International Journal of Technology and Engineering System (IJTES)
Vol 8. No.1 – Jan-March 2016 Pp.95-100
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976-1345

SECURE INTERNET SERVICES FOR CONTINUOUS AND OBVIOUS USER IDENTITY AUTHENTICATION

M.K.Tamilazhagi,
PG Scholar, Department of CSE,
E.G.S Pillay Engineering college,
Nagapattinam, India
tamilazhagimk@gmail.com

Mr.V.M.Suresh
Assistant Professor, Department of CSE,
E.G.S Pillay Engineering College,
Nagapattinam, India

ABSTRACT

Biometric technology can be used for a tremendous number of applications. Session Management in distributed internet services is popularly based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. Appearing biometric solutions allow alternate username and password with biometric data during session installation, but in such an approach still a single authentication is allowed acceptable and the identity of a user is considered changeless during the entire session. Additionally, the length of the session timeout may contact on the operation of the service and consequent client satisfaction. It analyze promising alternatives offered by applying biometrics in the management of sessions. A secure protocol is labeled for constant authentication through continuous user verification. The protocol determines modifying timeouts based on the quality, frequency and type of biometric data expressly captured from the user.

keywords:- *User Authentication, Biometrics, Security, Web Server*

I.INTRODUCTION

Network Security is a prevention and monitor unauthorized access, misuse, modification or denial of a computer and network-available resources. Network security involves the identification of access to data in a network, which is controlled by the network administrator. A strong system is one in which the cost of attack is greater than the potential gain to the attacker. Contrarily, a weak system is one where the cost of attack is less than the unrealized gain. Authentication factors are grouped into these three levels: 1) what you know (e.g., password), 2) what you have (e.g., token), and 3) who you are (e.g., biometric).

Knowledge-base are characterized by secrecy and includes password. The term password includes single words, expressions and PINs (Personal Identification Numbers) that are firmly kept secrets used for authentication. But there are various accountability 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, arbitrary, changing password is challenging to remember. Also, each time it is communal for authentication, so it becomes less secret. They do not provide good understanding detection, and they do not offer much defense against repudiation.

Object-based are represented by physical retention 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 and smart card. A token can provide three advantages when combined with a password.

ID-Based are characterized by uniqueness to one person. One advantage of a biometric is that it is less easily stolen than the other users, so it provides a stronger defense against repudiation. For both ID records and biometrics, the dominant security defense is that they are difficult to copy. However, if a biometric is adjustable or a document is lost, they are not as easily disposable as passwords or tokens.

SECURE INTERNET SERVICES

Biometrics is the science of constituting identity of specific based on the physical and behavioral attributes of the user. The importance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality commit on the accurate determination of an individual’s identity in the situation of several different applications. Some of biometric data is illustrated as follows.

FACE BIOMETRICS

A general face recognition system includes frequent steps. Face detection, Feature extraction and face recognition. Face detection and recognition includes many integral parts, each part is a correlate to the other. Depending on regular system each part can work individually. Face disclosure is a computer technology that is based on learning algorithms to designate human faces in digital images.

KEYSTROKE BIOMETRICS

Keystroke biometrics or checking keystroke dynamics is considered to be an uncomplicated behavioral established method for authenticating users which employs the person’s typing patterns for validating his identity. Keystroke dynamics is “not what you type, but how you type.” In this way, the user types in text, as usual and without any kind of unused work to be done for authentication. Besides, it only involves the user’s own keyboard and no other exterior hardware.

FINGERPRINT SCAN BIOMETRICS

Fingerprint verification is one of the most well-known and important biometrics. Because of their singleness and compactness over time, fingerprints have been used for identification for over a century, more newly becoming computerized due to advancements in computing capabilities. Fingerprint identification is popular because of the inherent ease in obtainment, the various sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration**.**

II.RELATED WORKS

David M. Nicol et al. [1] have proposed in network security for new techniques to designating system perseverance and compile how they are now being extended to evaluate system security. To find that many techniques from dependability evaluation can be practiced in the security domain, but that significant challenges remain, largely due to fundamental contrast between the accidental nature of the faults commonly affected in dependability evaluation, and the intentional human nature of cyber-attacks.

Sandeep Kumar et al. [2] have designed in the main core of our work is to build a multi-modal biometric evaluation mechanism into the operating system so that authentication collapse can naturally lock up the computer within some estimate of the time it takes to corrupt the computer. This must be done with low false positives in order to realize a usable system show through preliminary results that combining multiple suitably chosen modalities in our theoretical framework can completely do that with currently available off-the-shelf components.

