Enabling Privacy and Continuous Identity Verification for Secure Web Services

A.Raveendranadh Kumar & T.Swapna
[1]M.Tech Student, Dept. of CSE, SKU College of Engineering, Anantapur, India.
[2]Lecturer,Dept. of CSE, SKU College of Engineering, Anantapur, India.

ABSTRACT:

In distributed Internet services, Session management is conventionally based on username and password, explicit logouts and user mechanisms session expiration using classic timeouts. Authentication of user systems is traditionally based on pairs of username and password and verifies the identity of the user only at login phase. Checking’s are not performed during working sessions, which are concluded by an explicit logout or expire after an idle activity period of the user. Observations conduct to arguing that a single authentication point and a single biometric data cannot guarantee a sufficient degree of security. Similarly to traditional authentication processes which depend on username and password, biometric user authentication is generally represented as a “single shot”, providing user verification only during login phase when one or more biometric traits may be necessitated. 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. Biometric solutions permit substituting username and password with biometric data throughout session establishment, an approach still a single verification is deemed adequate, and the identity of a user is considered immutable during the entire session. In addition, the session length timeout may impact on the usability of the service and consequent client satisfaction. This paper investigates auspicious alternatives suggested by applying biometrics in the management of sessions. A secure protocol is defined for perpetual authentication through continuous user verification. The protocol directs adaptive timeouts based on the frequency, quality and biometric data type transparently acquired from the user. The functional behavior of the protocol is illustrated through Matlab simulations, while model-based quantitative analysis is carried out to assess the ability of the protocol to contrast security attacks *exercised by different kinds of attackers. At last, the current prototype for PCs and Android Smartphone's is discussed.*

KEY WORDS: Security, web servers, mobile environments, authentication, CHASMA.

INTRODUCTION:

Due to the fashionable trends increase within the quality and frequency of cyber-attacks, Security of web-based applications is a vital concern. Biometric techniques offer rising resolution for trustworthy and secure authentication, wherever watchword and username square measure replaced by biometric knowledge. Although, parallel to the spreading usage of biometric systems, the motivation in their misuse is additionally growing, particularly considering their potential application within the money and banking sectors. Cyber security is info security as applied to any or all computers and networks. pc security additionally includes protection from unplanned events and natural disasters. Most pc security measures involve coding of information and passwords. Encoding is that the translation of information into a type that's not comprehendible type. A watchword could be a cipher, word or phrase that provides a user access to a selected program. A user has already logged into a security-critical service, then the user leaves the computer unattended within the work space for a moment the user session is active, permitting impostors to impersonate the user and access strictly personal knowledge. In these situations, the services wherever the users square measure documented are often victimized simply. the essential resolution for this can be to use terribly short session timeouts and request the user to input his login knowledge once more and once more, however this can be not a satisfactory resolution. So, to timely establish misuses of pc resources and forestall that, solutions supported biometric continuous authentication square measure planned, meaning turning user verification into never-ending method instead of a past authentication. During this manner it applies multi-level verification life science authentication will depend upon multiple life science traits.

LITERATURE SURVEY:

1.‘’L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina,’’ Quantitative Security Evaluation of a Multi-Biometric Authentication System, Biometric authentication systems verify the users identity by wishing on their distinctive traits, like fingerprint, iris, face, signature, voice, etc. bioscience is usually perceived as a robust authentication methodology. In follow much well-known vulnerability exist, and security aspects ought to be rigorously thought of, particularly once it's adopted to secure the access to applications dominant vital systems and infrastructures. During this paper we tend to perform a quantitative security analysis of the CASHMA multi-biometric authentication system, assessing the safety provided by totally different system configurations against attackers with different capabilities. The obtained results give helpful insight on the safety offered by the various system configurations, and demonstrate the practicability of the approach to model security threats and countermeasures in real eventualities.

2.“ 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, Current ICT infrastructures area unit characterized by increasing necessities of responsibility, security, performance, accessibility, ability. A relevant issue is delineating by the quantitative of the system with reference to the increasing variety of users and applications, therefore requiring a careful orienting of resources. Moreover, new security problems to be faced arise from exposing applications and information to the web, therefore requiring AN attentive analysis of potential threats and also the identification of stronger security mechanisms to be enforced, which can turn out a negative impact on system performance and quantitative properties. The paper presents a model-based analysis of quantitative and security tradeoffs of a multi-service web-based platform, by evaluating however the introduction of security mechanisms could cause a degradation of performance properties. The analysis focuses on the OPENNESS platform, a web-based platform providing totally different reasonably services, to totally different classes of users. The analysis aims at distinguishing the bottlenecks of the system, underneath totally different configurations, and assesses the impact of security countermeasures that were known by a radical threat analysis activity antecedently dole out on the target system. The modeling activity has been dole out exploitation the random Activity Networks (SANs) formalism, creating full use of its characteristics of modularity and reusability. The analysis model is realized through the composition of a group of predefined guide models that facilitates the development of the general system model, and also the analysis of various configurations by composing them in numerous ways in which.

