ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

A Secure Protocol for Perpetual Authentication through Continuous User Verification

N. Keerthi[1], S.G.Nawaz[2], M.Harathi[3], Dr. R.Rama Chandra[4]

M.Tech Student, Dept. of CSE, SKD Engineering College, GOOTY, Affiliated To JNTUA, India [1]

Associate Professor & HOD, Dept. of CSE, SKD Engineering College, GOOTY, Affiliated To JNTUA, India [2]

Associate Professor, Dept. of CSE, SKD Engineering College, GOOTY, Affiliated To JNTUA, India [3]

Principal, SKD Engineering College, GOOTY, Affiliated To JNTUA, India [4]

ABSTRACT: Secure user authentication is key in most of contemporary ICT systems. User authentication systems square measure historically supported pairs of username and secret and verify the identity of the user solely at login section. No checks square measure performed throughout operating sessions, that square measure terminated by a precise logout or expire once associate degree idle activity amount of the user. Security of web-based applications may be a serious concern, as a result of the recent increase within the frequency and complexness of cyber-attacks; biometric techniques supply rising answer for secure and sure authentication, wherever username and secret square measure replaced by biometric information. However, parallel to the spreading usage of biometric systems, the motivation in their misuse is additionally growing, particularly considering their potential application within the money and banking sectors. In this paper a new approach for user verification and session management is developed and applied within the Context Aware Security by hierarchic structure design system for secure biometric identification on the web. CASHMA is in a position to control firmly with any quite internet service, as well as services with high security demands as on-line banking services, and it's meant to be used from completely different consumer devices. counting on the preferences and needs of the owner of the net service, the CASHMA authentication service will complement a standard authentication service, or we are able to replace it. we tend to exploit the novel chance introduced by statistics to outline a protocol for continuous authentication that improves security and value of user session. The protocol computes adaptative timeouts on the premise of the trust expose within the user activity and within the quality and type of biometric information noninheritable transparently through watching in background the user's actions.

KEYWORDS: Security, Web Servers, Mobile Environments, Authentication.

I. INTRODUCTION

In this 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 behavioral 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. Infact, 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. This approach is also susceptible for attack because the identity of the user is constant during the whole session. Suppose,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

here we consider this 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. The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this 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. Finally, 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.

II. LITERATURE SURVEY

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(password), 2) what you have (token), and 3) who you are (Biometric).

A. KNOWLEDGE-BASED

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

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

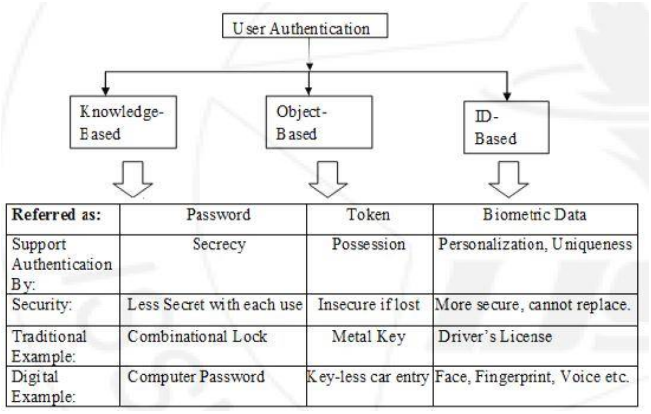
They are characterized by uniqueness to one person. A driver's license, passport, etc., all belong in this category. So does a biometric, such as a fingerprint, face, voiceprint, eye scan, or signature. One advantage of a biometric is that it is less easily stolen than the other authenticators, so it 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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016



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 SYSTEM

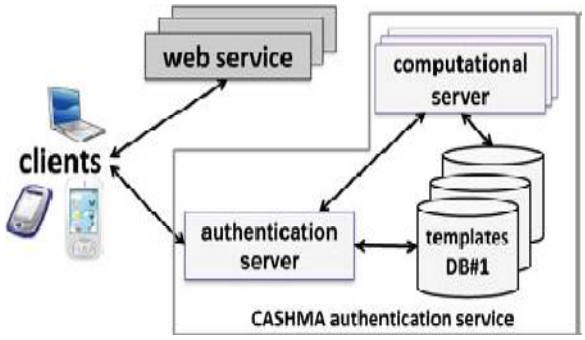


Fig.2.CASHMA Authentication service

Session management in distributed Internet services is traditionally based on username and password, and explicit logouts and timeouts that expire due to idle activity of the user. Biometric solutions allow substituting username and password with biometric data; e.g., a user may submit its fingerprint instead of the pair username-password. However a single verification step is still deemed sufficient and the identity of a user is considered immutable during the entire session. Additionally, the static length of the session timeout may impact on the usability of the service and consequent client satisfaction. CASHMA can authenticate to web services, ranging from services with strict security requirements as online banking services to services with reduced security requirements as forums or social networks. Additionally, it can grant access to physical secure areas as a restricted zone in an airport, or a military zone (in such cases the authentication system can be supported by biometric kiosk placed at the entrance of the secure area). We explain the usage of the CASHMA authentication service by discussing the sample application scenario in Fig. 2 where a user u wants to log into an Online Banking service using a smart phone.

An alternative for the establishment and management of sessions is offered by biometrics, and consists on multimodal biometric continuous authentication performed through continuous user verification based on biometric data acquired. The sensors on the client (e.g., the camera and microphone of a smart phone or of a laptop) acquire biometric data transparently to the user and sent to the authentication service. This makes user verification a continuous process, rather than a one-time occurrence. Also the length of the timeout may be configured depending on the user history and the trust that the authentication service place in the user.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

B. CHALLENGES AND OPPORTUNITIES

Considering separately uni-modal and multi-modal biometrics systems, identify:

The main challenges of applying a continuous authentication approach for Internet services using a mobile device in heterogeneous environments(e.g., noisy environments as train stations, market place), and

• The main opportunities offered by such approach.

