Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Critical Review on Security Attributes: Authentication and Authorization

Mohd. Nazir*
Department of Computer Science, Jamia Millia Islamia
(Central University), New Delhi, India

Abstract—Web applications are prevalent platforms for information and services delivery over Internet. These applications are increasingly used to deliver the security critical services, such as financial transactions, commercial business. Software security is also vulnerable because the size and complexity of today's information system is growing rapidly. More security lapses are likely to be exploited in coming future. Therefore, software security is an inevitable aspect in current scenario and can no longer be considered as an afterthought. This research paper provides a critical review on security attribute, authentication and authorization. An effort has been made in this regard to provide a brief overview of pertinent knowledge about the important security attributes that are authentication and authorization. The paper discusses the definitions, classifications and then investigates methods on security attribute. The study concludes with possibility of quantitative estimation of software security at design phase via authentication and authorization.

Keywords— Software security, Security attributes, Authentication, Authorization, Authentication Configuration

I. INTRODUCTION

In today's world, Web applications are one of the most prevalent platforms for information and services delivery over Internet. These applications are increasingly used to deliver the security critical services, such as financial transactions, commercial business, and cyber community services etc. SANS Application Security Programs and Practices April-2015 Survey [18] reports that many organizations (38%) do not have sufficient control over their applications, so unable to identify all of the applications which they need to secure. The 34% organizations are still struggling to create an effective bridge between security and development (in-house, outsourced and third-party) When the web applications are developed and tested without considering little or no security aspect in mind in general, which results in variety security holes and often become a viable target for security attacks leading to severe economic losses [17]. The security problems are becoming complex with the complexity of the application along with the sophisticated techniques of attackers to exploit the vulnerabilities. The heterogeneous nature and the growing complexity of web application emphasise on the need to make them more secure. Recent studies shows that attacks against web applications are constitute more than 60% of the total attempts to exploit vulnerabilities. Attackers constantly modify their techniques to bypass these security systems; researchers in turn modify their approaches to handle new attacks [17]. More security lapses are likely to be exploited in coming future. Therefore, software security is an inevitable aspect in current scenario and can no longer be considered as an afterthought.

The three pillars of software security are considered as risk management, software security touch points and knowledge [1]. These are pillars in absence to which no security is complete and effective. Knowledge which belongs to any special person in any special field cannot pass the same on another generation. That is why people fail to absorb the great knowledge of the great persons who are already dead. Once information or knowledge gathered from any sources, knowledge should be shared so that people and institutions might be profited. Software security knowledge includes principles, guidelines, rules, vulnerabilities, exploits, attack patterns and historical risks. These are being used for many times. This knowledge will work better when used in a unified way. This knowledge will be a supportive and very instrumental for assuring the security of software. In order to spread software security knowledge software development staff must be trained and time to time they should be updated about current scenario and prevailing practices, and associated risks. For this purpose many software training programs should be organized, covering all the elements involved in software security. The problems practitioners are facing should have the extensive and detailed deliberation; discussions among panel of experts during such forums and training programs. However these three pillars of software security can be applied in a very systematic and cohesive and integrate and sensible manner. An effort has been made in this regard to provide a brief overview of pertinent knowledge about the important security attributes that are authentication and authorization.

Security is about preventing intelligent opponents from reaching their nasty objective. Software security is also vulnerable because the size and complexity of today's information system which is blossoming rapidly. Although the systems are free from bugs, misbalanced configuration of the system allows the intruders to find their way for encroachment. Now day's complex systems are prone to allow the enough space for attackers to easily exploit the loop

holes in the system. Security is still one of the holy grails of web applications [19]. It is essentially needed to first define security categorically and consequently understand what the security is? For a researcher working in this area, security generally means to create and/or develop such software that is beyond the reach of corrupt practitioners. In other words, software that is not easily accessible to the rogues. One of the core properties of the secure software Implies that it must only be available and accessible to its authentic and authorized users 2]. In computing systems, authentication and authorization must work in tandem to provide effective security. Without authentication, there would be no way to determine or identify if individuals are who they claim to be. Without some sort of authorization in place, it may not matter who they claim to be as with no authorization in place, essentially anyone could access anything simply by telling the truth about who they are.

II. SECURITY ATTRIBUTES: AUTHENTICATION AND AUTHORIZATION

The two major security attributes, authentication and authorization is the vital element of identity and access management that works as separate security mechanism to help assuring security.

Authentication: The act of verifying or validating end user, system credentials or service is called authentication. Authentication plays an important role in identification mechanism. It verifies the user by login credentials like user id, passwords, tokens or access codes. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. It accepts the information through user and checks his or her credibility and validates that information against authorization process [3, 4].