3.”U. Uludag and A.K. Jain”, 3) Attacks on Biometric Systems: A Case Study in Fingerprints, in spite of diverse blessings of biometrics-based personal authentication systems over ancient security systems supported token or data, they're liable to attacks which will decrease their security significantly. During this paper, we have a tendency to analyze these attacks within the realm of a fingerprint biometric system. we have a tendency to propose Associate in Nursing attack system that uses a hill climb procedure to synthesize the target item templates and judge its feasibility with intensive experimental results conducted on an oversized fingerprint info. Many measures which will be used to decrease the likelihood of such attacks and their ramifications also are conferred.

4.” O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing “, Automated Generation and Analysis of Attack Graphs, An integral a part of modeling the world read of network security is constructing attack graphs. Manual attack graph construction is tedious, fallible, and impractical for attack graphs larger than 100 nodes. During this paper we tend to gift an automatic technique for generating and analyzing attack graphs. We tend to base our technique on symbolic model checking algorithms, rental US construct attack graphs mechanically and with efficiency. We tend to conjointly describe 2 analyses to assist decide that attacks would be most cost-efficient to protect against. We tend to enforced our technique in an exceedingly tool suite and tested it on a tiny low network example, which has models of a firewall associated an intrusion detection system.

5) “S. Evans and J. Wallner”, Risk-Based Security Engineering through the Eyes of

the Adversary, today, security engineering for advanced systems is often done as an advert hoc method. Taking a risk-based security engineering approach replaces today's accidental ways with an additional rigorous and disciplined approach that uses a multi-criterion call model. This approach builds on existing techniques for desegregation risk analysis with classical systems engineering. An ensuing security metric may be compared with price and performance metrics in creating engineering trade-off selections.

RELATED WORK:

EXISTING SYSTEM:

Once the identity of the user has been verified, the system resources are obtainable for a fixed period of time or till explicit logout from the user. This approach assumes that a single verification is adequate, and that the user's identity is constant throughout the whole session. In existing, a multi-modal biometric verification system is designed and developed to detect the physical existence of the user logged in a computer. The related 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 obtained are weighted in the verification of the user process, based on type of the biometric traits and time, since different sensors are able to provide raw data with different timings. The second one introduces the use 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 obtained (aging) values decreases. The paper applies a degeneracy function that measures the improbability of the score computed by the verification function.

DISADVANTAGES OF EXISTING SYSTEM:

None of existing approaches hold up continuous authentication. Emerging biometric solutions allow substituting username and password with biometric data throughout session establishment, but in such an approach still a single verification is deemed adequate, and the user's identity is considered immutable throughout the whole session.

PROPOSED SYSTEM:

This paper presents a new strategy 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 capable to operate securely with any kind of web service, including services with high security demands as online banking services, and it is determined to be used from different client devices, e.g., Smartphone's, Desktop PCs or even biometric kiosks located 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 conventional 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 session of the user is open and secure despite possible idle activity of the user, while potential misuses are detected by constantly confirming the presence of the proper user.

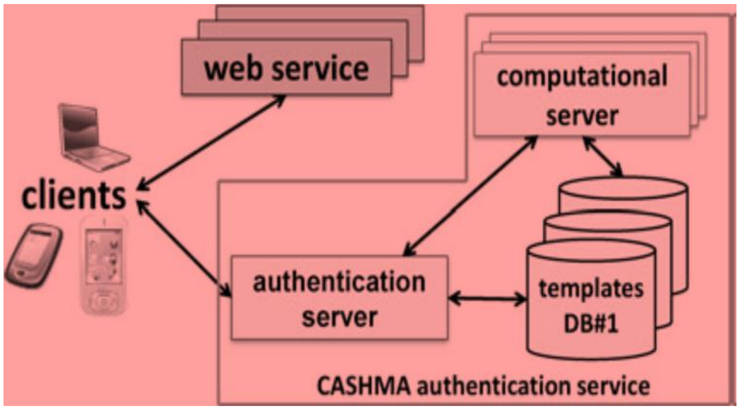
ADVANTAGES OF PROPOSED SYSTEM:

Our approach does not obtain that the reaction to a verification of the user 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. It offers a tradeoff between security and usability.

IMPLEMENTATION:

System Model, Authentication Server, CASHMA Certificate Continuous Authentication are the modules in user identity verification.

