Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Continues and Transparent User Identity Verification for Secure Internet Services

Ch.Ramesh Kumar
Associate Professor & HOD,
Department of CSE,
Malla Reddy Engineering College
& Management Sciences, Kistapur,
Medchal, Hyderabad.

Y.Ashwini
Assistant Professor,
Department of CSE,
Malla Reddy Engineering College
& Management Sciences, Kistapur,
Medchal, Hyderabad.

Santhosh Kumar Khajapu
M.Tech Student,
Department of CSE,
Malla Reddy Engineering College
& Management Sciences, Kistapur,
Medchal, Hyderabad.

Abstract:

In the field of internet services secure internet services is important issue. Traditional distributed internet services are based on session management of username password, logouts and user session expiration based on timeouts. Biometric authentication provides solution to substitute password with biometric information in session creation with single verification. In proposed work, additional level of security can be provided & multiple verification can deployed for authentication. In this paper we present continuous authentication of user by multiple authentication. The user identity is continuously verified by applying different authentication in session management. A secure data flow with privacy preservation for the session management by using biometric systems will be offered. This paper described a technique used to secure raw data along with dummy bit insertion in hash code & for less memory utilization. The use of biometric allows identity to be obtained clearly. The result we have obtained based on real data from this research is satisfactory.

Keywords:

Web Security, Authentication, Continuous Authentication, Biometric Authentication, Web Services.

1.INTRODUCTION:

The large use of web applications & internet services increases day by day, E-commerce, online banking for transaction processing and email are part of daily practice for many communities.

Therefore user authentication is important to create trust between user & internet services, that includes connecting a digital identity with single and accurate person. Previous system is implemented as one time identity proof during first log on process. Again here the legitimacy of user is believed to be same during entire session. Security of internet services & web application is measure issue because of increasing cyber attacks. Authentication method which depends on username & password, biometric authentications are" single shot" offers user verification only in login. One time user identity been verified the system services & resources are made available until user logouts and available for fixed time period. Many of the time user leaves already logged in system unattended for small or longer period in between other person can access same system intentionally for misuse.

Solution to this problem is to provide session timeouts but this is not ultimate solution. Biometric authentication & technique provides solution for trusted and secure authentication, where the password and username is replaced by biometric data. Biometric authentication is a process of determining & identifying the legitimate person's identity based on physiological & behavioral features which include face recognition, fingerprint identification, retinal scans, and voice recognition. Biometric authentication deals with actually identifying person based on their unique physiological or behavioral characteristics instead of their exclusive knowledge (e.g. username/Password) or possession(e.g. smartcard). Traditional biometric solution also provides single authentication it gives authentication only during login phase and the identity of user is stable during entire session and again single authentication cannot provide adequate amount of security.

We have already discussed this example, consider the situation: a user has login to a security significant web or internet service, and then user/person leaves the system unattended for certain time. In this situation the services can be misused easily. To continuously detect and monitor the adverse misuse of computer resources & internet services from unauthorized entrée, the best solution is provide constant continuous and clear authentication is required instead of one time authentication. This is a guaranteed approach to web services & computer systems than usual one. A major problem that continuous authentication aims to deal with is that user system or devices (mobile, laptop etc.) is used stolen after the user has already logged in. This paper presents a novel approach for continuous multiple verification & session supervision which is applied secure biometric authentication on the internet. It can function securely with different types of web services, with high safety and security requirements like online banking services.

2.AIM:

The aim of this paper to present the results of an exhaustive investigation into optimizing the recognition performance and an evaluation of the security processes required to maximize the security of the approach whilst minimizing user inconvenience.

3.OBJECTIVE:

The proposed framework encompasses the following objectives:

- To evaluate the performance current authentication techniques and asset the requirement of additional authentication.
- To investigate feasibility of behavioral biometric authentication techniques for deployment on mobile devices.
- To design and evaluate a new multi-modal behavioral biometric technique that provides reliability, transparent and continuous authentication for mobile devices.
- To design a multi-tier authentication architecture that flexible and scalable in that it can be applied to other biometric techniques along with transparent and continuous authentication of users.
- To implement and evaluate an authentication system to study its practical performance.

4. LITERATURE SURVEY

4.1) Quantitative Security Evaluation of a Multi-Biometric Authentication System:

Biometric authentication systems verify the identity of users by relying on their distinctive traits, like fingerprint, face, iris, signature, voice, etc. Biometrics is commonly perceived as a strong authentication method; in practice several well-known vulnerabilities exist, and security aspects should be carefully considered, especially when it is adopted to secure the access to applications controlling critical systems and infrastructures. In this paper we perform a quantitative security evaluation of the CASHMA multi-biometric authentication 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.

4.2) Model-based evaluation of scalability and security tradeoffs: A case study on a multi-service platform:

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.

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The evaluations 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.