C. DESIGN A SOLUTION

Design and evaluate a simple continuous authentication for mobile devices that authenticate to Internet services. Consider separately the case of uni-modal biometric systems and a multi-modal one. Consider two different kinds of Internet services:

- Internet services with stringent requirements in terms of security.
- Internet services with stringent requirements in terms of availability of the communication, but relaxed requirements on security.

IV. IMPLEMENTATION

A complete analysis of the CASHMA system was carried out during the CASHMA project, complementing traditional security analysis techniques with techniques for quantitative security evaluation. Qualitative security analysis, having the objective to identify threats to CASHMA and select countermeasures, was guided by general and accepted schemas of biometric attacks. A quantitative security analysis of the whole CASHMA system was per-formed.

A. SYSTEM MODEL

In this module, we create the procedure mannequin to assess and put into effect our proposed method. CASHMA can authenticate to net offerings, ranging from services with strict security standards as online banking services to services with decreased safety specifications as forums or social networks. Additionally, it will probably furnish entry to bodily at ease areas as a constrained zone in an airport, or a army zone (in such circumstances the authentication system can be supported by way of biometric kiosk placed on the entrance of the comfortable area). We provide an explanation for the utilization of the CASHMA authentication provider by means of discussing the pattern utility situation, where a person u desires to log into a web-based banking service.

User identification" refers back to the identification of the consumer obtained from the financial institution for the cause of logging into the web Banking facility furnished by the financial institution.

Login Password" is a distinct and randomly generated password known best to the patron, which can be transformed via the consumer to his/her convenience. This is a means of authenticating the user ID for logging into Internet Banking.

"Transaction Password" is a unique and randomly generated password known only to the customer, which can be changed to his/her convenience. This is a means of authentication required to be provided by the customer for putting through the transaction in his/her/their/its accounts with Bank through Internet Banking. While User ID and Password are for valid access into the internet application, giving valid Transaction Password is for authentication of transaction/requests made through internet.

B. AUTHENTICATION SERVER

In web banking as with natural banking approaches, security is a principal trouble. Server will take each precaution vital to be sure your understanding is transmitted safely and securely. The today's ways in web banking method protection are used to develop and reveal the integrity and security of the system.

The Server maintains the functionality:

- customer details
- Activation of Beneficiary
- Transaction details
- spark off Blocked Account

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

C. CASHMA CERTIFICATE

In this module, we reward the know-how contained within the physique of the CASHMA certificate transmitted to the purchaser by the CASHMA authentication server, integral to understand important points of the protocol. Time stamp and sequence number univocally determine each and every certificate, and preserve from replay assaults. Identity is the user identification, e.g., a number.

Selection represents the end result of the verification procedure applied on the server part. It involves the expiration time of the session, dynamically assigned by way of the CASHMA authentication server. In fact, the worldwide believe degree and the session timeout are consistently computed considering the time immediate where the CASHMA software acquires the biometric information, to hinder skills issues regarding unknown delays in communique and computation.

D. CONTINUOUS AUTHENTICATION

A secured protocol is defined for perpetual authentication by means of steady user verification. The protocol determines adaptive timeouts centered on the nice, frequency and form of biometric data transparently received from the user. Using biometric authentication permits credentials to be bought transparently, i.e., without explicitly notifying the user or requiring his/her interplay, which is primary to warranty higher carrier usability.

The thought behind the execution of the protocol is that the consumer consistently and transparently acquires and transmits proof of the person identification to keep access to a web service. The principal challenge of the proposed protocol is to create and then hold the person session adjusting the session timeout on the groundwork of the arrogance that the identity of the user in the method is genuine.

V. CONCLUSION

This paper provides various existing 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. Therefore this paper attempts to provide a comprehensive survey of research on the underlying building blocks required to build a continuous biometric authentication system by choosing bio-metric. Continuous authentication verification with multi-modal biometrics improves security and usability of user session.

REFERENCES

[1]Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, Andrea Bondavalli, Member, IEEE, “Continuous and Transparent User Identity Verification for Secure Internet Services”, IEEE Transactions on Dependable and Secure Computing, Manuscript Id, December 2013.
[2]CASHMA - Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB 2005.
[3]L. Hong, A. Jain, and S. Pankanti, “Can Multi-biometrics Improve Performance?,” Proc. AutoID’99, Summit, NJ, pp. 59–64, 1999.
[4]S. Ojala, J. Keinanen, J. Skytta, “Wearable authentication device for transparent login in nomadic applications environment,” Proc. 2nd International Conference on Signals, Circuits and Systems (SCS 2008), pp. 1-6, 7-9 Nov. 2008.
[5]BioID, “Biometric Authentication as a Service (BaaS), “BioID press release, 3 March 2011, https://www.bioid.com [online].
[6]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, April 2007.
[7]L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, “Quantitative Security Evaluation of a Multi-Biometric Authentication System,” Computer Safety, Reliability and Security, F. Ortmeier and P. Daniel (eds.), Lecture Notes in Computer Science, Springer, vol. 7613, 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 Annual Computer Security Applications Conference (ACSAC '05), pp. 441- 450, 2005. IEEE Computer Society, Washington, DC, USA.
[9] A. Altinok and M. Turk, “Temporal integration for continuous multi-modal biometrics,” Multimodal User Authentication, pp. 11-12, 2003.
[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.