MODULES DESCRIPTION:



System Model:

In this chief system module, we produce 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 diminished security requirements as forums or social networks. In addition, it can grant access to physical secure areas as a limited zone in an airport, or a military zone. We elucidate 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 intention of logging into the Internet Banking facility offered by the Bank. "Login Password" is a unique and randomly generated password known only to the customer, which can be varied 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. Although 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 conventional banking methods, security is a chief concern. Server will take every safety measure necessary to be sure your information is transmitted safely and securely. The most recent methods in Internet banking system security are used to enlarge and monitor the integrity and security of the system. The Server preserves the functionality: Customer Details, Transaction Details, Activation of Beneficiary, and Activate Blocked Account

CASHMA Certificate

In this CHASMA Certificate module, we represent the information enclosed in the body of the CASHMA certificate conveyed to the client by the CASHMA authentication server, necessary to understand details of the protocol. Sequence number and Time stamp univocally identify each certificate, and defend from replay attacks. ID is the user Identification number, e.g., a number. Decision represents the conclusion of the verification procedure carried out on the server side. It comprises the expiration time of the session, dynamically allocated by the CASHMA authentication server. In reality, the global trust level and the session timeout are forever computed considering the time instant in which the CASHMA application obtains the biometric data, to pass up potential problems related to unfamiliar delays in communication and computation.

Continuous Authentication:

A secure protocol is described for perpetual authentication during continuous user verification. The protocol concludes adaptive timeouts based on the frequency, quality and type of biometric data transparently obtained from the user. The employ of biometric authentication permits credentials to be obtained transparently, i.e., without explicitly notifying the user or requiring his/her interaction, which is crucial to guarantee better service usability. The proposal behind the execution of the protocol is that the client continuously and transparently obtains and transmits confirmation of the user identity to preserve access to a web service. The chief task of the proposed protocol is to create and then continue the user session adjusting the session timeout on the basis of the confidence that the user identity in the system is genuine.

Session Management:

A web session is a sequence of network HTTP request and response transactions associated to the same user. Modern and complex web applications require the retaining of information or status about each user for the duration of multiple requests. Therefore, sessions provide the ability to establish variables – such as access rights and localization settings – which will apply to each and every interaction a user has with the web application for the duration of the session.

Web applications can create sessions to keep track of anonymous users after the very first user request. An example would be maintaining the user language preference. Additionally, web applications will make use of sessions once the user has authenticated. This ensures the ability to identify the user on any subsequent requests as well as being able to apply security access controls, authorized access to the user private data, and to increase the usability of the application. Therefore, current web applications can provide session capabilities both pre and post authentication.

Once an authenticated session has been established, the session ID (or token) is temporarily equivalent to the strongest authentication method used by the application, such as username and password, passphrases, one-time passwords (OTP), client-based digital certificates, smartcards, or biometrics (such as fingerprint or eye retina). See the OWASP

CONCLUSION:

We make use of the novel possibility established by biometrics to describe a protocol for continuous authentication that progresses security and usability of user session. The protocol calculates adaptive timeouts on the basis of the expectation posed in the user activity and in the kind and quality of biometric data obtained transparently through monitoring in background the user's actions. Some architectural design decisions of CASHMA are here conferred. At First, the system exchanges raw data and not the features extracted from them or templates, while cripto-token approaches are not considered; this is due to architectural decisions where the client is set aside very simple. We mention that our proposed protocol works with no changes using features, templates or raw data. Second, privacy concerns should be tackled considering National legislations. At present, our prototype only achieves some checks on face recognition, where only one face (the biggest one) rusting from the detection of user's face.

REFERENCES:

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

[2] BioID "Biometric Authentication as a Service (BaaS)," BioID Press Release, https://www.bioid.com, Mar. 2011.

[3] 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.

[4] 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.

[5] U. Uludag and A.K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints," Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622-633, 2004.

[6] D.M. Nicol, W.H. Sanders, and K.S. Trivedi, "Model-Based Evaluation: From Dependability to Security," IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, pp. 48-65, Jan.-Mar. 2004.

[7] 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.

[8] 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.

1. A.RAVEENDRANADH KUMAR has received the B. Tech (Information Technology) degree from Moghal college of engineering and technology, Hyderabad,Telangana in 2014, and pursuing M.Tech (Computer science and Engineering) in Srikrishna Devaraya University College of Engineering and Technology, Anantapuramu district (AP).

2. T.Swapna received her B.Tech Degree in Computer Scince and Engineering from Sri Venkateswara College of Engineering,Bengalor,India, in 2010; M.Tech in BNM Institute of technology,Bengalor , India, in 2012. She has experience of 3 years in teaching graduate level and she presently working as Lecturer in Department of CSE Srikrishna Devaraya University College of Engineering. Anantapuramu district (AP).