ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Continuous User Identity Verification Using the CASHMA System for Secure Internet Services

Ashlesha Kolarkar
Assistant Professor
Department of CSE
Lords Institute of Engineering and Technology.

M.Archana
M.Tech (S.E)
Department of CSE
Lords Institute of Engineering and Technology.

ABSTRACT

Nowadays, it becomes serious concern to provide more security to web services. So, secure user authentication is the fundamental task in security systems. Traditionally, most of the systems are based on pairs of username and password which verifies the identity of user only at login phase. Once the user is identified with username and password, no checks are performed further during working sessions. But emerging biometric solutions substitutes the username and password with biometric data of user. In such approach still single shot verification is less efficient because the identity of user is permanent during whole session. Hence, a basic solution is to use very short period of timeouts for each session and periodically request the user to input his credentials over and over. But this is not a proper solution because it heavily affects the service usability and ultimately the satisfaction of users. This paper explores the system for continuous authentication of user using his credentials such as biometric traits. The use of continuous biometric authentication system acquires credentials without explicitly notifying the user or requiring user interaction that is, transparently which is necessary to guarantee better performance and service usability.

KEYWORDS: ***Web Security, Authentication, Continuous user verification, biometric authentication.***

INTRODUCTION

The usage of web based applications and technologies are growing day by day rapidly. There are many world events that have been directed our attention toward safety and security. Therefore security of such web-based applications is becoming important and necessary part of today's technology world. Hence, now day's biometric techniques offer emerging secure and trusted user identity verification. Every biometrics refers that the identification of a person based on his or her physiological or behavioral characteristics. Now days there are many devices based on biometric characteristics that are unique for every person. In the biometric technique, username and password is replaced by biometric data. Biometrics are the science and technology of determining and identifying the legitimate user identity based on physiological and behavioral traits which includes face recognition, retinal scans, fingerprint, voice recognition and keystroke dynamics [3]. Also many of the biometric devices are based on the capturing and matching of biometric characteristics in order to produce a properpositive identification. The spreading use of biometric security systems increases their misuse, especially in banking and financial sectors. Biometric user authentication is formulated as a single shot verification which provides user verification only during login time. Once the identity of user is verified, the system resources are available to user for fixed period of time and the identity of user is permanent for entire session. Hence, this approach is also susceptible

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

to attack. Suppose, here we consider this simple scenario: a user has al-ready logged into a security-critical service, and then the user leaves the PC unattended in the work area for a 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. The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this is not a satisfactory solution[1]. To detect the misuse of computer resources and prevent it from unauthorized user, one solution is provided which is called biometric continuous authentication, which turns the user verification into continuous authentication instead of one time authentication. The use of biometric authentication acquires user credentials without explicitly notifying the user to enter data over and over. This provides guarantee of more security to system than traditional one [1].

In this technology era security of web-based applications is a serious concern, due to the recent increase in the frequency and complexity of cyber-attacks, biometric techniques offer emerging solution for secure and trusted user identity verification, where username and password are replaced by bio-metric traits. Biometrics is the science and technology of determining identity based on physiological and behavioral traits. Biometrics includes retinal scans, finger and handprint recognition, and face recognition, handwriting analysis, voice recognition and Keyboard biometrics. Also, parallel to the spreading usage of biometric systems, the incentive in their misuse is also growing, especially in the financial and banking sectors. Infact, 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 time 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 is also susceptible for attack because the identity of the user is constant during the whole session. Suppose, here we consider this simple scenario: a user has al-ready logged into a security-critical service, and then the user leaves the PC unattended in the work area for a 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.

The basic solution for this is to use very short session timeouts and request the user to input his login data again and again, but this is not a satisfactory solution. So, to timely identify misuses of computer resources and prevent that, solutions based on bio-metric continuous authentication are proposed, that means turning user verification into a continuous process rather than a onetime authentication. Biometrics authentication can depend on multiple biometrics traits. Finally, the use of biometric authentication allows credentials to be acquired transparently i.e. without explicitly notifying the user to enter data over and over, which provides guarantee of more security of system than traditional one.

