Securing Internet Services By Using User Identity Verification.

Ms.Patil Poonam Pramod.[1], Prof.Jawalkar Prashant[2]

*[1]Sudent, Department Of Computer Engineering, JSPM'S Bhivrabai Sawant Institute of Technology & Research Wagholi, Pune, Maharashtra, India,**poonamppatil8@gmail.com***

*[2]Asst.Prof, Department Of Computer Engineering, JSPM'S Bhivrabai Sawant Institute of Technology & Research Wagholi, Pune, Maharashtra, India,**prashant.jawalkar@gmail.com***

ABSTRACT

Session management in disseminated Internet services is customarily in light of username and password, explicit logouts and components of user session termination utilizing fantastic timeouts. Developing biometric solution permit substituting username and password with biometric information during session establishment, however in such a methodology still a single verification is considered sufficient, and the identity of a user is viewed as unchanging during the whole session. Also, the length of the session timeout may effect on the convenience of the service and subsequent user fulfillment. This project proposing an alternate method by applying authentication via continuous user verification by applying iris application in the service of sessions. Existing fingerprint authentication can make mistakes with the dryness or dirty of the finger's skin, as well as with the age (is not appropriate with children, because the size of their fingerprint changes quickly). So we proposed iris authentication for Continuous and Transparent User Identity Verification. Iris recognition is a method of biometric identification that uses mathematical pattern-recognition techniques on images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance. A secure protocol is characterized for perpetual authentication through consistent user check. The protocol decides versatile timeouts taking into account the quality, recurrence and kind of biometric information straightforwardly procured from the user.

Keyword : - *Iris,CASHMA,*

1.Introduction

In this technology security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attack s, 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.

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. 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 iris continuous authentication is proposed, that means turning user verification into a continuous process rather than a onetime authentication. Finally, the use of iris 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.

1.1 Problem Definition:

User authentication systems are traditionally based on pairs of username and password and verify the identity of the user only at login phase. No checks are performed during working sessions, which are terminated by an explicit logout or expire after an idle activity period of the user. Emerging biometric solutions provides substituting username and password with biometric data during session establishment, but in such an approach still a single shot verification is less sufficient, and the identity of a user is considered permanent during the entire session. A basic solution is to use very short session timeouts and periodically request the user to input his credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users.

To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an authorized one, solutions based on multi-modal biometric continuous authentication are proposed, turning user verification into a continuous process rather than a onetime occurrence. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple bio-metrics traits. In this project we take iris for biometric authentication. The use of iris authentication allows credentials to be acquired transparently, i.e., without explicitly notifying the user or requiring his/her interaction, which is essential to guarantee better service usability.

1.2 Literature Survey:-

1.Using continuous biometric verification to protect interactive login sessions

In this paper we describe the theory, architecture, implementation, and performance of a multimodal 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. The main thrust of our work is to build a multimodal biometric feedback mechanism into the operating system so that verification failure can automatically lock up the computer within some estimate of the time it takes to subvert the computer. This must be done with low false positives in order to realize a usable system.

2.Continuous Verification Using Multimodal Biometrics

Conventional verification systems, such as those controlling access to a secure room, do not usually require the user to reauthenticate himself for continued access to the protected resource. This may not be sufficient for high-security environments in which the protected resource needs to be continuously monitored for unauthorized use. In such cases, continuous verification is needed. In this paper, we present the theory, architecture, implementation, and performance of a multimodal biometrics verification system that continuously verifies the presence of a logged-in user. Two modalities are currently used - face and fingerprint - but our theory can be readily extended to include more modalities. We show that continuous verification imposes additional requirements on multimodal fusion when compared to conventional verification systems. We also argue that the usual performance metrics of false accept and false reject rates are insufficient yardsticks for continuous verification and propose new metrics against which we benchmark our system.

3.Temporal integration for continuous multimodal biometrics

Typically, biometric systems authenticate the user at a particular moment in time, granting or denying access to resources for the complete session. This model of authentication does not appropriately address environments where a different individual may take over a system from the original user (either willingly or otherwise). We propose a multimodal system that performs authentication continuously by integrating information temporally as well as across modalities. Such continuous authentication provides ongoing (rather than onetime) verification and can easily be coupled with another system for dynamically adjusting access to privileges accordingly. We present an initial approach for temporal integration based on uncertainty propagation over time for estimating channel output distribution from recent history, and classification with uncertainty. Our method operates continuously by computing expected values as a function of time differences.

4.Model-based evaluation: from dependability to security

The development of techniques for quantitative, model-based evaluation of computer system dependability has a long and rich history. A wide array of model-based evaluation techniques is now available, ranging from combinatorial methods, which are useful for quick, rough-cut analyses, to state-based methods, such as Markov reward models, and detailed, discrete-event simulation. The use of quantitative techniques for security evaluation is much less common, and has typically taken the form of formal analysis of small parts of an overall design, or experimental red team-based approaches. Alone, neither of these approaches is fully satisfactory, and we argue that there is much to be gained through the development of a sound model-based methodology for quantifying the security one can expect from a particular design. 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 dependability evaluation, and the intentional, human nature of cyber attacks.

