ISSN(Online): 2395-7638

International Journal of Recent Research in Science, Engineering and Technology

Vol. 6, Issue 8, August 2020

Face Session Timeout Internet Secure Services

Shamil Ahmed

Assistant Professor, Department of CSE, Vels University, Chennai, Tamil Nadu, India.

ABSTRACT: Session management in distributed internet services is traditionally based on username and password .This paper explores promising alternatives offered by biometrics for the management of session.

KEYWORDS: **SECURITY, WEB SERVERS, AUTHENTICATION.**

I. INTRODUCTION

When a user connects to your application you can force them to provide logon credentials. If the user successfully authenticates they wouldn't expect to provide these credentials again unless the logon times out or they are executing a privileged action. Session management allows your application to only require the users to authenticate once and also confirm that the user executing a given action is the user who provided the original credentials. Attacks against sessions are often focused on obtaining a valid session value through either exploiting your users or taking advantage of weaknesses in the session management functionality. The main objective of this project to explores promising alternatives offered by applying biometrics in the management of sessions. To provide secure session management in the internet services and better user performance. 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. Security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber attacks. There is no advance use of biometric authentication in the traditional authentication process. No continuous and transparent authentication services is provided in the before version system.

II. RELATED WORK

This paper presents a new approach for user verification and session management that is applied in the Context Aware Security by Hierarchical Multilevel Architectures system for secure biometric authentication on the internet. Context Aware Security by Hierarchical Multilevel Architectures is able to operate securely with any kind of web service, including services with high security demands as online banking services.

It is intended to be used from different client devices. The work in proposes a biometric continuous authentication solution for local access to high-security systems as ATMs.By using this approach we can guarantee better service usability. Continuous authentication is used to detect misuse of computer resources and prevent that an unauthorized user maliciously replaces authorized one.

ISSN(Online): 2395-7638

International Journal of Recent Research in Science, Engineering and Technology

Vol. 6, Issue 8, August 2020

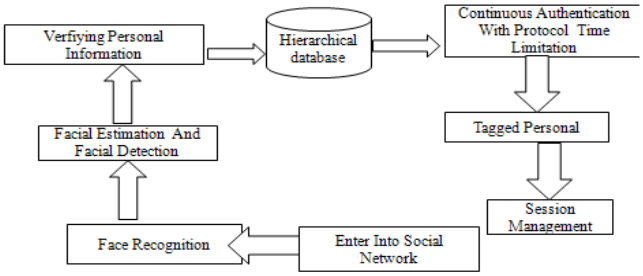

FIG 1: OVERVIEW OF ARCHITECTURE

III. PROPOSED WORK

A new approach for user verification and session management.A new technique applied in this approach is Context Aware Security by Hierarchical Multilevel system.Used for secure authentication on the internet.Context Aware Security by Hierarchical Multilevel is secured with any kind of web service.It is intended to be used from different client devices .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 onetimeverification and can easily be coupled with another system for dynamically adjusting access to privileges accordingly.

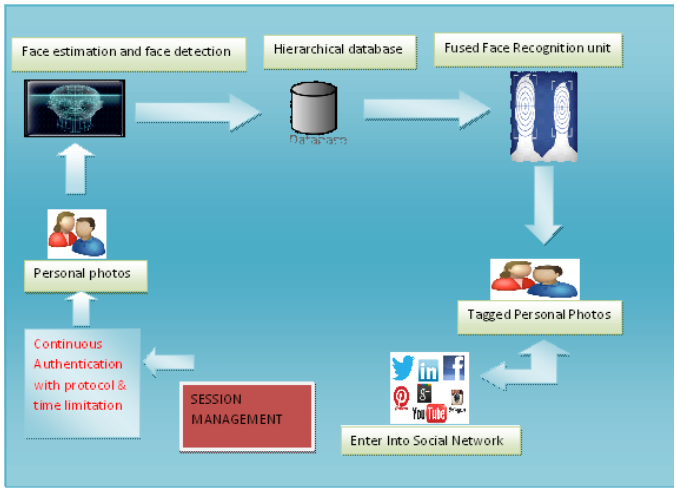

FIG 2: SYSTEM ARCHITECTURE

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. Our preliminary experiments show that temporal information improves authentication accuracy.

These empirical results are promising and justify further investigation. An integral part of modeling the global view of network security is constructing attack graphs. In practice, attack graphs are produced manually by Red Teams.

ISSN(Online): 2395-7638

International Journal of Recent Research in Science, Engineering and Technology

Vol. 6, Issue 8, August 2020

Construction by hand however is tedious, error prone, and impractical for attack graphs larger than a hundred nodes. In this paper we present an automated technique for generating and analyzing attack graphs. We base our technique on symbolic model checking algorithms, letting us construct attack graphs automatically and efficiently. We also describe two analyses to help decide which attacks would be most cost effective to guard against. We implemented our technique in a tool suite and tested it on a small network example, which includes models of a firewall and an intrusion detection system. While the implementation described in the paper combines 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.

IV. QUANTITATIVE SECURITY EVALUATION

Security assessment relied for several years on qualitative analyses only. Leaving aside experimental evaluation and data analysis model-based quantitative security assessment is still far from being an established technique despite being an active research area. Specific formalisms for security evaluation have been introduced in literature, enabling to some extent the quantification of security. Attack trees are closely related to fault trees: they consider a security breach as a system failure, and describe sets of events that can lead to system failure in a combinatorial way they however do not consider the notion of time.

V. CONCLUSION

We exploited the novel possibility introduced by biometrics to define a protocol for continuous authentication that improves security and usability of user session. The protocol computes adaptive timeouts on the basis of the trust posed in the user activity and in the quality and kind of biometric data acquired transparently through monitoring in background the user's actions. We remark that our proposed protocol works with no changes using features, templates or raw data. Second, privacy concerns should be addressed considering National legislations.

At present, our prototype only performs some checks on face recognition, where only one face (the biggest one rusting from the face detection phase directly on the client device) is considered for identity verification and the others deleted. Third, when data is acquired in an uncontrolled environment, the quality of biometric data could strongly depend on the surroundings. While performing a client-side quality analysis of the data acquired would be a reasonable approach to reduce computational burden on the server, and it is compatible with our objective of designing a protocol independent from quality ratings of images.

VI. REFERENCES

[1] Context Aware Security by Hierarchical MultilevelArchitectures, 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 (SCS '08), pp. 1-6, Nov. 2008.
[4] BioID "Biometric Authentication as a Service (BaaS),"BioIDPressRelease, Mar. 2011.
[5] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "ContinuousVerification Using Multimodal Biometrics," IEEE Trans. PatternAnalysis and Machine Intelligence, vol. 29, no. 4, pp. 687-700, Apr.2007.