***Authorization*:** A trusted specific operation is performed by authenticated user is called authorization. Authentication establishes who a user is, and authorization determines what that user is permitted to do and what is not. Authorization process is just like to show the identity at the time of checking. In multi user computer system, authorization provides the privileges to access process or resources preceded by authorization [3, 4].

III. REGRESS REVIEW ON AUTHENTICATION AND AUTHORIZATION

Authentication: Authentication mechanism elevates the question in three classic ways to do so: what you know: it discusses about the password that belongs to the actual account holder. What you have: it explains the supporting tools to unlock like card, tokens, keys etc. what you are: it can express in terms of biometric authentication like retina, iris, voice, fingerprint, palm print or a combination of these systems to identify the user. The first way a system provides computer security is by controlling access to that system. Table 1 discusses the different type of configuration involved in an authentication procedure [4, 9].

Table 1: Different Types of Authentication Configuration

Authentication Type Configuration	Remarks
Realm-based Authentication	*User authenticates to a realm or sub realm in the Access Manager Information tree.*
Role-based Authentication	*User authenticates to a role within a realm or sub realm of the directory information tree.*
Service-based Authentication	*User authenticates to a specific service or application registered to a realm or sub realm.*
User-based Authentication	*User authenticates using an authentication process configured specifically for him or her.*
Authentication Level-based Authentication	*Administrator specifies the security level of the modules to which identities can authenticate.*
Module-based Authentication	*User specifies the module instance to which the user will authenticate.*
Organization-based Authentication	*User authenticates to an organization or sub organization.*

The review highlights the fact that the security quality of a software product can vary drastically depending on its design and the way of implementation. Literature survey shows that considerable efforts are being made towards acceptable metrics for authentication. The following section briefly describes some of the pertinent contributions made by the researchers and practitioners. Most of the work carried out in the area strengthens the need and importance of authentication mechanism.

A work carried out by Christopher Mallow entitled 'Authentication Methods and Techniques' discusses basic methods and techniques for accomplishing authentication on computer and network systems [5]. Different types of Authentication System are as follows: **Centralized authentication system:** In this scheme number of users can remotely authenticate through a catalyzed authentication system. Many different systems and protocols were developed for this purpose: remote-authentication protocols such as RADIUS (Remote Access Dial-In User Service), TACACS (Terminal Access Controller Access-Control System), Kerberos, and DIAMETER; and directory-based systems such as Novell's NDS (Novell Directory Services), Microsoft's Windows NT domains, and later, Active Directory. **Multi facto authentication:** This sachem provides more reliability and security of personal information by providing multiple authentication system.

The model offers tokens corresponding to individual access code. For example, ATM cards, as tokens, have their authentication strength increased when they are used by combining them with a PIN number. Smart cards are another token-based, multi-factor authentication system. **Split authentication:** This methodology works by splitting passwords or cryptographic keys among multiple sections. PGP permit splitting keys among multiple parties, so that messages may be encrypted, decrypted, or signed only when all parties submit their individual part of the split key. **Message authentication:** A message must be authenticated, or at least verified that it has not been altered in transit. This is known as integrity. In this case, a message authentication code (MAC) may be used.

A review paper in 1997 by Michael K. Reiter and Stuart G. Stubbebine of AT & T Labs, Research, USA entitled 'Towards Acceptable Metrics of Authentication' developing a set of guiding principles for the design of authentication metrics [6]. The model proposed that user locates a sequence of authorities such that the user can authenticate the first authority in that sequence. After that each authority in that sequence can authenticate the next authority and the last authority in the path or sequence is in fact the target person of key of interest. If the user trusts every authority on the path, then perhaps it can believe that a proper name-to-key binding has been obtained.

Ali Alkhalifah, Geoff D. Skinner presented a novel scheme for enhancing the knowledge based authentication (KBA) by using factoids not based on personal details. The paper entitled 'Enhanced Knowledge Based Authentication Using Iterative Session Parameters' published in 2010 uses past session parameters in an iterative fashion as the basis for future KBA questions. KBA works as customer authentication process for electronic transaction purpose [7]. The identification process of users is sometimes based on question answer process or PIN and passwords. The work tries to establish some assurance level based on knowledge question for authentication techniques. The first level used as a single authentication factor, where user has to answer one secret question that is not based on personal data. On a second level, multiple authentication factors are being used whose base is on previous personal data. In that case user have to answer two challenging question like last login and session id. At third level, three questions must be answered by the user regarding login time, date and session id. At the last level, users have to answer all questions that are offered in that interface e.g. last login time and transaction details. On the basis of above discussion researchers developed a set of security criteria to enhance KBA. These sets are guessability, the independence, the observation and the communication. They tested and measured the performance on developed system by applying these criteria by simulating four levels that further helpful to enhance knowledge based authentication scheme.