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 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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 OF EXISTING SYSTEM:

- 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.

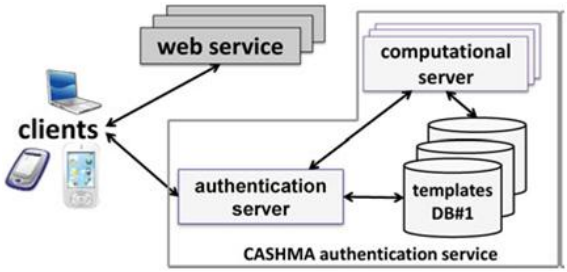
PROPOSED SYSTEM:

- 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.

ADVANTAGES OF PROPOSED SYSTEM:

- 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.

SYSTEM ARCHITECTURE:



Definition of Attackers:

One of the main challenges in security analysis is the identification of possible human agents that could pose security threats to information systems. The work in defined a Threat Agent Library (TAL) that provides a standardized set of agent definitions ranging from government spies to untrained employees. TAL classifies agents based on their access, outcomes, limits, resources, skills, objectives, and visibility, defining qualitative levels to characterize the different properties of attackers. For example, to characterize the proficiency of attackers in skills, four levels are adopted: “none” (no proficiency), “minimal” (can use existing techniques), “operational” (can create new attacks within a narrow domain) and “adept” (broad expert in such technology). The “Limits” dimension describes legal and ethical limits that may con-strain the attacker. “Resources” dimension defines the organizational level at which an attacker operates, which in turn determines the amount of resources available to it for use in an attack. “Visibility” describes the extent to which the attacker intends to hide its identity or attacks.

TABLE I: Attackers and Their Characteristics

	ORG	TMA	GEN	INS
Access	External	External	External	Internal
Limits	Extra-legal, major	Extra-legal, minor	Extra-legal, major	Extra-legal, minor
Resources	Government	Contest	Individual	Organization
Skill-Hack	Operational	Adept	None	Minimal
Skill-Spoofing	Operational	None	None	Minimal
Visibility	Covert	Clandestine	Overt	Clandestine

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Agent threats in the TAL can be mapped to ADVISE adversary profiles with relatively low effort. The "access" attribute is reproduced by assigning different sets of access domains to the adversary; the "skills" attribute is mapped to one or more attack skills; the "resources" at-tribute can be used to set the weight assigned to reducing costs in the ADVISE model. Similarly, "visibility" is modeled by the weight assigned to the adversary in avoiding the possibility of being detected. The attributes "out-comes" and "objectives" are reproduced by attack goals, their payoff, and the weight assigned to maximize the payoff. Finally, the "limits" attribute can be thought as a specific attack skill describing the extent to which the attacker is prepared to break the law. In this paper, it is rep-resented by the "Lawfulness" attack skill. In our work we have abstracted four macro-agents that summarize the agents identified in TAL, and we have mapped their characteristics to adversary profiles in the ADVISE formalism. To identify such macro-agents we first have discarded those attributes that are not applicable to our scenario; then we aggregated in a single agent those attackers that after this process resulted in similar profiles. Indeed, it should be noted that not all the proper-ties are applicable in our evaluation; most notably, "objectives" are the same for all the agents i.e., extending the session timeout as much as possible. Similarly "outcome" is not addressed since it depends upon the application to which the CASHMA authentication service provides access. Moreover, in our work we consider hostile threat agents only (i.e., we do not consider agents 1, 2 and 3), as opposed to non-hostile ones, which include for example the "Untrained Employee".

