system is integrated into the operating system. The paper uses false accept rate and false reject rate and additional performance metrics: time to correct reject, probability of time to correct reject and usability. Problem with given system is failure in the inbuilt feedback system may lead to access by imposter.

S. Ojala et al,in [3], presented wearable authentication device (a wristband) for a continuous user authentication and transparent login procedure in web applications. By wearing the authentication device, the user can login transparently through a wireless channel and can transmit the authentication data to computers by just approaching them. Here fingerprint is used for authentication using the wristband and to ensure that the person is wearing the device, it measures continuously vital signs (skin temperature and heart rate) along with body capacitance and acceleration. The heart rate of the user could be obtained from the pulse oximeter output. The received signal strength of the wireless connection offered an inexpensive and simple way to implement the transparent login by estimating the range between the user and a terminal. Major drawback of the system is failure in the inbuilt feedback system may lead to access by imposter. And temperature and heartbeat is being sensed for continuing the session, which is not a personal identity thus leading to imposter access of sensitive data.

Joseph Roth et al,in [4], used the method of keystroke for recognizing a legal user. Using digraphs, a virtual alphabet is learned from keystroke sound segments. Then the digraph latency within the pairs of virtual letters along with the other statistical features is used to generate match scores. The resultant scores are used to indicate the similarity between two sound streams. If the computed similarity score is high then the user can continue the session otherwise he/she is found to be an imposter and logged out of the system. Drawback of the system is that current database is constrained in the number of subjects, single keyboard, consistent typing environment, and single day of collection. And keystroke can also be done by illegal user as the system lacks in identifying keystrokes using supervised learning or context sensitive threshold.

Andrea et al, in [5], proposed a secure protocol 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 system uses face verification for continuous authentication. The CASHMA authentication service [9] includes an authentication server, a set of computational servers and databases of templates that contain the biometric templates of the enrolled users. Clients acquire the biometric data (the raw data) corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server as part of the authentication procedure towards the target web service. A client contains sensors to acquire the raw data and the CASHMA application which transmits the biometric data to the authentication server. The authentication server verifies the user identity, and grants the access if the user is enrolled in the CASHMA authentication service and if 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. Problem with given system is that qualities of images are not considered very specifically. And during low light conditions the application may fail to detect legal user due lack of quality.

III. EXISTING SYSTEM

In traditional systems once the user's identity has been verified, the system resources are available for a fixed period or until explicit logout from the user. Which 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.

In existing S. Ojala [3], a multi-modal biometric verification system is designed and developed to detect the physical presence of the user logged in a computer. The work in another existing paper Andrea [5], proposes a multi-modal biometric continuous authentication solution for local access to high-security systems as ATMs, where the raw data acquired are weighted in the user verification process, based on type of the biometric traits and time, since different sensors can provide raw data with different timings. It introduces the need of a temporal integration method which depends on the availability of past observations: based on the assumption that as time passes, the confidence in the acquired (aging) values decreases. The paper applies a degeneracy function that measures the uncertainty of the score computed by the verification function. In all of implemented multimodal biometric system biometric traits are needed to be transferred over the network for processing.

To detect and prevent access from unauthorized person, we are proposing a solution which is based on biometric data of user and turn user verification into continuous process rather than a onetime occurrence.

IV. PROPOSED SYSTEM

Proposed system provides a new method for continuous user authentication that continuously collects biometric information. It turns user verification into continuous process than a onetime occurrence. Hence, proposed system provides an implementation of an efficient authentication system for secure internet services that provides continuous and transparent user identity verification using biometric traits. Also tries to reduce network traffic by converting biometric information in One Time Key(OTK) and transferring it over network instead of whole biometric data again and again.

A. System Architecture

The Fig.2 illustrates idea about system architecture. Session management is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using timeouts. Which is replaced with continuous verification using biometric traits of user. In proposed system assume that user has been logged in to the system using strong authentication system. Then for continuous verification user's biometric traits are acquired transparently and continuously and are send to the server by converting it in form of OTK. Server will match the OTK with its OTK, generated from stored biometric traits of authorized user. If both match then session is continued otherwise it will be turned off.

