IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Multi-Level Security for Internet Banking Services

V.L. Sowjanya[1], Mrs. K. Santosh Jhansi[2]

PG Scholar, Department of CSE, MVGR College of Engineering, Vizianagaram, India [1]

Assistant Professor, Department of CSE, MVGR College of Engineering, Vizianagaram, India [2]

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 conveince of the service and subsequent user fulfilment. This paper proposing an alternate method by applying authentication via multi-level user verification by applying biometrics an application in the service of sessions.

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 biometric continuous authentication are proposed, that means turning user verification into a continuous process rather than a onetime authentication. In this way it applies multi-level verification Biometrics authentication can depend on multiple biometrics traits. SECURE user authentication is fundamental in most in most of modern ICT systems. To avoid that a single biometric trait is forged, biometrics authentication can rely on multiple biometrics traits .new approach for users verification and session management are discussed in this paper that is defined and implemented in the context of the multi-modal biometric authentication system CASHMA-(Context Aware Security by Hierarchical Multilevel Architecture). The CASHMA system realizes a secure biometric authentication service on the Internet, in this users need to remember only one username and use their biometric data rather than passwords to authenticate in multiple web services. CASHMA operate securely with any kind of web service for example online banking, military zones.

II. LITERATURE SURVEY

1) Quantitative Security Evaluation of a Multi-Biometric Authentication System

AUTHORS: L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina,

Biometric authentication systems verify the identity of users by relying on their distinctive traits, like fingerprint, face, iris, signature, voice, etc. Biometrics is commonly apparent as a strong authentication method; in tradition a number of familiar vulnerabilities exist, and protection aspects must be cautiously measured, particularly when it is adopted to safe the access to applications controlling essential systems and infrastructures. In this paper we perform a quantitative

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

security evolution of the CASHMA multi-biometric verification system, assessing the security provided by different system configurations against attackers with different capabilities. The analysis is performed using the ADVISE modeling formalism, a formalism for security evaluation that extends attack graphs; it allows to combine information on the system, the attacker, and the metrics of interest to produce quantitative results. The obtained results provide useful insight on the security offered by the different system configurations, and demonstrate the feasibility of the approach to model security threats and countermeasures in real scenarios.

2) Model-based evaluation of scalability and security tradeoffs: A case study on a multi-service platform
AUTHORS: L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and A. Bondavalli
Current ICT infrastructures are characterized by increasing requirements of reliability, security, performance, availability, adaptability. A relevant issue is represented by the scalability of the system with respect to the increasing number of users and applications, thus requiring a careful dimensioning of resources. Furthermore, new security issues to be faced arise from exposing applications and data to the Internet, thus requiring an attentive analysis of potential threats and the identification of stronger security mechanisms to be implemented, which may produce a negative impact on system performance and scalability properties. The paper presents a model-based evaluation of scalability and security tradeoffs of a multi-service web-based platform, by evaluating how the introduction of security mechanisms may lead to a degradation of performance properties. The evaluation focuses on the OPENNESS platform, a web-based platform providing different kind of services, to different categories of users. The evaluation aims at identifying the bottlenecks of the system, under different configurations, and assess the impact of security countermeasures which were identified by a thorough threat analysis activity previously carried out on the target system. The modeling activity has been carried out using the Stochastic Activity Networks (SANs) formalism, making full use of its characteristics of modularity and reusability. The analysis model is realized through the composition of a set of predefined template models, which facilitates the construction of the overall system model, and the evaluation of different configuration by composing them in different ways.

3) "Continuous Verification Using Multimodal Biometrics"
AUTHORS: . T. Sim, S. Zhang, R. Janakiraman, and S. Kumar.
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.

4) Attacks on Biometric Systems: A Case Study in Fingerprints
AUTHORS: U. Uludag and A.K. Jain
In spite of numerous advantages of biometrics-based personal authentication systems over traditional security systems based on token or knowledge, they are vulnerable to attacks that can decrease their security considerably. In this paper, we analyze these attacks in the realm of a fingerprint biometric system. We propose an attack system that uses a hill climbing procedure to synthesize the target minutia templates and evaluate its feasibility with extensive experimental results conducted on a large fingerprint database. Several measures that can be utilized to decrease the probability of such attacks and their ramifications are also presented.

III. RELATED WORK

3.1 Existing System:

- Once the client's personality has been affirmed, the framework assets are accessible for a settled time frame or until express logout from the client. This approach accept that a solitary confirmation (toward the start of the session) is adequate, and that the personality of the client is constant amid the entire session.
- In existing, a multi-modular bio-metric check framework is composed and created to identify the physical presence of the client signed in a PC.
- The work in another current paper, proposes a multi-modular bio-metric ceaseless validation answer for neighbourhood access to high-security frameworks as ATMs, where the crude information procured are weighted in the client confirmation handle, in view of i) kind of the bio-metric attributes and ii) time, since various sensors can give crude information diverse timings. Point ii) presents the need of a fleeting combination technique which relies on upon the accessibility of past perceptions: in view of the presumption that over the long haul, the trust in the obtained (maturing) values diminishes. The paper applies a decadence capacity that measures the vulnerability of the score registered by the check work.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Disadvantages of Existing System:

- None of existing approaches supports continuous authentication.
- Emerging biometric solutions allow replacing username and password with biometric data during session establishment, but in such an approach still a single verification is deemed sufficient, and the identity of a user is considered constant during the complete session.