Mark Jakobsson , Liu Yang, Susanne Wetzel describes a technique aimed at addressing longstanding problems for password reset on his contribution 'Quantifying the Security of Preference Based Authentication ' in the year 2008. The contribution allows that users are authenticated using their preferences. The security features are being evaluated in three ways e.g. user experiments, user emulations and attacker simulation. The security of the system is evaluated on the realistic attackers. The first one is naïve attacker and other is the strategic attacker who knows the aggregate distribution [8]. At the root of almost all acts of security violations, there is one or more software vulnerability that can be exploited by an attacker to perform actions. The above mentioned description reveals the fact regarding authentication procedure for ensuring security of the system is discussed in Table 2 [4, 9] below.

Table 2: Details Regarding Authentication Mechanism

Authentication Mechanism	*Remarks*
Password Authentication Protocol	In Password Authentication Protocol (PAP), the user provides a username and password, and these are compared with values stored in a table to see if they match.
Challenge Handshake Authentication Protocol (CHAP)	*The device doing the authenticating, usually a network server, sends the client program an ID value and a random number, and both the sender and peer share a predefined secret word, phrase or value. The client strings together the random value (or nonce), the ID, and the secret, and calculates a new value from them using what is called a hash function. This new value is sent to the authenticator, which has built the same string and calculated a similar hash. The authenticator compares the result with the value it received from the client. If the values match, the peer is authenticated.*
Mutual authentication	*A two-way authentication where client authenticates to the server, and then the server authenticates to the client or workstation. This allows the server to verify that the user is at an authorized workstation.*
One-time password	*A variation of the username/password combination with OTP. The user creates a password, and the system creates a variation of the password each time a password is required. In this way, the same password is never used twice.*
Per-session authentication	One way to do per-session authentication is to increment a counter with every transmission. Because the password changes constantly, this form of authentication protects against attackers who snoop.
Tokens	A token or token card is usually a small device that supplies the response to a challenge that is received when trying to log on. One type of a token is a credit card-size device with a built-in keypad. At login, the server issues a

	challenge with a number. The user keys this number into the token card, and the card displays a response. The user inputs this response and sends it to the server, which calculates the same result it expects to see from the token. If the numbers match, the user is authenticated.
Biometrics	Biometrics, using personal measurements such as fingerprints, hand outlines, iris and retina scanners, voice recognition, handwriting analysis, and keyboard analysis can be a one-stop shop for authentication.
Remote access (TACACS and RADIUS)	Specialized login and authentication system: 1. Remote Authentication Dial-In User Service (RADIUS) 2. Terminal Access Controller Access Control System (TACACS), handling large amounts of login traffic can bog down a server. These protocols allow a network server to offload the user authentication and authorization to a central server. A typical enterprise network may have an access server attached to a modem pool, along with a RADIUS or TACACS server to provide authentication services.
DIAMETER	DIAMETER is a protocol that authenticates remote dial-up users, and also provides authorizations and accounting. DIAMETER supports the extensions to various network services.
Kerberos	A network authentication protocol developed in the 1980s at the Massachusetts Institute of Technology (MIT), called Kerberos. Kerberos provides secure transport across insecure media, such as the Internet. Named after the three-headed watchdog guarding the underworld in Greek mythology, Kerberos follows a three-step login process.

Authorization: A regress review is discussed regarding authorization in this section. A research paper entitled 'Identification and Implementation of Authentication and Authorization Patterns in the Spring Security Framework' by Aleksander Dikanski, Roland Steinegger, Sebastian Abeck, of Research Group Cooperation & Management (C&M), Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany argues regarding the usefulness of patterns for design of security functionality. Mature security products or frameworks are usually employed to implement such functionality. In this paper, the Spring Security framework is examined to provide support for authentication and authorization patterns. A real world case study is presented, in which the findings are employed to implement security requirements in a web application. With this approach it is possible to overcome the gap between pattern-based security design and implementation to implement high quality security functionality in software systems. The proposed work identifies RABC, ABAC and username/password authentication and implement those for spring security [10].

