ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Continuous and Clear User Identity Verification for Secure Web Services: A Survey

Poonam Mahale[1], Prof. N. L.Bhale[2]

Student, Dept. of Computer Engineering, MCOERC, Nashik, Savitribai Phule Pune University, Maharashtra, India[1]

Head, Dept. of IT, MCOERC, Nashik, Savitribai Phule Pune University, Maharashtra, India[2]

ABSTRACT: Now a day, 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. This paper explores a secure protocol by applying biometrics for the session management. A proposed system is defined for eternal authentication through continuous or regular user verification. The biometric authentication in this paper will allow users to acquire the credentials clearly/transparently; this means the system does not require the user interaction for the continuous verification. Clear user identity verification is essential for better performance and service usability.

KEYWORDS: Web services, Security, Authentication, Continuous user verification, Biometric authentication.

I. INTRODUCTION

The wide use of web based applications and technologies are increasing day by day. The web based applications are vulnerable to security attacks or threats. This leads to the necessity of safety and security. The security of web based applications is becoming very important and necessary part of this technology world. To achieve this, biometric techniques offer secure and trusted user identity verification. The biometrics is the identification of a person based on his/her behavioural/psychological characteristics. The biometric characteristics are unique for every person. Biometric technique uses the biometric data of a person instead of traditional username and password. 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 [2]. Many of the biometric devices capture and match biometric characteristics in order to produce a proper positive identification. The wide use of biometric security systems gives rise to their misuse, especially in banking and financial sectors.

Traditional user name and password is not sufficient to authenticate the user identity throughout the users working session. Because once the user's identity is verified the system is available to him/her for a whole working session. Due to this permanent identity of user, the above approach is susceptible to attack. Any user can access the system in a middle of the session when the authenticated user leaves the system. A simple solution to 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 [1]. To detect the unwanted misuse of computer resources and to prevent access from unauthorized user, the solution is to provide the biometric continuous user authentication instead of one time authentication. Biometric authentication does not require entering data over and over by the user. It gets user credentials explicitly without notifying the user.

This provides guarantee of more security to to web services computer system than the traditional one [1]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

II. RELATED WORK

In this section, we have studied previous research papers related to the traditional authentication systems. These papers focused only on the single short authentication of the user. The security system methods are described as a strong or weak. It depends on the intensity of the attack. The brief review of previous research papers is as follows:

The first knowledge based identity considered for authentication is password the term password includes single word, phrases or PINs (a personal identification number) that can be closely kept as a secret for user authentication. But the password based authentication schemes are vulnerable to attacks. This is the drawback of this scheme. The passwords can also be guessed by an attacker and each time it is shared for authentication. So, it becomes less secret [3].

The second object based identity for user authentication is token. This can be smart card or bank card [3]. The disadvantage of the token is its inconvenience and cost. The token can be lost stolen. But there is one advantage of physical object i.e. if the token is lost, owner can see evidence of this and can act accordingly [3].

The third ID based identity is biometric data. As it uses user biometric such as fingerprint, face, eye scan, voice print or signature it can provide stronger defence against attacks. The ID documents and biometrics are difficult to copy [3]. Compared to username and password biometrics provide higher level of security [5],[6]. Biometrics is not as easily replaceable as passwords and tokens in case of document lost or biometrics is compromised.

To achieve computer security through biometrics there are four ways:

- Face Biometrics:

  It includes detection and recognition of human faces from a digital image or a video frame from a video source. To do this facial database is used & selected facial features from the image are compared with database. It is normally used in security systems [7], [8]. Detection and recognition includes many complementary parts, each part is complement to one another. Face biometrics is based on learning algorithms to allocate human faces in digital images [2]. It is typically used in security systems.

- Keystroke Biometrics :

  Keystroke biometrics is considered to be an effortless behavioural based method for authenticating users. It employs the person's typing patterns for validating his identity [4]. Keystroke dynamics does not check what you type, but checks how you type.

- Finger Print Scan Biometrics:

  Fingerprint biometrics is one of the most popular and important biometrics. Their uniqueness and consistency over time, they have been used for identification everywhere. It becomes very popular due to its ease in acquisition.

- Voice Biometrics:

  A voice biometric is the numerical modelling which consists of sound, pattern and rhythm of an individual's voice. A voice biometric or voice print is unique to an individual like a finger or palm print. Any Authentication application is required to add voice biometric authentication to the process of authentication and security. Voice verification technology uses the different characteristics of a person's voice to differentiate between speakers. Speech recognition provides input to an application with voice. Speech recognition is the way by which a computer identifies spoken words. Machine or program receives and interprets dictation, or to understand and carry out spoken commands through voice or speech recognition system. Voice biometrics is an interaction tool to a user with the system for registration and verification [9].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Continuous authentication is the process of authenticating the user identity through the complete working session. But a significant problem is that there is a possibility that the user device is used, stolen or forcibly taken by the person even while the authenticated person already logged into a security service.

