IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

A Multi-Factor Authentication Scheme Using Attributed Access Control and Message Context

Ayman A.Rahim A.Rahman

Department of CIS, IT, Jerash University, Jerash, Jordan

Abstract: This paper presents an authentication method with different authentication levels. This system is different from other multi-factor authentication methods in that it enhances the levels with an access control. The access control contains attributes of the most authenticated user assigned in structured mode. Each sent message must classify according to its global context. The manager of the system takes this global context and submits it to a context analyser whose responsibility is to deduce lower levels of that global context. Then the manager forwards it to the suitable authenticated user in selected lower levels of the multi-factor scheme.

Keywords: Authentication, Multi-factor Level, Attribute Access Control, Message Context

I. INTRODUCTION

This Protection of sensitive data is a growing concern for organizations worldwide because of its financial implications [1]. Access to sensitive information starts with authentication. User names and passwords are commonly used by people during a log in process to validate user identity [2]. Passwords remain as the most common mechanism for user authentication in computer security systems. However, the use of passwords includes disadvantages, such as poor choice of passwords by users and vulnerability to capture [3,4,5]. Another major problem is that users tend to reuse passwords for different sites [6]. Several studies indicate that more than 70% of phishing activities are designed to steal user names and passwords. The Anti-Phishing Working Group reported [7] that the number of malicious Web pages designed to steal user credentials at the end of the second quarter in 2008 increased by 258% over the same period in 2007. Therefore, protecting user credentials from fraud attacks is extremely important. Many studies have proposed schemes to protect user credentials against theft [8,9, 10].

Authentication is the process of confirming or denying the claimed identity of a user [11]. The service provider has to trust the authentication performed by the identity provider of the user. This process is critical in terms of security because authorization and access control of the service highly depend on the authentication results. Weak authentication jeopardizes the security of the dependent service by increasing the risk that a user can impersonate another person and improperly gain access [12]. One effective authentication method is a mathematical model that combines different authentication methods, similar to that used in multifactor authentication, to build a high security trust system [13, 14].

Multi factor authentication (MFA) overcomes the vulnerability of passwords, which refers to the use of more than one factor in the authentication process [15, 16, 17]. One form of attack on networked computing systems is eavesdropping on network connections to obtain authentication information, such as the login IDs and passwords of legitimate users. Once captured, this information can be used at a later time to gain access to the system. One-time password (OTP) systems are designed to counter this type of attack, called a replay attack [18,19]. An OTP is valid for only one login session or transaction. OTPs prevent a number of shortcomings associated with traditional authentication (such as usernames and passwords) [20].

Attribute based systems are useful in practice because they are flexible, intuitive, and highly deployable. A common example is attribute-based directory searching where the attributes of an employee (e.g., department, location) are used to find the employee. In this example the flexibility comes from the ability to combine ⟨attribute, value⟩ pairs arbitrarily and intuitiveness comes from a common understanding of employee attributes. In general, attribute-based systems are deployable because most attributes associated with an enterprise are already present in various enterprise databases and assigned to enterprise users; e.g., in LDAP directories for the example above. Other examples of attribute-based systems include attribute-based authentication, access control, and trust negotiation [21,22,23,24,25].

Attributes define, classify, or annotate the datum to which they are assigned. The semantics of an attribute indicate some purpose or characteristic and, when used within larger collections, enable efficient identification and classification of like objects. For example, individuals in enterprise systems are often segregated into groups of common interest or duty based on a given set of attributes [26], e.g., function, department, university. These attributes are then used to associate sets of permissions and tasks to the specified individuals. Existing systems principally rely on the assignment and subsequent enforcement of policies by trusted and often centralized

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

servers. However, these servers are acutely ill-equipped to deal with disconnected and asynchronous clients. Reliance upon centralized servers further limits scalability and mandates a single point of trust.

Attribute-based encryption (ABE) [27], a generalization of identity-based cryptosystems, incorporates attributes as inputs to its cryptographic primitives. Objects are encrypted using a set of attributes describing the intended receiver. A principal possessing this subset as part of their pool of attributes can recover the original plaintext. More flexible requirements are achievable through the use of a thresholding primitive, for which only k-of-n attributes are necessary to perform decryption. Furthermore, decryption under both the standard and threshold approaches is collusion-resistant as multiple parties are unable to meaningfully pool attributes. Such cryptographic mechanisms allow encryption to inextricably bind expressive, enforceable access policy to objects.