Another work in this area titled 'Role-Based Authorization Constraints Specification Using Object Constraint Language' was proposed by Gail-Joon Ahn, Department of Computer Science, University of North Carolina at Charlotte and Michael. E. Shin, Department of Information and Software Engineering, George Mason University augmenting that no access right is leaked to an authorized user. Constraints are an important aspect of role-based access control (RBAC). In this paper researcher discuss another approach to specify constraints by using declarative language, Object Constraints Language (OCL) that is part of the Unified Modeling Language (UML) and has been used in object-oriented analysis and design. This research paper demonstrated that user can specify role-based authorization constraints using an industry standard constraint specification language, OCL [11].

The article written by Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink and Charles E. Youmank, in IEEE Computer in 1996 entitled 'Role-Based Access Control Models' introduces a family of reference models for role- based access control (RBAC) in which permissions are connected with roles, and users are made members of appropriate roles. The essential impression of RBAC is derived with early multi-user computer systems that control general purpose customization facility and its administration itself. This novel work discusses a reference model to methodically deal with varied components of RBAC and their interactions [12].

A research paper in IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews entitled 'Constructing Authorization Systems Using Assurance Management Framework' by Hongxin Hu, *and* Gail-Joon Ahn, in July 2010 expresses the views on Model-driven approach to developing secure software and systems. An emerging trend is being used in the early stage of multilayered software development life cycle (SDLC), which is based on an assurance management framework (AMF), focusing on the development of authorization systems. AMF assists inclusive awareness security policies, models, verification, generation of security enforcement codes, and exact conformance testing. This approach is also helpful to understand the requirement of software engineers and security professionals for the analysis, design, implementation and testing of security properties in constructing real authorization systems [13].

A white paper by Rudolph Araujo & Shanit Gupta from Foundstone Professional Services in Feb 2005 on the topic of 'Design Authorization Systems Using SecureUML' describes the Foundstone SecureUML template, a Microsoft Visio template built to model authorization systems. The tool allows architects to control the power and suppleness of the Visio environment while modeling their role-based access control systems. Foundstone Professional Services, a division of McAfee, measurably protect the most critical threats by applying a planned approach to security [14].

Adam J. Lee from University of Pittsburg and Ting Yu from North Carolina State University on his research paper 'Towards Quantitative Analysis of Proofs of Authorization: Applications, Frameworks and Techniques' proposed a formal model that permits quantitative evaluation of the policy enforcement process of in both users to ideal and user to

user terminals. This paper quantifies the robustness of user's proof of authorization to probable perturbation in the system. They developed several classes of scoring functions like deterministic, simple ordering, authorization relevant, bounded, monotonic to satisfy policies by using useful risk metrics for decision making. They developed a framework for quantitative analysis of trust management proofs of authorization and articulate set of necessary requirements and desirable features for authorization scoring function [15].

The security expert and researcher Yuhui Zhong and Bharat Bhargava from Center for Education and Research in Information Assurance and Security and Department of Computer Science, Purdue University, USA developed a trust enhanced role mapping server, which can shared RBAC mechanism for authorization based on evidence and trust. The contribution entitled 'Authorization based on Evidence and Trust' presents an algorithm to evaluate reliability of evidence and role assignment policies. This works helps to quantify trust, formalization of evidence and trust, evaluation of reliability of evidences on the basis of machine reasoning and proof. This work is also beneficial in the area of e-commerce [16].

IV. RELEVENT FINDINGS

The regress review of previous sections about authentication and authorization at different phases on different issues provides a concrete conclusion on the basis of the diverse properties of security is as follows:

- The field of software security is still in its infancy and only quantitative assessment of security attributes may facilitate to deduce the mechanism for predicting how much the software under development is secured.
- Since meaningful quantitative metrics are largely missing or unavailable, the security community primarily uses qualitative mechanism or metrics for authentication and authorization
- The study concludes the facts that quantitative estimation of software security including authentication and authorization as key factor is possible at the design phase of development.
- It may help to better understand both the design and architecture information of the software system, which in turn will enable to comprehend the process of development and evitable maintenance.
- The proposed study may help to discover the underlying bugs, vulnerabilities and threats in the software design at the early stage of the SDLC leading to reduce effort significantly on security assurance and avoidance of unnecessary overhead.

V. CONCLUSION

The security problems are becoming complex with the complexity of the application along with the sophisticated techniques of attackers to exploit the vulnerabilities. The heterogeneous nature and the growing complexity of web application emphasise on the need to make them more secure. Recent studies reveals the fact that attacks against web applications constitute more than 60% of the total attempts to exploit vulnerabilities and they constantly modify their techniques to bypass these security systems. Therefore, it may be concluded that software security is an inevitable aspect in current scenario and can no longer be considered as an afterthought. The three pillars of software security are considered as risk management, software security touch points and knowledge. These are pillars in absence to which no security is complete and effective. Moreover, these three pillars can be applied in a very systematic and cohesive, may be instrumental if incorporated or integrate in a sensible manner. An effort has been made to provide a brief overview of pertinent knowledge about the important security attributes like authentication and authorization. The paper examined the pertinent literature review based on authentication and authorization. The review provides concrete information regarding the configuration and a mechanism for security attributes. Moreover, it concludes that there is possibility for quantitative assessment of security attributes with their relative properties at design time. That will greatly help for better assessment and judgement of security of the software.