Algorithm 1 shows flow of proposed system.

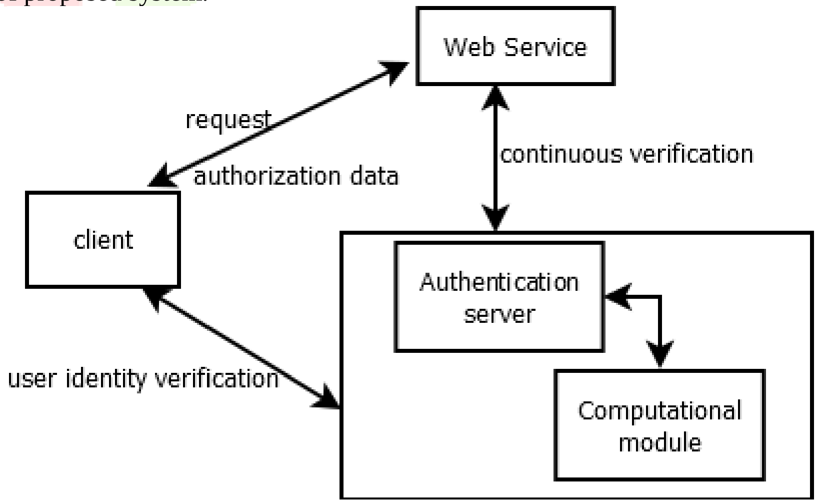

Fig. 2 Proposed System Architecture

Algorithm 1: Continuous Verification

1. Client logins to the system.
2. server performs user verification, and will generate a symmetric key if authorized user.

3. Access granted with session timeout if authorized along with the symmetric key.

For continuous verification

4. client generates one-time key by its current biometric traits and symmetric key sent by server using hashing technique.
5. key is send to authorization server,
6. server also generates one-time key by users stored biometric traits and symmetric key with same hashing technique.
7. if both server side and client-side keys are same then
   users continuous access is granted
   else
   web service access will be revoked.

V. Conclusion

The paper explores various existing methods used for continuous authentication using different biometrics. As initial one-time login verification is inadequate to address the risk involved in post logged in session, paper exploited the novel possibility to propose a solution to build a continuous user verification system by choosing multimodal biometric. Also, provids solution to reduce network traffic by making use of OTK instead of transferring biometric data which is quite large and will take more time to transfer.

References

[1] 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.

[2] 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.

[3] S. Ojala, J. Keinanen, and J. Skytta, "Wearable Authentication Device for Transparent Login in Nomadic Applications Environment," Proc. Second Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 1-6, Nov. 2008.

[4] Joseph Roth, Xiaoming Liu, Arun Ross and Dimitris Metaxas, "Investigating the Discriminative Power of Keystroke Sound and provide authentication," IEEE Trans. Information Forensics and Security, vol. 10, no. 2, pp. 333-345, Feb. 2015.

[5] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Agnelo Marguglio and Andrea Bondavalli, "Continuous and Transparent User Identity Verification for Secure Internet Services", IEEE Trans. Dependable and Secure Computing, vol. 12, no. 3, pp. 270-283, June. 2015.

[6] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, , Quantitative Security Evaluation of a Multi-biometric Authentication System," International Conference on Computer Safety, Reliability, and Security SAFECOMP 2012: Computer Safety, Reliability, and Security pp 209-221

[7] L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and A. Bondavalli, "Model-based evaluation of scalability and security tradeoffs: A case study on a multi-service platform," Electronic Notes in Theoretical Computer Science 310 (2015) pp 113–133

[8] U. Uludag and A.K. Jain , "Attacks on Biometric Systems: A Case Study in Fingerprints,"

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

[10] Koichiro Niinuma and Anil K. Jain, "Continuous User Authentication Using Temporal Information", Proc. SPIE 7667, Biometric Technology for Human Identification VII, 76670L (April 14,2010); doi:10.1117/12.847886.

[11] 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.

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