3.2 Proposed System:

- This paper displays another approach for client check and session administration that is connected in the setting mindful security by progressive multilevel models (CASHMA) framework for secure biometric confirmation on the Internet.
- CASHMA can work safely with any sort of web administration, incorporating administrations with high security requests as web based managing an account administrations, and it is expected to be utilized from various customer gadgets, e.g., advanced mobile phones, Desktop PCs or even biometric stands put at the passageway of secure territories. Contingent upon the inclinations and prerequisites of the proprietor of the web benefit, the CASHMA validation administration can supplement a conventional verification benefit, or can supplant it.
- Our nonstop validation approach is grounded on straightforward obtaining of biometric information and on versatile timeout administration on the premise of the trust postured in the client and in the diverse subsystems utilized for confirmation. The client session is open and protected regardless of conceivable sit out of gear action of the client, while probable abuses are identified by consistently affirming the nearness of the correct client.

Advantages of Proposed System:

- Our approach does not require that the reaction to a user verification mismatch is executed by the user device (e.g., the logout procedure), but it is transparently handled by the CASHMA confirmation benefit and the web services, which apply their own reaction procedures
- Provides a trade off between usability and security.

III. THE SYSTEM ARCHITECTURE

CASHMA means Context-Aware Security by Hierarchical Multilevel Architectures. This system is used for secure biometric authentication on the internet. CASHMA is able to operate securely with any kind of web service, including services with high security demands as online banking services. Depending on Preferences and requirements of the owner of the web service the CASHMA authentication service replace the traditional authentication service. The system architecture is consisting of the CASHMA authentication service, the clients and the web services and they are connected through communication channels. Fig. 1 describes the continuous authentication system to a web service. The authentication server, which interacts with the clients, computational servers that perform comparisons of biometric data for verification of the users, and databases of templates contains the biometric templates of the users (that are required for user authentication or verification purpose). The web service demands the authentication of users to the CASHMA authentication server. These services are any kind of Internet service. Finally, by clients we mean the users' devices like (laptops, Desktop PCs, tablets, etc.) which acquire the biometric data corresponding to the various biometric traits from the users, and transmit those data to the CASHMA authentication server towards a target web service. A client contains. i) Sensors - acquire the raw data, ii) the CASHMA application - transmits the raw data to the authentication server. The CASHMA authentication server applies user authentication and verification procedures that compare the raw data with the biometric templates stored.

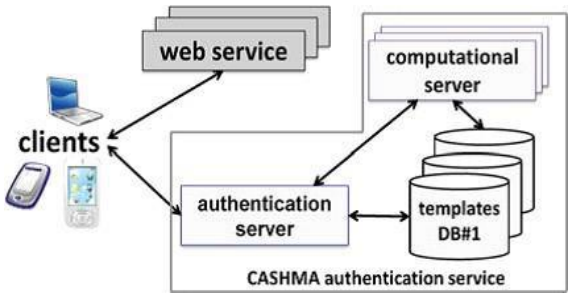

Figure 1: System Architecture

Consider online banking where a user wants to log into an online banking service using a smart phone. Here user and web services must be enrolled to CASHMA authentication service and user must be installed CASHMA application on his smart phone. The smart phone contacts the online banking service, which replies requesting the client to contact the

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

CASHMA authentication server and get an authentication certificate. Using the CASHMA application, the smart phone sends its unique identifier and biometric data to the authentication server for verification. The authentication server verifies the user identity, and grants the access if: i) it is enrolled in the CASHMA authentication service, ii) it has rights to access the online banking service and, iii) the acquired biometric data match those stored in the templates database associated to the provided identifier. In case of successful user verification, the CASHMA authentication server releases an authentication certificate to the client, proving its identity to third parties, and includes a timeout that sets the maximum duration of the user session. The client presents this certificate to the web service, which verifies it and grants access to the client. The CASHMA application operates to continuously maintain the session open: it transparently acquires biometric data from the user, and sends them to the CASHMA authentication server to get a new certificate. Such certificate, which includes a new timeout, is forwarded to the web service to further extend the user session.

IV. CONCLUSION

We exploited the novel possibility introduced by biometrics to define security for continuous authentication that improves security and usability of user session. It computes adaptive time outs on basis of trust posed in user activity. Some architectural design decisions of CHASMA are here discussed. First, the system exchanges raw data and not the features extracted from them. While crypto-token approaches are not considered. This is due to architectural decisions where the client is kept very simple. This paper explores multi-level user verification in order to provide more security for internet banking services.

REFERENCES

[1] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.
[2] 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.
[3] 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.
[4] D.M. Nicol, W.H. Sanders, and K.S. Trivedi, “Model-Based Evaluation: From Dependability to Security,” IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, Jan.-Mar. 2004.
[5] 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.
[6] A. Ceccarelli, A. Bondavalli, F. Brancati, and E. La Mattina, “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.