2. SYSTEM ARCHITECTURE

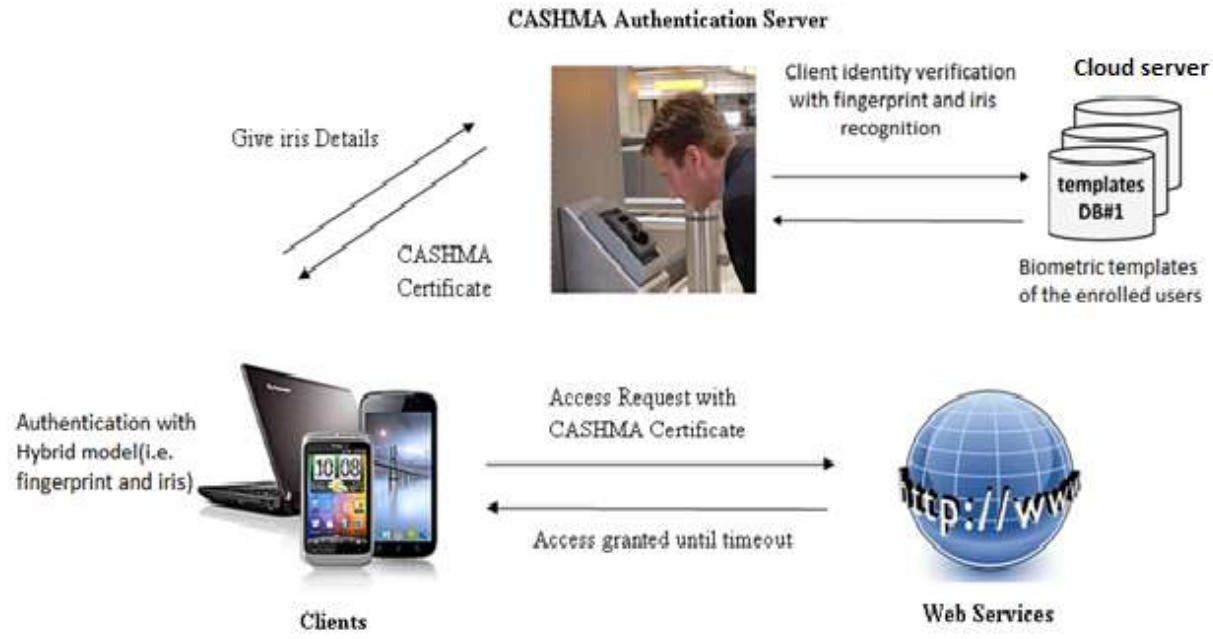

Fig-1: System Arch.

3. Algorithm Used in Proposed System:

Continuous Iris Authentication Protocol

Input: Iris

Output: Continuous Authentication

Initial Phase:

Step 1: Client send Iris to CASHMA Authentication Server.

Step 2: CASHMA Authentication Server verify Client Identity then send CASHMA Certificate to client.

Step 3: Client send access request with CASHMA Certificate to Web service.

Step 4: Web service accept the access request. So Client access web until "timeout".

Maintenance Phase:

Step 5: Client send Iris to CASHMA Authentication Server.

Step 6: CASHMA Authentication Server verify the Client Identity then send a fresh CASHMA Certificate to client.

Step 7: Now Client send CASHMA Certificate to Web service for update the session timeout.

4. CONCLUSIONS

The existing initial one time login verification is inadequate to address the risk involved in post logged in session. Therefore this project attempts to provide a continuous iris authentication system. Continuous multi-modal iris authentication verification with improves security and usability of user session.

5. ACKNOWLEDGEMENT

This is a great pleasure & immense satisfaction to express my deepest sense of gratitude & thanks to everyone who has directly or indirectly helped me in completing my project work successfully. I express my gratitude towards project guide Prof… and Head of Department of Computer Engineering Dr. G. M. Bhandari, P.G. coordinator Dr. A. C. Lomte, Bhivarabai Sawant Institute Of Technology and Research College Of Engineering, Pune who guided & encouraged me in completing the project work in scheduled time. I would like to thanks our Principal Dr. T.K.Nagaraj for allowing us to pursue my project in this institute.

6. 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] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics," Proc. Workshop Multimodal User Authenti-cation, pp. 11-12, 2003.

[4] D.M. Nicol, W.H. Sanders, and K.S. Trivedi, "Model-Based Evalu-ation: From Dependability to Security," IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, Jan.-Mar. 2004.

[5] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing, "Automated Generation and Analysis of Attack Graphs," Proc. IEEE Symp. Security and Privacy, pp. 273-284, 2002.

[6] E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, and W.H. Sanders, "Adversary-Driven State-Based System Security Evaluation," Proc. the Sixth Int'l Workshop Security Measurements and Metrics (MetriSec '10), pp. 5:1-5:9, 2010.

[7] S. Ojala, J. Keinanen, and J. Skytta, "Wearable authentication device for transparent login in nomadic applications environment, " Proc. Seco nd Int'l Conf. Signals, Circuits and Systems (SCS '08), pp. 1-6, Nov. 2008.

[8] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, "Quantitative Security Evaluation of a Multi-Biometric Authenti-cation System," Proc. Int'l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.