The attributes of the four identified agents are summarized in Table 1. As discussed names have the only purpose to identify agents; their characteristics should be devised from agent properties. "Adverse Organization" (ORG) represents an external attacker, with government-level resources (e.g., a terrorist organization or an adverse nation-state entity), and having good proficiency in both "Hack" and "Spoofing" skills. It intends to keep its identity secret, although it does not intend to hide the attack itself. It does not have particular limits, and is prepared to use violence and commit major extra-legal actions. This attacker maps agents 6, 7, 10, 15, and 18. "Technology Master Individual" (TMA) represents the attacker for which the term "hacker" is commonly used: an external individual having high technological skills, moderate/low resources, and strong will in hide himself and its attacks. This attacker maps agents 5, 8, 14, 16, and 21. "Generic Individual" (GEN) is an external individual with low skills and resources, but high motivation – either rational or not – that may lead him to use violence. This kind of attacker does not take care of hiding its actions. The GEN attacker maps 4, 13, 17, 19, and 20. Finally, the "Insider" attacker (INS) is an internal attacker, having minimal skill proficiency and organization-level resources; it is prepared to commit only minimal extra-legal actions, and one of its main concerns is avoiding him or its attacks being detected. This attacker maps agents 9, 11, and 12.

Evaluations: The composed model has been solved using the discrete-event simulator provided by the Möbius tool. All the measures have been evaluated by collecting at least 100.000 samples, and using a relative confidence interval of ±1%, confidence level 99%. For consistency, the parameters of the decreasing functions are the same as in Fig. 3 (s = 90 and k = 0.003); FMRs of subsystems are also the same used in simulations of Section 5 (voice: 0.06, fingerprint: 0.03, face: 0.05); for all subsystems, the FNMR has been assumed to be equal to its FMR. Results in Fig. 6 show the effectiveness of the algorithm in contrasting the four attackers. The left part of the figure depicts the measure Pk (t), while Tk is shown in the right part. All the attackers maintain the session alive with probability 1 for about 60 time units. Such delay is given by the initial session timeout, which depends upon the characteristics of the biometric subsystems, the de-creasing function (1) and the threshold gmin. With the same parameters a similar value was obtained also in Matlab simulations described (see Fig.3): from the highest value of g (u, t), if no fresh biometric data

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

is received, the global trust level reaches the threshold in slightly more than 50 time units. By submitting fresh biometric data, all the four attackers are able to renew the authentication and extend the session timeout. The extent to which they are able to maintain the session alive is based on their abilities and characteristics.

CONCLUSION

This paper provides various existing methods used for continuous authentication using different biometrics. Initial one time login verification is inadequate to address the risk involved in post logged in session. Therefore this paper attempts to provide a comprehensive survey of research on the underlying building blocks required to build a continuous biometric authentication system by choosing bio-metric. Continuous authentication verification with multi-modal biometrics improves security and usability of user session.

REFERENCES

[1]Andrea Ceccarelli, Leonardo Montecchi, Francesco Brancati, Paolo Lollini, Angelo Marguglio, Andrea Bondavalli, Member, IEEE, "Continuous and Transparent User Identity Verification for Secure Internet Services", IEEE Transactions on Dependable and Secure Computing, Manuscript Id, December 2013.

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

[3] L. Hong, A. Jain, and S. Pankanti, "Can Multi-biometrics Improve Performance?," Proc. AutoID'99, Summit, NJ, pp. 59–64, 1999.

[4] 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.

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

[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, April 2007.

[7] L. Montecchi, P. Lollini, A. Bondavalli, and E. La Mattina, "Quantitative Security Evaluation of a Multi-Biometric Authentication System," Computer Safety, Reliability and Security, F. Ortmeier and P. Daniel (eds.), Lecture Notes in Computer Science, Springer, vol. 7613, 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 Annual Computer Security Applications Conference (ACSAC '05), pp. 441- 450, 2005. IEEE Computer Society, Washington, DC, USA.

[9] A. Altinok and M. Turk, "Temporal integration for continuous multi-modal biometrics," Multimodal User Authentication, pp. 11-12, 2003.

[10] C. Roberts, "Biometric attack vectors and defenses," Computers & Security, vol. 26, Issue 1, pp. 14-25, 2007. [11] S.Z. Li, and A.K. Jain, Encyclopedia of Biometrics, First Edition, Springer Publishing Company, Incorporated, 2009.

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