II. RELATED WORKS

In reference [28] the authors described a new approach for developing and implementing an advanced authentication method within active directory network services. For advance authentication process a new type of user multi-factor authentication based on the classical three-factor authentication extended by the position information and time is described in this paper. The main objectives of this applied research are extended security features for more robust and more secure user's authentication process. Application scenario of advanced multi-factor authentication method within corporate networks based on the Microsoft Active Directory network services is presented. Five different factors for user's authentication provide more secured access control layer for current corporate networks with Microsoft Active Directory with only small implementation costs.

The second research is related to a cloud computing which are used to deliver services from a share pool of computing resources. In this research work, a novel access control framework is proposed that can address the security and privacy issues for cloud. The framework is based on dynamic trustworthiness of user and provides an effective and feasible access control solution for cloud. A multi layer security standard, policies and access control mechanism are provided with proposed framework. The access control is based on the trustworthiness of the user, which is demonstrated by static and dynamic trust evidence. The dynamic trustworthiness is used to reduce the possibility to perform unauthorized activities and ensures that only authorized user's access cloud resources. The prototype of the proposed framework is developed in NetLogo on Linux platform and demonstrated with test cases. The analysis of simulated results shows that proposed mechanism is highly efficient and robust under existing security threats [29].A proposed system in reference [30] is a privacy-preserving system using Attribute based Multifactor Authentication. This system provides privacy to data of users with efficient authentication and stores them on cloud servers such that servers do not have access to sensitive user information. Meanwhile users can maintain full control over access to their uploaded files and data, by assigning fine -grained, attribute -based access privileges to selected files and data, while different users can have access to different parts of the System. This application allows clients to set privileges to different users to access their data.

The countless advantages of cloud computing has brought a massive change to the lifestyle and the way to cope with the world today, yet the cloud has to reach maturity. However, the main barrier to its widespread adoption is the security and privacy issues. In order to create and maintain mutual trust among the customers and the cloud service providers, a well –defined trust foundation should be implemented. The data stored in the cloud remotely by individual customer or an organization, so they lost control over the data, thus creating a security dilemma. The most challenging and hot research area in cloud computing now a day is the data security and access control.

An effective measure to protect cloud computing resources and services in the start is to implement an access control mechanism. In reference [31], the features of various access control mechanisms are discussed and a novel framework of access control is proposed for cloud computing, which provides a multi -step and multifactor authentication of a user. The model proposed is well-organized and provably secure solution of access control for externally hosted applications.

III.PROPOSED SYSTEM

This system presents a method of authentication by construction different levels of authentication. This procedure needs designing an access control characterized by the different attributes of each authenticated user. The attributes include the following parameters:

1: Strength of his/her password.
2: Degree of his/her history trust which includes: Trusted, Moderate, Attempted hostile and Hostile.
3: IP attributes such as very safe, safe, Moderate, Dangerous.
4: Position transition periods.
5: Authentication levels.
These parameters are illustrated in figure 1.

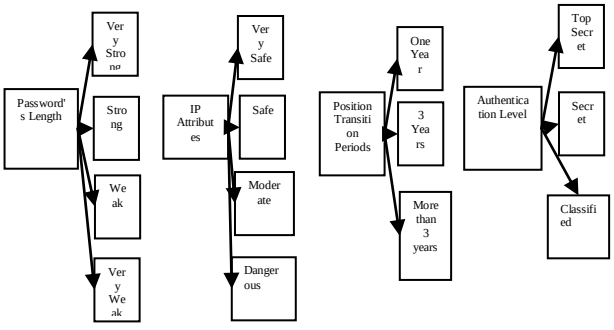

Fig 1: The Structure of the Attributed Access Control

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Another access control is assigned for the unique attributes of each user which contains different specialized data for that user such as the last two letters of his/her surname , the birth date of his/her father , the middle two digits of the phone numbers and the last lecturers he or she affects on him.

The system is intended to forward each document to the suitable authentication user depending on the information contained in the access controls. This task is successfully performed when each document must have a certain format. Each document must contain a global topic related to its context and detailed specialized sub-topics of the global one. So the document may have different sub-topics until it reaches to the intended interest of its topic.

The purpose of this format is that to enable the manager of the system to forward that document to the proper authenticated user. This user may stay in different levels of authentication. The decision of the manager must consider different parameters such as the special topics of each document ,the level of secrecy of that document such as whether it is top secret , secret or classified and the attributes of the most authenticated and specialized user.

