International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Authentication of User Identity Using Cashma

1.BARIGALA SWARAVEENA, 2.Dr .THANVEER JAHAN, 3.V.Janaki

, 1.PG Scholar, Department of CSE ,Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana Mail id:swaraveenabarigala@gmail.com

2.Associate Professor Department of CSE, Vaagedevi College of Engineering, Bollikunta, Warangal, Telangana Mail id : thanvijahan@gmail.com

3. Professor,HOD Depertment of CSE, Vaagedevi College of Engineering, Bollikunta, Warangal,Telangana

ABSTRACT

Session management in distributed Internet services is traditionally based on username and password, explicit logoffs, and user session expiration mechanisms that use typical timeouts. Emerging biometric solutions can replace the username and password with biometric data when establishing the session, but only one check is considered sufficient and the identity of a user is considered immutable for a period of time. the whole session. In addition, the length of the session timeout can affect service usability and customer satisfaction. This article explores promising alternatives offered by the application of biometrics in session management. A secure protocol is defined for perpetual authentication through continuous verification of the user. The protocol determines adaptive latency based on the quality, frequency and type of biometric data acquired transparently by the user. The functional behavior of the protocol is illustrated by Matlab simulations, while model-based quantitative analysis is performed to evaluate the protocol's ability to counter security attacks by different types of attackers. Finally, the current prototype for Android PCs and smartphones is discussed. Keywords - Security, Web servers, mobile environments, authentication.

I. INTRODUCTION

In almost every aspect of human life, computer devices (such as computers, smartphones, tablets, or smart watches) become important gadgets. Communications, aviation and financial services are highly controlled by computer systems. People entrust vital information such as medical and court records, handle transactions, pay bills and private documents. However, this growing reliance on computer systems, combined with the growing importance of global accessibility

in cyberspace, has revealed new threats to the security of the computer system. In addition, crimes and impostors in cyberspace are almost everywhere. For most existing computer systems, once the user's identity is verified on login, system resources are available to that user until they exit the system or lock the session. In fact, system resources are available to any user during this time. This may be appropriate for low-security environments, but may lead to session hijacking, in which an attacker targets an open session, e.g. when people leave the computer unattended for longer or shorter periods of time, for example to take a cup of coffee, talk to a colleague, or simply because they are not used to locking a computer because of the inconvenience. In high-risk environments or where the cost of unauthorized use of a computer is high, continuous verification of the user's identity is extremely important. By using continuous verification, the identity of the human who exploits the computer is continually verified. The username and password of the traditional authentication system are replaced by a biometric feature in the case of a biometric technique. Biometrics is the science and technology of determining and identifying the correct user identity based on physiological and behavioral traits that include facial recognition, retinal scans, voice recognition of fingerprints and dynamics of the strikes. The biometric authentication of the user is formulated as a single hit check. Single hit verification provides user verification only at login time. If the identity of the user is verified once, then the system resources are available to the user for a fixed period of time and the user's identity is permanent for the entire session. A basic solution is to use very short session timeouts and periodically ask the user to enter their credentials again and again. To detect misuse of computer resources in a timely manner and prevent an unauthorized user from replacing an unauthorized user, solutions based on multimodal continuous biomimetric authentication are proposed, transforming the user's verification into a continuous process over time. place of a single occurrence. To prevent a single biometric trait from being falsified, biometric authentication can rely on several biometric features. A new approach for user verification and session management is discussed in this article which is defined and implemented in the context of the CASHMA multi-modular biometric authentication system (Multi-level hierarchical architecture contextual security). The CASHMA system

provides a secure biometric authentication service on the Internet, in which users must remember a single username and use their biometric data rather than passwords to authenticate in multiple web services. CASHMA operate securely with any type of web service, for example online banking, military zones and the airport area that require high security services.

II. THE CASHMA ARCHITECTURE

CASHMA stands for Context-Aware security by multi-level hierarchical architectures. This system is used for secure biometric authentication on the Internet. CASHMA is able to operate securely with any type of web service, including services with high security requirements as an online banking service. Depending on the preferences and requirements of the Web service owner, the CASHMA Authentication Service replaces the traditional authentication service. International Journal of Technical Research and

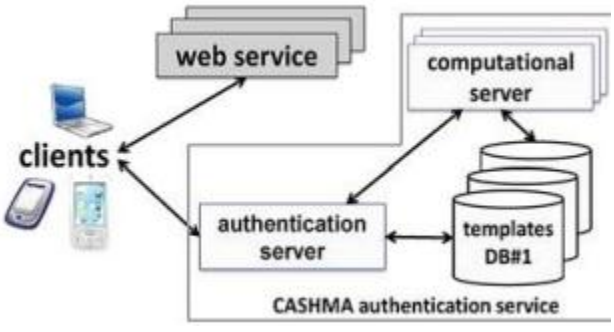

Fig.1. overall view of the CASHMA architecture

The system architecture is composed of the CASHMA authentication service, clients and Web services, and they are connected via communication channels. Figure 1 describes the continuous authentication system to a Web service. The authentication server, which interacts with the clients, the calculation servers that perform biometric data comparisons for the user verification, and the model databases contain the biometric templates of the users (required for authentication of the user or verification). The Web service requires user authentication to the CASHMA authentication server. These services are any type of Internet service. Finally, by customer, we mean the devices of the users (laptops, desktop PCs, tablets, etc.) that acquire the biometric data corresponding to the different biometric traits of the users, and transmit this data to the CASHMA authentication server to a site target. a service. A client contains.