William H. Sanders et al. [3] proposed the system and adversary characterization data that are collected as input for the executable model. This project also describes the simulation algorithms for adversary attack behavior and the computation for the anticipation that an attack attempt is successful. A simple case study illustrates how to analyze system security using the ADVISE method. A devise is presently under development to simplify automatic model generation and simulation. The ADVISE method aggregates security-significant information about a system and its adversaries to produce a perceptive security analysis profitable for holistic system security decisions.

Anil K. Jain et al. [4] focused on the information security require the conservation of information elements (e.g., multimedia data) thereby that only authorized users are able to access the contents available in digital media As a result, these keys are stored elsewhere (for example, on a computer or a smart card) and released based on some different authentication mechanism (e.g., password). Mostly passwords are so simple, that they can be easily suggested (especially based on social engineering methods) broken by simple dictionary attacks. It is not surprising that the most frequently used password is the word “Password”. Biometric authentication or simply biometrics refers to constituting identity based on the physical and behavioral aspects (also known as traits or identifiers) of an individual such as face, fingerprint, hand geometry, keystroke, signature, voice, etc. Biometric systems offer several dominance over traditional authentication design. They are inherently more reliable than password-based insuring authentication as biometric traits cannot be lost or abandoned (passwords can be lost or forgotten) biometric traits are difficult to copy, share and distribute (passwords can be declared in hacker websites) and they require the person being authenticated to be present at the time and point of authentication (users can deny that they have shared the password). It is complicated to duplicate biometrics (it requires more time, money, experience, access privileges) and it is unlikely for a user to repudiate having accessed the digital content using biometrics.

Skytta J et al. [5] focused on wearable authentication device for continuous user authentication and transparent login actions in pastoral applications environment, where users are mobile and current authentication methods are impossible. The wearable authentication device is a wristband in which the user authentication is done by using the fingerprint and to ensure that the person is exhausting the device, it measures continuously his vital signs (skin temperature and heart rate) along with body coincidence and acceleration. By wearing the authentication device, the user can login continuously to any computer simply by approaching it.

Jidnya Shah et al. [6] proposed technique utilizes minutiae triplet information to estimate the orientation map of the parent fingerprint. The predicated orientation map is noticed to be remarkably consistent with the underlying ridge flow. Preliminary results indicate that the clearly random minutiae distribution of a fingerprint can reveal important class information. Additionally, contrary to what has been claimed by several minutiae-based fingerprint system vendors, demonstrate that the minutiae template of a user may be used to regenerate fingerprint images.

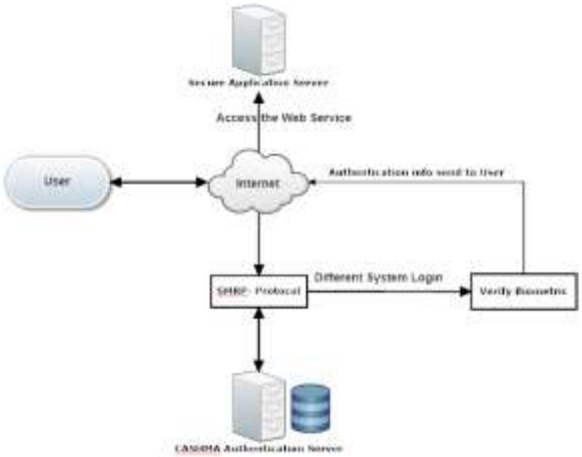
Zach Jorgensen et al. [7] proposed the idea of using one's behavior with a pointing device, such as a mouse or a touchpad, as a behavioral biometric for authentication goal has gained increasing attention over the past decade. A number of interesting approaches based on the idea have developed in the literature and promising experimental results have been reported. The results of several experiments that illustrate our observations and suggest guidelines for evaluating future authentication approaches based on mouse dynamics. He also discuss a number of avenues for additional research that are fundamental to advance the state of the art in this area.

Poonam Mahale et al. [8] proposed the web services become a very popular way of communication and online transactions for the people. These services are widely distributed all over the world. So, the security of these web services is a major challenge in present days. To achieve the security, the better user authentication mechanisms are important in security systems. A conventional security system verifies the user identity using the pair of username and password at the time of user login. Once the user is successfully authenticated with the username and password, he/she is able to access the service but no further checks are provided during the sessions in which user is working. Emerging biometric mechanisms replaces the username and password by biometric profile of user during the session establishment, but in this approach a single short verification is not sufficient and the user's identity is considered as a permanent during the entire session. A solution is to provide the session timeouts and request user to input his/her credentials over and over, but these impacts the user's service usability and ultimately the satisfaction of user.