The system has the following components: Trusted Manager (TM), Service Provider (SP), Service Requester (SR), Access Control (AC), and Message Context Analyzer (MCA). These components and the relations among them are illustrated in figure 2:

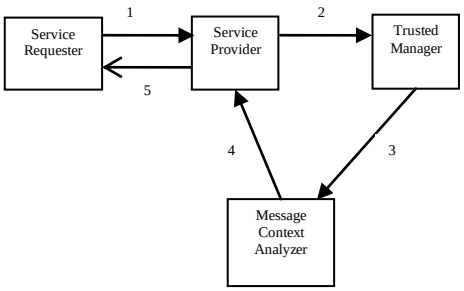

Fig. 2 The Main Components of Proposed Authentication System

When any document is sent to the manager, the manager sends it to the message context analyzer which takes the general topic of that document (GT). Then MCA searches to more detailed and specialized topic of GT. This procedure divides the document into lower levels of that document. Suppose the global topic is GT [HT] where HT means the high level of the global topic. Then HT may be divided into HT_1, HT_2,…HT_n.

After getting these details, the trusted manager forwards it to the proper authenticated user. The structure of the authenticated users takes the form of different levels. Each level is assigned to a certain general topic for each document. Each level consists of sub-trusted manager and a structure of different sub-levels .Each sub-level is further divided into further sub-levels depending on the number of lowers levels of each general document. If we face a lower level that is not included in the authenticated user's structure, the sub-manager must forward it to nearest sub-level. Figure 3 illustrates the structure of forwarding the document to the suitable authenticated user.

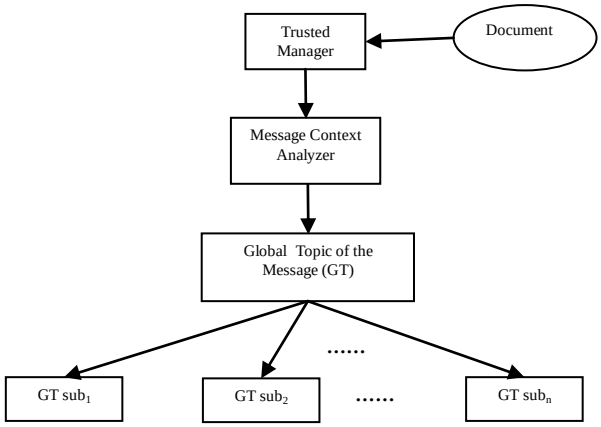

Fig. 3 The General Structure of the Proposed Multi- Factor System

Now the minor topic ($GT\ sub_n$) is sent to the suitable executive manager (EM) for each level in the multifactor authentication levels. So for each authenticated level there is a specialized EX. Each EX will receive the minor topic and forward it to the level concerned with that topic. For this purpose, the system constructs a multifactor authentication levels as shown in figure 4.

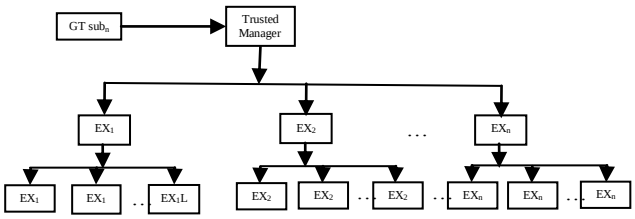

Fig.4 Some Levels of Multifactor Authenticated Executive Managers

The procedure of forwarding the minor topic of each document is that if $GTsub_n$ is found in the most lower level of each executive manager sub-level then , this manager forwards the minor topic directly to the authenticated user in that level .

Otherwise, the manager selects directly the predecessor to that sublevel. So if the exact minor level is not found for example in level n then the manager decides to forward it to the n-1 at the same minor level because the topic in this level is closely related to the exact minor topic of the document. It is possible to find more than an authenticated user in the same minor topic. The solution of choosing the proper authenticated user is done by examining the attributes of these users as listed in table 1. This responsibility of this task is done by the executive manger of that level.

IV. CONCLUSION

This proposed system enhances the authentication method. Multi-factor authentication provides different authenticated levels and prevents most common attacks against the system because the enemy faces a difficulty to find which the authenticated level is responsible for an intended intruder's task. This method is also used for the management of authentication by examining each document to deduce its context and further it is subdivided into more minor sub-context in order to forward it to the proper authenticated user. This task is accomplished by an efficient message context analyser. Finally, the system combines different secure features of an authenticated method, such as multi-levelling, message context and specialized information for each authenticated user .These combined parameters leads to designing a strong authenticated method.

