OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SURVEY ON CONTINUOUS USER IDENTITY VERIFICATION TO AVOID CYBER ATTACK

Mr. Sonu Chaudhary[1], Mr. Vishwas Aware[2], Mr. Anand Hulmani[3], Mr. Md Shadabalam Ansari[4], Prof. Kanchan Wankhade[5]

B.E. Students, Dept. of Computer Engineering, Dhole Patil College of Engineering, Wagholi, Pune, Maharashtra,India[1 2 3 4]

Asst. Professor, Dept. of Computer Engineering, Dhole Patil College of Engg,Wagholi, Pune, Maharashtra,India[5]

Abstract: **In web applications, user authentication is normally based on username and password, come forth biometric solutions allow biometric data during session establishment. But in Unimodal biometric approaches only use a single verification is considered and the identity of the user is permanent during the entire session. A secure protocol is defined for constant authentication through continuous user verification. Biometric techniques suggest solution for secure, trusted and protected authentication. In between the logging session time, the one-time-password (OTP) is send on users registered email id and also randomly one questions will be asked to the user between the 5-10 mints. The user's identity has been verified, the system resources are available for fixed period of time and identity of the user is constant during entire session. The proposed system detects misuses of computer resources and prevents malicious activities based on multi-modal biometric continuous authentication. Biometric and user information's are stored in smart phones and web services**

Keywords: *Authentication, Security, Mobile environments, web servers*

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, Gmail OTP verification and users personal information. 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 with OTP verification, biometric user authentication is typically formulated as a single shot, providing user verification periodically 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, 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, 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 and personal question verification 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.

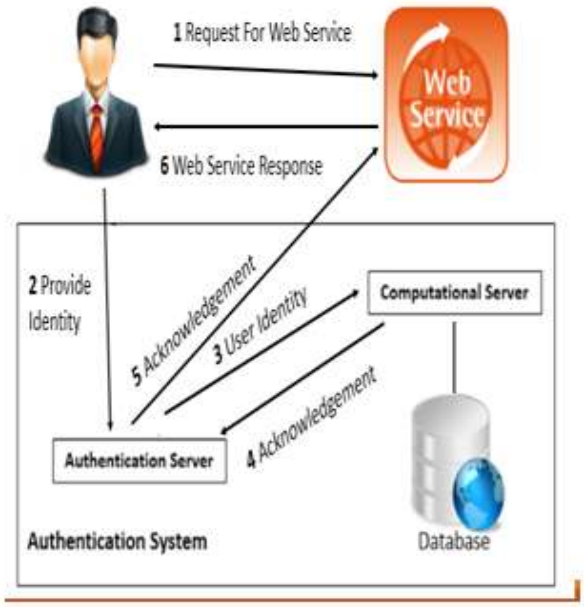

Figure: System Architecture

II RELATED WORK

1. Andrea Ceccarelli, Leonardo Montecchi "Continuous and Transparent User Identity Verification for Secure Internet Services" IEEE TRANSACTIONS MAY/JUNE 2015

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. The protocol determines adaptive timeouts based on the quality, frequency and type of biometric data transparently acquired from the user. The functional behaviour of the protocol is illustrated through Matlab simulations, while model-based quantitative analysis is carried out to assess the ability of the protocol to contrast security attacks exercised by different kinds of attackers.

2. Elizabeth LeMay, Willard Unkenholz, "Adversary-Driven State-Based System Security Evaluation" MetriSec2010 September 15, 2010, Bolzano-Bozen, Italy.

This paper describes the system and adversary characterization data that are collected as input for the executable model. This paper also describes the simulation algorithms for adversary attack behavior and the computation for the probability that an attack attempt is successful. A simple case study illustrates how to analyze system security using the ADVISE method. A tool is currently under development to facilitate automatic model generation and simulation. The ADVISE method aggregates security-relevant information about a system and its adversaries to produce a quantitative security analysis useful for holistic system security decisions.

3. S.kumar, T.sim "Using Continuous Biometric Verification to Protect Interactive Login Sessions", 2012

This paper we describe the theory, architecture, implementation, and performance of a multi-modal passive biometric verification system that continually verifies the presence/participation of a logged-in user. We assume that the user logged in using strong authentication prior to the starting of the continuous verification process. While the implementation described in the paper combines a digital camera-based face verification with a mouse-based fingerprint reader, the architecture is generic enough to accommodate additional biometric devices with different accuracy of classifying a given user from an imposter

4. D.M.Nicol,W.H.Sanders, "Model-Based Evaluation: From Dependability to Security", IEEE TRANSACTIONS 2004

In this work, we survey existing model-based techniques for evaluating system dependability, and summarize How they are now being extended to evaluate system security. We find that many techniques from dependability evaluation can be applied in the security domain, but that significant challenges remain, largely due to fundamental differences between the accidental nature of the faults commonly assumed in depend ability evaluation, and the intentional, human nature of cyber-attacks.

5. T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," IEEE Trans. Apr. 2007.

In this paper we describe a system that continually verifies the presence/participation of a logged-in user. This is done by integrating multimodal passive biometrics in a Bayesian framework that combines both temporal and modality information holistically, rather than sequentially. This allows our system to output the probability that the user is still present even when there is no observation. Our implementation of the continuous verification system is distributed and extensible, so it is easy to plug in additional asynchronous modalities, even when they are remotely generated. Based on real data resulting from our implementation, we find the results to be promising.

III PROPOSED ALGORITHM

Algorithm for Bio- Metric verification

```
for x = 0 to image. Size:
  for y = 0 to image. Size:
  diff += abs (image1.get(x, y).red - image2.get(x, y).red)
  diff += abs (image1.get(x, y).blue - image2.get(x, y).blue)
  diff += abs (image1.get(x, y).green - image2.get(x, y).green)
 end
```

```
end
return ((float)(diff)) / ( x * y * 3)
```

IV Simulation Results

User request to access web service. User needs web service access certificate. Web service checks for user authentication, CASHMA system generate the certificates. CASHMA system accept user information and compute it. CASHMA system validates this user information (i.e. user id, bio-metric verification, answer of questions) from database. Certificates are sends towards the web service.

V Conclusion

In this paper we studied system which provides various existing methods used for continuous authentication using username & password, OTP verification, figure print biometrics, random questions. Initial one time login verification is inadequate to address the risk involved in post logged in session. Therefore this system attempts to provide a comprehensive survey of research on the underlying building blocks required to build a biometric authentication continuous OTP and Random question system by choosing bio-metric. Continuous authentication verification with multi-modal biometrics improves security and usability of user session.

References

1. CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.
2. 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.
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
4. (SCS ’08), pp. 1-6, Nov. 2008.[4] BioID “Biometric Authentication as a Service (BaaS),” BioID Press Release, https://www.bioid.com, Mar. 2011.
5. 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.
6. 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.
7. 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.
8. Altinok and M. Turk, “Temporal Integration for Continuous Multimodal Biometrics,” Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.
9. Roberts, “Biometric Attack Vectors and Defences,” Computers & Security, vol. 26, no. 1, pp. 14-25, 2007.
10. S.Z. Li and A.K. Jain, Encyclopedia of Biometrics. first ed., Springer, 2009.