4.3) Attacks on Biometric Systems: A Case Study in Fingerprints:

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.

4.4) Automated Generation and Analysis of Attack Graphs:

An integral part of modeling the global view of network security is constructing attack graphs. Manual attack graph construction 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.

4.5) Risk-Based Security Engineering through the Eyes of the Adversary:

Today, security engineering for complex systems is typically done as an ad hoc process. Taking a risk-based security engineering approach replaces today's ad hoc methods with a more rigorous and disciplined approach that uses a multi-criterion decision model. This approach builds on existing techniques for integrating risk analysis with classical systems engineering. A resulting security metric can be compared with cost and performance metrics in making engineering trade-off decisions.

5.EXISTING SYSTEM:

•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 assumes that a single verification (at the beginning of the session) is sufficient, and that the identity of the user is constant during the whole session.
•In existing, a multi-modal biometric verification system is designed and developed to detect the physical presence of the user logged in a computer.
•The work in another existing paper, proposes a multimodal biometric continuous authentication solution for local access to high-security systems as ATMs, where the raw data acquired are weighted in the user verification process, based on i) type of the biometric traits and ii) time, since different sensors are able to provide raw data with different timings. Point ii) introduces the need of a temporal integration method which depends on the availability of past observations: based on the assumption that as time passes, the confidence in the acquired (aging) values decreases. The paper applies a degeneracy function that measures the uncertainty of the score computed by the verification function.

DISADVANTAGES:

•None of existing approaches supports continuous authentication.
•Emerging biometric solutions allow substituting 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 immutable during the entire session.

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

6.PROPOSED SYSTEM

•This paper presents a new approach for user verification and session management that is applied in the context aware security by hierarchical multilevel architectures (CASHMA) system 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, and it is intended to be used from different client devices, e.g., smart phones, Desktop PCs or even biometric kiosks placed at the entrance of secure areas. Depending on the preferences and requirements of the owner of the web service, the CASHMA authentication service can complement a traditional authentication service, or can replace it.

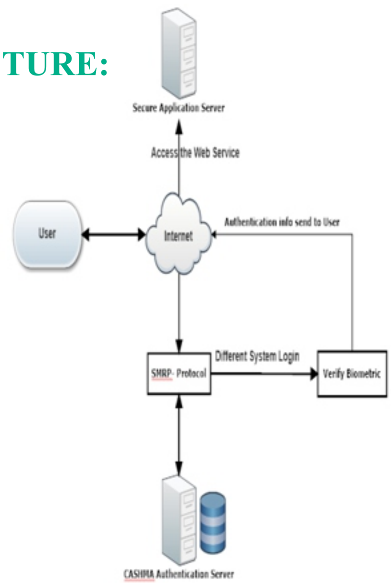
•Our continuous authentication approach is grounded on transparent acquisition of biometric data and on adaptive timeout management on the basis of the trust posed in the user and in the different subsystems used for authentication. The user session is open and secure despite possible idle activity of the user, while potential misuses are detected by continuously confirming the presence of the proper user.

ADVANTAGES:

•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 authentication service and the web services, which apply their own reaction procedures.

•Provides a tradeoff between usability and security.

7.ARCHITECTURE:



8.MODULES DESCRIPTION

System Model:

•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.

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:

o Customer Details

o Activation of Beneficiary

o Transaction Details

o Activate Blocked Account

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

CASHMA Certificate:

•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.

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.

9.CONCLUSION:

This Authentication System provides a novel approach of continuously validating the identity of a user in real time through the use of biometrics traits. This system shows efficient use of biometrics to identify the legitimate user. Also, it continuously verifies the physical identity of legitimate user through their biometric data. This authentication is able to achieve a good balance between security and usability with continuous and transparent user verification. Hence, continuous authentication verification with biometrics improves security and usability of user session.

10.FUTURE WORK:

In future research user satisfaction, security level, cost and maintenance, I think this is the important and main challenges. The next step would be to put more attention to the check level of security, also to do more testing in order to get more accurate results in research area.

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. 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)," BioID Press Release, https://www.bioid.com, Mar. 2011.

[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, Apr. 2007.

[6] 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.

[7] 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.

Authors Biography

Santhosh Kumar Khajapu completed his B.Tech(CSE) degree in CMR Engineering College in 2014. He is pursuing M.Tech. in Computer Science & Engineering from Department of Computer Science & Engineering in Malla Reddy Engineering College & Management sciences, Kistapur, Medchal,Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA, India.. His research interest include cloud, data mining, Big Data and networking.

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Y.Ashwini, working as Assistant Professor, department of computer science and engineering, in Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal ,Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA., India. Her research interests include data mining, computer networks.

Ch. Ramesh Kumar, working as Assoc. Prof & Head of the Department of Computer Science and Engineering in Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal, Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA., India. he has several international publications to his credit. His research interests include Software reuse, Software performance, Software testing ,Data Mining and cloud computing.