i) Sensors - acquire raw data,

ii) the CASHMA application - transmits the raw data to the authentication server. The CASHMA authentication server enforces authentication and user verification

procedures that compare raw data with stored biometric templates. Consider online banking when a user wants to connect to an online banking service using a smartphone. Here, the user and web services must be registered with the CASHMA authentication service and the user must be installed on the CASHMA application of their smartphone. The smartphone contacts the online banking service, which responds by asking the customer to contact the CASHMA authentication server and obtain an authentication certificate. Using the CASHMA application, the smartphone sends its unique identifier and biometric data to the authentication server for verification. The authentication server verifies the identity of the user and grants access if: i) it is registered with the CASHMA authentication service, ii) it has the right to access the online banking service and iii) the acquired biometric data correspond to those stored in the database models associated with the provided identifier. In the event of a successful user verification, the CASHMA authentication server releases an authentication certificate from the client, proving its identity to third parties and includes a timeout defining the maximum duration of the user's session. . The client presents this certificate to the web service, which verifies it and grants access to the client. The CASHMA application makes it possible to keep the session open at all times: it acquires the user's biometric data transparently and sends them to the CASHMA authentication server to obtain a new certificate. This certificate, which includes a new delay, is passed to the web service to further expand the user session. Fig2. Online banking using CASHMA

III. THE CASHMA CERTIFICATE

The information contained in the body of the CASHMA certificate transmitted to the user by using the CASHMA authentication server, imperative to recognize important points of the protocol. The CASHMA certificates consist of Time stamp and sequence number univocally identify each certificate, and it look after from replay attacks. Id is the person id, e.g., a number. Choice represents the final result of the verification process carried out on the server side. It includes the expiration time of the session, dynamically assigned by the CASHMA authentication server. Typically ,the global trust stage and the session timeout are at all times computed by way of considering the time immediate in which the CASHMA application acquires the biometric data, to restrict potential issues

concerning unknown delays in conversation and computation. Due to the fact such delays will not be predicable in prior, simply supplying a relative timeout value to the user will not be viable, so the CASHMA server thus provides the absolute immediate of time at which the session must expire. The CASHMA certificates will probably be expired when the expiration timeout attain zero.

IV. THE CONTINUOUS AUTHENTICATION PROTOCOL

The continuous authentication protocol provides adaptive session times to a web service to establish and maintain a secure session with a client. The waiting time is adapted according to the confidence that the CASHMA authentication system places in the biometric subsystems and in the user. The execution of the protocol is composed of two consecutive phases: the initial phase and the maintenance phase. The initial phase is to authenticate the user in the system and establish the session with the web service. During the maintenance phase, the session timeout is adaptively updated when the user's identity verification is performed using new raw data provided by the client to the server. CASHMA authentication. The user (the client) contacts the web service for a service request; the Web service responds that a valid CASHMA authentication service certificate is required for authentication

CONCLUSION

The session management system is based entirely on the user name and password, and the sessions are terminated by explicit disconnections or expiration of session timeouts. Methods used for continuous authentication using different biometrics. The initial single login verification is inadequate to handle the risk associated with a post-connected session. We exploited the new opportunity introduced by biometrics to define a continuous authentication protocol that improves the security and usability of the user's session. The protocol calculates adaptive timeouts based on trust placed in the user's activity and the quality and type of biometric data acquired transparently by monitoring the user's actions in the background. . Continuous authentication verification with multi-modal biometrics improves the security and usability of the user's session. The functions proposed for the evaluation of the waiting time of the session are selected from a very large set of possible alternatives.

REFERENCES

[1] CASHMA-Context Aware Security by Hierarchical Multilevel Architectures, MIUR FIRB, 2005.

[2] Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, Andrea Bondavalli ”Continuous and Transparent User Identity Verification for Secure Internet Services” IEEE Transaction on De-pendable and Secure Computing, VOL. 12,NO. 3,JUNE 2015

[3] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, Arun Ross, James L. Wayman, ”Biometrics: A Grand Challenge” International Conference on Pattern Recognition , Aug 2004. [4] 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.

[5] T.F. Dapp, “Growing Need for Security in Online Banking: Biometrics Enjoy Remarkable Degree of Acceptance,,” Banking & Technology Snapshot, DB Research, Feb. 2012.

[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.

[7] 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.

AUTHOR’S PROFILE:

Barigala Swaraveena, PG Scholar, Department of CSE ,Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana Mail id:swaraveenabarigala@gmail.com

Dr.THANVEER JAHAN Associate Professor Department of CSE, Vaagedevi College of Engineering, Bollikunta, Warangal, Telangana Mail id : thanvijahan@gmail.com