International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

Implementation of User Identity Verification for Secure Internet Services

Pruthvi M P[1], Tharunya B[2], Vinutha J S[3], Varsha Varadarajan[4], Prathibha B S[5],Avinash B[6]

[1234]Student,Dept of Information Science, NIE College, Karnataka, India
[56]Assistant professor, Dept of Information Science, NIE College, Karnataka, India

---

ABSTRACT: In recent years, fingerprint recognition technique is the dominant technology in the biometric market. A number of recognition methods have been used to perform fingerprint matching. The Straightforward matching between the fingerprint pattern to be identified and many already known patterns would not serve well due to its high sensitivity to errors (e.g. various noises, damaged fingerprint areas, or the finger being placed in different areas of fingerprint scanner window and with different orientation angles, finger deformation during the scanning procedure etc.).In this paper, we proposed effective fingerprint matching based on two methods I. e. method 1(pattern-based), Method 2(minutia-based). This paper presents extra patterns and features of fingerprint and show the matching between two fingerprints.

Index Terms- Fingerprint matching; pattern-based method; minutiae-based method;

INTRODUCTION

Session management in distributed Internet services is traditionally based on username and password, explicit logouts and mechanisms of user session expiration using classic timeouts. 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. Additionally, the length of the session timeout may impact on the usability of the service and consequent client satisfaction. This paper explores promising alternatives offered by applying biometrics in the management of sessions. 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.

SECURE user authentication is fundamental in most of modern ICT systems. 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; biometric techniques [1] offer emerging solution for secure and trusted authentication, where username and password are replaced by biometric data. However, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially considering their possible application in the financial and banking sectors [2]. Such observations lead to arguing that a single authentication point and a single biometric data cannot guarantee a sufficient degree of security [7]. In fact, similarly to traditional authentication processes which rely on username and password, biometric user authentication is typically formulated as a “single shot”, providing user verification only during login phase 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 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. For instance, 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. This problem is even trickier in the context of mobile devices, often used in public and crowded environments, where the device itself can be lost or forcibly stolen 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 [7]. A basic solution is to use very short session timeouts and periodically request the user to input his/her credentials over and over, but this is not a definitive solution and heavily penalizes the service usability and ultimately the satisfaction of users.

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. The approach we introduced in CASHMA for usable and highly

secure user sessions is a continuous sequential (a single biometric modality at once is presented to the system) multi-modal biometric authentication protocol, which adaptively computes and refreshes session timeouts on the basis of the trust put in the client. Such global trust is evaluated as a numeric value, computed by continuously evaluating the trust both in the user and the (biometric) subsystems used for acquiring biometric data. In the CASHMA context, each subsystem comprises all the hardware/software elements necessary to acquire and verify the authenticity of one biometric trait, including sensors, comparison algorithms and all the facilities for data transmission and management.

Trust in the user is determined on the basis of frequency of updates of fresh biometric samples, while trust in each subsystem is computed on the basis of the quality and variety of sensors used for the acquisition of biometric samples, and on the risk of the subsystem to be intruded.

RELATED WORK

To timely detect misuses of computer resources and prevent that an unauthorized user maliciously replaces an Authorized one, research work is keeping going from long back still misbehavior and phishing not been avoided as of our survey we done work and those are:

L. Montecchi et al; proposed Biometric authentication systems verify the identity of users by relying on users 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 that research they performed 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.

N. Nostro et al, proposed 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. In this paper they 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.

U. Uludag and A.K. Jain presented 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, they analyzed these attacks in the realm of a fingerprint biometric system and proposed 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.

O. Sheyner et al, experimented 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 and presented an automated technique for generating and analyzing attack graphs. Their technique on symbolic model checking algorithms, letting everyone construct attack graphs automatically and efficiently, they also describe two analyses to help decide which attacks would be most cost-effective to guard against. And finally implemented technique in a tool suite and tested it on a small network example, which includes models of a firewall and an intrusion detection system.

PROBLEM DEFINAITION:

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 multi-modal 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.

PROBLEM STATEMENTS:

- 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.

PROPOSED SYSTEM:

In 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., smartphones, 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.

MAIN OBJECTIVES:

- 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.

IMPELEMENTAION:

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.

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

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.

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.

REFERENCES:

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

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

[3] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, "Quantitative Security Evaluation of a Multi-Biometric Authentication" University of Florence, 50134 Firenze, Italy -2012

[4] L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and A. Bondavalli." Model-based evaluation of scalability and security tradeoffs: A case study on a multi-service platform". Volume 310, 5 January 2015, Pages 113-133.

[5] U. Uludag and A.K. Jain." Attacks on Biometric Systems: A Case Study in Fingerprints". Article in Proceedings of SPIE - The International Society for Optical Engineering 6 · January 2004.

[6] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing." Automated Generation and Analysis of Attack Graphs". Proceedings of the 2002 IEEE Symposium on Security and Privacy (S&Pí02)

[7] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, "Using Continuous Biometric Verification to Protect Interactive Login Sessions," Proc. 21st Ann. Computer Security pplications Conf. (ACSAC '05), pp. 441-450, 2005.

[8] A.K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security,vol. 1, no. 2, pp. 125-143, June 2006.

[9] L. Allano, B. Dorizzi, and S. Garcia-Salicetti, "Tuning Cost and Performance in Multi-Biometric Systems: A Novel and Consistent View of Fusion Strategies Based on the Sequential ProbabilityRatio Test (SPRT)," Pattern Recognition Letters, vol. 31, no. 9, pp. 884-890, 2010.

[10] S. Evans and J. Wallner, "Risk-Based Security Engineering through the Eyes of the Adversary," Proc. the IEEE Workshop Information Assurance, pp. 158-165, June 2005.

[11] M. Afzaal, C. Di Sarno, L. Coppolino, S. D'Antonio, and L. Romano, "A Resilient Architecture for Forensic Storage of Events in Critical Infrastructures," Proc. Int'l Symp. High-Assurance Systems Eng. (HASE), pp. 48-55, 2012.

[12] M. Cinque, D. Cotroneo, R. Natella, and A. Pecchia, "Assessing and Improving the Effectiveness of Logs for the Analysis of Software faults," Proc. Int'l Conf. Dependable Systems and Networks (DSN), pp. 457-466, 2010.

[13] N. Mendes, A.A. Neto, J. Duraes, M. Vieira, and H. Madeira, "Assessing and Comparing Security of Web Servers," Proc. IEEE Int'l Symp. Dependable Computing (PRDC), pp. 313-322, 2008.

[14] L. Montecchi, N. Nostro, A. Ceccarelli, G. Vella, A. Caruso, and A. Bondavalli, "Model-based evaluation of scalability and security tradeoffs: A case study on a multi-service platform," Electronic Notes in Theoretical Computer Science, vol. 310, pp. 113–133, 2015.