III.PROPOSED DESIGN

An approach for user verification and session management that is applied in the context aware security by hierarchical multilevel architectures (CASHMA) system for immune biometric authentication on the Internet. CASHMA is able to operate securely with any measure of web service, including services with high security appeal as online banking services, and it is planned to be used from different client devices. The CASHMA authentication service can aggregate a classical authentication service, or can replace it. CASHMA for adaptable and highly secure user sessions is a continuous consequent (a single biometric modality at once is granted to the system) multi-modal biometric authentication protocol which flexibility measure and refreshes session timeouts on the basis of the trust put in the client. CASHMA includes correctness to protect the biometric data and to assured user privacy, including policies and procedures for proper registration. Protection of the acquired data during its transmission to the authentication and computational servers and its storage, robustness improvement of the algorithm for biometric authentication.

- ❖ The application operates to continuously maintain the session open.
- ❖ It transparently acquires biometric data from the user, and sends them to the authentication server to get a new certificate.
- ❖ The main task of the proposed protocol is to create and then maintain the user session adjusting the session timeout on the basis of the confidence that the identity of the user in the system is genuine



System Architecture

THE USER TRUST LEVEL

The user trust level indicates the trust placed by the CASHMA authentication service in the user u at time t, i.e., the possibility that the user u is a convenient user just considering his behavior in terms of device usage (e.g., time since last keystroke or other action)and the time since last acquisition of biometric data.

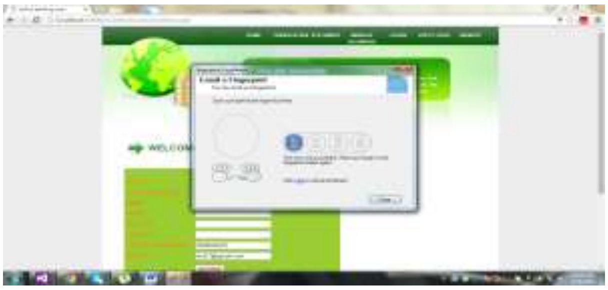
THE GLOBAL TRUST LEVEL

The Global trust level describes the belief that time the user in the system is actually a permissible user considering the combination of all subsystems trust levels.

THE TRUST THRESHOLD

The Trust threshold is a lower threshold on the global trust level required by a specific web service. The user is authenticated and is assumed access to the service.

IV. EXPERIMENTAL ANALYSIS



Enroll a Fingerprint

CASHMA Certificate

Continuous Authentication

V.CONCLUSION

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 evidently through monitoring in background the user's actions. While performing a client-side quality analysis of the data acquired would be a reasonable approach to reduce computational burden on the server and it is compatible with our objective of designing a protocol independent from quality ratings of images this goes against the CASHMA requirement of having a light client.

REFERENCES

[1] Allano.L, Dorizzi.B and Garcia-Salicetti.S, "Tuning Cost and Performance in Multi-Biometric Systems: A Novel and Consistent View of Fusion Strategies Based on the Sequential Probability Ratio Test (SPRT)," Pattern

Recognition Letters, vol. 31, no. 9, pp. 884-890, 2010.

[2] Casey.T, “Threat Agent Library Helps Identify Information SecurityRisks,” White Paper, Intel Corporation, Sept. 2007.

[3] Ceccarelli.A, Bondavalli.A, Brancati.F and La Mattina.E, “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.

[4] Cinque.M, Cotroneo.D, Natella.R, and Pecchia.A, “Assessing and Improving the Effectiveness of Logs for the Analysis of Software faults,” Proc. Int’l Conf. Dependable Systems and Networks (DSN), pp. 457-466, Sep 2010.

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

[6] Evans.S and Wallner.J, “Risk-Based Security Engineering through theEyes of the Adversary,” Proc. the IEEE Workshop Information Assurance, pp. 158-165, June 2005.

[7] Sandeep Kumar, T. Sim, Rajkumar Janakiraman, and S. Zhang. Using continous biometrics verification to protect interactive login sessions. To appear in the 21st Annual Computer Security Applications Conference, 2014
.