REFERENCES

[1] G. McGraw, 'Software Security: Building Security In', Addison Wesley Professional, ISBN:978-0-321-35670-3, 2006

[2] M. Dowd, J.McDonald, 'The Art of Software Security Assessment: Identi-fying and Preventing Software Vulnerabilities', Addison Wesley Profes-sional, ISBN: 978-0-321-44442-4

[3] G,H. Walton, T. A. Longstaff, R.C. Linder, 'Computational Evaluation of Software Security Attributes', IEEE, 1997.

[4] M. Bishop, 'Computer Security: Art and Science', Addison Wesley, ISBN:0-201-44099-7, 2002

[5] C. Mallow, 'Authentication Methods and Techniques' web reference: www.giac.org/cissp-papers/2.pdf

[6] M. K. Reiter, Stuart G. Stubbebine, 'Towards Acceptable Metrics for Authentication', AT & T Labs, Research, Murray Hill, New Jersey, ISSN:1081-6011/97, IEEE 1997, pp:10-20

[7] A. Alkhalifah, Geoff D. Skinner, 'Enhanced Knowledge Based Authentication Using Iterative Session Parameters', World Academy of Science, Engineering and Technology, 2010, pp:293-299

[8] M. Jakobsson, Liu Yang, Susanne Wetzel, 'Quantifying the Security of Performance-based Authentication', ACM, ISSN:978-1-60558-294-8/08, 2008, pp:61-69

[9] R. Lehtinen, 'Computer Security Basics', O'Reilly Publisher, ISBN:13:978-0-59-600669-3

[10] A. Dikanski, R. Steinegger, S. Abeck,, 'Identification and Implementation of Authentication and Authorization Patterns in the Spring Security Framework', Research Group Cooperation & Management (C&M), Karlsruhe

Institute of Technology (KIT), Karlsruhe, Germany, web reference: http://cm.tm.kit.edu/CM-Web/05.Publikationen/2012/[DS+12] Authentication and Authorization Patterns in Spring Security.pdf.

[11] G.Joon Ahn, M. E. Shin , 'Role-Based Authorization Constraints Specification Using Object Constraint Language', Department of Computer Science, University of North Carolina at Charlotte, , Department of Information and Software Engineering, George Mason University, web reference: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.1111&rep=rep1&type=pdf

[12] R. S. Sandhu, E. J. Coynek, Hal L. Feinsteink and Charles E. Youmank, 'Role-Based Access Control Models', IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47.

[13] H. Hu, IEEE, and G. Joon Ahn,,'Constructing Authorization Systems Using Assurance Management Framework', IEEE Transactions On Systems, Man, and Cybernetics—Part C: Applications And Reviews, Vol. 40, No. 4, July 2010.

[14] R. Araujo, S. Gupta, 'Design Authorization Systems Using SecureUML', Found stone Professional Services, February 2005, web reference: foundstone.com.au/us/.../wp-design-authorization-systems-secureuml.pdf.

[15] A. J. Lee , T. Yu , 'Towards Quantitative Analysis of Proofs of Authorization: Applications, Frameworks and Techniques', University of Pittsburg, North Carolina State University, web reference: http://www4.ncsu.edu/~tyu/pubs/lee2010csf.pdf

[16] Y. Zhong, B. Bhargava, 'Authorization based on Evidence and Trust', Center for Education and Research in Information Assurance and Security and Department of Computer Science, Purdue University, USA, web reference:www.csc.ncsu.edu/faculty/mpsingh/papers/mas/TAAS-10-certainty.pdf

[17] Li, X., & Xue, Y. (2011). A Survey on Web Application Security. *Technical report, Vanderbilt University*, 2011. URL http://www.truststc. org/pubs/814.html. *Accessed* 20 April 2014.

[18] SANS Survey report, 2015. URL https://www.sans.org/reading-room/whitepapers /analyst/ survey-application-security-programs-practices-35150 20 April 2015.

[19] Gu Tian-yang, Shi Yin-sheng and Fang You-yuan (2010). Research on Software Security Testing. *World Academy of Science, Engineering and Technology* Issure 69. (pp. 647-651).