S. Kumar [11] presents a multi-modal biometric verification system which detects the physical presence of the person logged in a system. Proposed approach lets the user logs in first using a strong authentication procedure and then based on multimodal biometrics a continuous verification process is started. On the failure of verification computer automatically locks up.
Similarly, in [12] a multi-modal biometric verification system is described, which verifies the presence of a user working with a computer continuously. The system reacts by locking the computer on failure of the authentication verification process.

A. Altinok[13] presented a multi-modal biometric continuous authentication system. To provide the local access to high-security systems like ATMs, a multimodal continuous authentication system is essential.

After studying the above mentioned research papers and taking weak points into consideration, the proposed system aims to develop a "Context Aware Security by Hierarchical Multilevel Architectures (CASHMA[10]) Authentication System" and the "Continuous Authentication Protocol. This will improve the security and usability of the user session

III. PROPOSED SYSTEM

The proposed system presents a new approach for verification of user and managing a session which allows secure biometric authentication while using internet. The approach uses "Context Aware Security by Hierarchical Multilevel Architectures (CASHMA [10]) Authentication System" and the "Continuous Authentication Protocol. As per the web service owner's requirement, the CASHMA authentication service can replace the traditional authentication service and can operate securely with any kind of internet/web service. It can also operate with the services having high security needs such as online banking services, and it will be accessible from different client devices, like Smartphone's, Desktop PCs etc. kept at the entrance of secure areas.

The overall view of the CASHMA architecture system is shown in Fig. 1. The system is composed of the three modules: 1) CASHMA authentication service, 2) the clients and 3) the web services (Fig. 1),

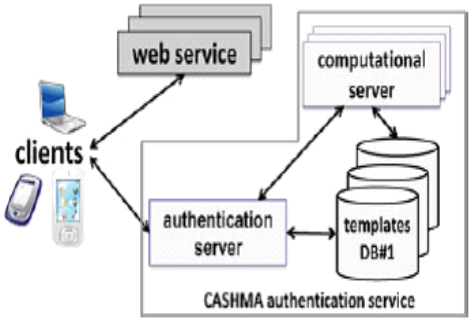

Fig.1. CASHMA Architecture overall View

Communication channels connect these modules. Each communication channel in Fig. 1 implements specific security measures which are not discussed here for brevity.

To setup and maintain a secure session with a client, the continuous authentication protocol is defined which allows providing adaptive session timeouts. The timeout is adapted on the basis the CASHMA authentication systems trust puts in the biometric subsystems and in the user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

This protocol allows clients to continuously and transparently acquires and transmits evidence of the user identity to maintain access to a web service. The main aim of the proposed protocol is to create and 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.

IV. CONCLUSION AND FUTURE WORK

This paper reviews various existing methods used for the continuous user identity verification using different biometrics. Traditional one time username and password verification is inadequate to meet the web security challenge. Therefore, this paper does the comprehensive survey of various research papers to exploit the novel possibility introduced using biometrics for developing the continuous authentication protocol that can improve the security and usability of the user session.

.

REFERENCES

1. Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, PaoloLollini, Angelo Marguglio, Andrea Bondavalli,, "Continuous andtransparent user identityverification for secure internet services", IEEETransactions On Dependable And Secure Computing, December 2013.
2. Omaima N. A. AL-Allaf, "Review of face detection systems basedartificial neural networks algorithms", The International Journal ofMultimedia Its Applications(IJMA) Vol.6, No.1, February 2014.
3. Lawrence O'Gorman, "*Comparing Passwords, Tokens, and Biometrics for User Authentication*", Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040.
4. Arwa Alsultan and Kevin Warwick, "*Keystroke Dynamics Authentication: A Survey of Free-text Methods*", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013.
5. 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.
6. 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
7. 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.
8. 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.
9. Dwijen Rudrapal, Smita Das, S. Debbarma, N. kar, N. Debbarma, "*Voice Recognition and Authentication as a Proficient Biometric Tool and its Application in Online Exam for P.H People*", International Journal of Computer Applications, Volume 39– No.12, February 2012.
10. CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.
11. 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.
12. 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.
13. A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.

BIOGRAPHY

Poonam Mahale is a M.E student in the Computer Engineering Department, MCOERC, Nashik, Savitribai Phule Pune University, Pune. Her research interests are Web security, Information assurance & security, Cyber security, Information Retrieval etc.

.