MULTILEVEL AUTHENTICATION SCHEME FOR DATA SECURITY IN TRANSPARENT COMPUTING

S.Chandrasekaran[1] | J.Jayaraj[2] | B.Arun[3]

[1](Dept of CSE, UG Scholar, Anand Institute of Higher Technology, Chennai, India, Chandrasekar007don@gmail.com)
[2](Dept of CSE, UG Scholar, Anand Institute of Higher Technology, Chennai, India, jayaraj97@gmail.com)
[3](Department of CSE, UG Scholar, Anand Institute of Higher Technology, Chennai, India, arunthamizh96@gmail.com)

***Abstract*—*The Multilevel Authentication Scheme in Transparent Computing can protect user data by providing different security levels, while offering multilevel access control and valid identity authentication. In this project, for the reason of secured security. We provide multilevel access (traditionally and biometrically) solutions for the user account. 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.*

1. INTRODUCTION

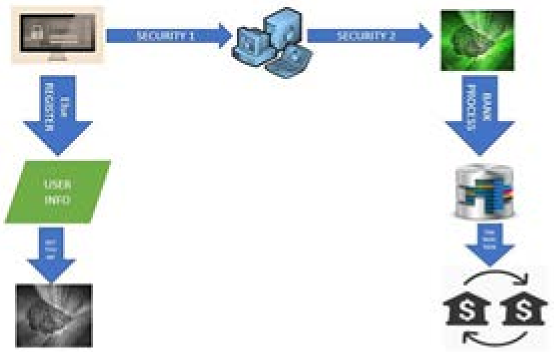
Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system. If you don't take basic steps to protect your work computer, you put it and all the information on it at risk. You can potentially compromise the operation of other computers on your organization's network, or even the functioning of the network as a whole. Technical measures like login passwords, anti-virus are essential. (More about those below) However, a secure physical space is the first and more important line of defense.

2. EXISTING SYSTEM

In an existing system username password verifications are used for authentication process. The identification of the user is constant during the whole sessions that time the cyber-attack is obtained. Reauthentication is the traditional process to identify user and cannot identify where user is an ongoing process. None of existing approaches supports continuous authentication. In this approach still a single verification is deemed sufficient, and the identity of a user is considered immutable during the entire session.

3. PROPOSED SYSTEM

In proposed system instead of username password and single biometric verifications. The proposed system provide continuous authentication process by using fingerprint scan biometrics. Continuous authentication – It detect the physical presence of the user logged in the computer. It provide two tier support for the protection. This username password and single biometric verifications technique supports intransitive authentication.



4. WORKING PRINCIPLE

1. System Model
2. Authentication Server
3. CASHMA Certificate
4. Continuous Authentication

A. *System Model*

In this module, we create the System model to evaluate and implement our proposed system. CASHMA can authenticate to web services, ranging from services with strict security requirements as online banking services to services with reduced security requirements as forums or social networks. Additionally, it can grant access to physical secure areas as a restricted zone in an airport, or a military zone (in such cases the authentication system can be supported by biometric kiosk placed at the entrance of the secure area). We explain the usage of the CASHMA authentication service by discussing the sample application scenario, where a user u wants to log into an online banking service. "User Id" refers to the identity of the user obtained from the Bank for the purpose of logging into the Internet Banking facility provided by the Bank. "Login Password" is a unique and randomly generated password known only to the customer, which can be changed by the user to his/her convenience. This is a means of authenticating the user ID for logging into Internet Banking. "Transaction Password" is a unique and randomly generated password known only to the customer, which can be changed to his/her convenience. This is a means of authentication required to be provided by the customer for putting through the transaction in his/her/their/its accounts with Bank through Internet Banking. While User ID and Password are for valid access into the internet application, giving valid Transaction Password is for authentication of transaction requests made through internet.

B. Authentication Server

In Internet banking as with traditional banking methods, security is a primary concern. Server will take every precaution necessary to be sure your information is transmitted safely and securely. The latest methods in Internet banking system security are used to increase and monitor the integrity and security of the system.

The Server maintains the functionality:

- Customer Details
- Activation of Beneficiary
- Transaction Details
- Activate Blocked Account

C. CASHMA Certificate

In this module, we present the information contained in the body of the CASHMA certificate transmitted to the client by the CASHMA authentication server, necessary to understand details of the protocol. Time stamp and sequence number univocally identify each certificate, and protect from replay attacks. ID is the user ID, e.g., a number. Decision represents the outcome of the verification procedure carried out on the server side. It includes the expiration time of the session, dynamically assigned by the CASHMA authentication server. In fact, the global trust level and the session timeout are always computed considering the time instant in which the CASHMA application acquires the biometric data, to avoid potential problems related to unknown delays in communication and computation.

D. Continuous Authentication

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 use of biometric 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.

The idea behind the execution of the protocol is that the client continuously and transparently acquires and transmits evidence of the user identity to maintain access to a web service. The main task of the proposed protocol is to create and then 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.

5. 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. Some architectural design decisions of CASHMA are here discussed. First, the system exchanges raw data and not the features extracted from them or templates, while crypto-token approaches are not considered; as debated, this is due to architectural decisions where the client is kept very simple. 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.

6. FUTURE ENHANCEMENT

At present, our prototype only performs some biometric check and face recognition system for online credit card cancellation, where only one biometric system is used. In future, we can add additional eye iris scanning and face recognition for account access. It creates more security for accessing the account. Level of authenticity must be keep on increasing as number of thefts can be minimized as much as possible.

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. AutoID’99, Summit, NJ, pp. 59–64, 1999.

[3] 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.

[4] BioID, ”Biometric Authentication as a Service (BaaS), “BioID press release, 3 March 2011, https://www.bioid.com [online].

[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, April 2007.

[6] 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.

[7] L. Montecchi, P. Lollini, A. Bondavalli, and La Mattina, “Quantitative Security Evaluation of a Multi-Biometric Authentication System,” Proc. Int’l Conf. Computer Safety, Reliability and Security, pp. 209-221, 2012.

[8] 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.

[9] A. Altinok and M. Turk, “Temporal Integration for Continuous Multimodal Biometrics,” Proc. Workshop Multimodal User Authentication, pp. 11-12, 2003.

[10] C. Roberts, “Biometric Attack Vectors and Defences,” Computers & Security, vol. 26, no. 1, pp. 14-25, 2007.

[11] S.Z. Li and A.K. Jain, Encyclopedia of Biometrics. first ed., Springer, 2009.