REFERENCES

[1] T. Faruquie, N. Sumit, and S. Venkata, "Protecting Sensitive Customer Information in Call Center Recordings", in International Conference on Services Computing,2009, IEEE: Bangalore p. 81-88.
[2] A. Bander , "Improving Usability of Password Management with Standardized Password Policies", Queensland University of Technology,: Australia , 2011.
[3] S Abdulaziz. and Y. Ahmad, "A New Approach in T-FA Authentication with OTP Using Mobile Phone". Springer 2009. 58: p. 9-17.
[4] S . Jiří and D . Radek, "Multifactor authentication systems". elektro revue, December 2010.**1**(1213-1539): p. 1-7.
[5] B . John, "Fourth-factor authentication: somebody you know". ACM, 2006: p. 1-11.
[6] R.R.Karthiga and K.Aravindhan, "Enhancing Performance of User Authentication Protocol with Resist to Password Reuse Attacks", International Journal Of Computational Engineering Research (IJCER), 2012. **2**(8): p. 106-115.
[7] H. Chun-Ying, M .Shang-Pin, and T . Kuan, "Using one-time passwords to prevent password phishing attacks". Science Direct, 2011.
[8] Y . Chuan and W . HAINING, "A Transparent Protection Against Phishing Attacks", ACM, 2010. 10(2): p. 31.
[9] Y. Heng, "Panorama: capturing system-wide information flow for malware detection and analysis", in ACM conference on Computer and communications security2007, ACM: USA. p. 116-127.
[10] G. Scott, "Trustworthy and Personalized Computing on Public Kiosks", in 6th international conference on Mobile systems, applications, and services, 2008, ACM: USA. p. 199-210.
[11] C. Priti and Dr. D.S. Adane," Graphical Knowledge Based Authentication Mechanism", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),, 2012. **2**(10): p. 48-54.
[12] T .Ivonne, M.Michael, and M.Christoph , " Using Quantified Trust Levels to Describe Authentication Requirements in Federated Identity Management. " in ACM workshop on Secure web services (SWS). 13 Oct 2008. New York, USA: ACM.
[13] V.Akash, "Authentication Trust Level Network Architecture", International Journal of P2P Network Trends and Technology, 2012. 2(6): p. 99 - 129.
[14] C . Nicolae and P .Claudiu, "Authentication model based on Multi-Agent Syste",. University of Craiova/ Department of Mathematics and Computer Science, 2011. 38(2): p.59-68.
[15] T . Do van , "Strong authentication with mobile phone as security token" ,IEEEXplore, 2009: p. 777-782.
[16] K .Jae-Jung and H .Seng-Phil, "A Method of Risk Assessment for Multi-Factor Authentication", Journal of Information Processing Systems,, 2011. **7**: p. 187--198.
[17] L .Jing-Chiou and S. Bhashyam, "A feasible and cost effective two-factor authentication for online transactions", in International Conference on Software Engineering and Data Mining (SEDM), 2010 2nd 2010, IEEEXplore: Chengdu, China. p. 47 - 51
[18] J .Jongpil, C .Min Young, and C. Hyunseung , "Integrated OTP-based User Authentication Scheme Using Smart Cards in Home Networks", in Proceedings of the 41st Annual Hawaii International Conference on System Sciences. 2008. Waikoloa, HI IEEE.
[19] N. Haller Bellcore and C. Metz , "A One-Time Password System", 2012.
[20] K.Aravindhan and R.R.Karthiga , " One Time Password: A Survey", International Journal of Emerging Trends in Engineering and Development, 2013. **1**(3): p. 613-623.
[21] N. Li, J. C. Mitchell, and W. H. Winsborough ," Design of a role-based trust management framework", In IEEE Symposium on Security and Privacy, Oakland , May 2002.
[22] P. A. Bonatti and P. Samarati. A uniform framework for regulating service access and information release on the web.J. Comput. Secur., 10(3):241–271, 2002.
[23] T. Yu, M. Winslett, and K. E. Seamons ," Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation", ACM Trans. Inf. Syst. Secur. , 6(1):1–42, 2003.
[24] L. Wang, D. Wijesekera, and S. Jajodia ," A logic-based framework for attribute based access control", In FMSE '04:ACM workshop on Formal methods in security engineering, Washington DC , pages 45–55. ACM, 2004.
[25] E. Damiani, S. D. C. di Vimercati, and P. Samarati , " New Paradigms for Access Control in Open Environments", In 5th IEEE International Symposium on Signal Processing and Information, Athens , December 2005.
[26] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman,"Role-based access control models", Computer , 29(2):38–47, 1996.
[27] A. Sahai and B. Waters," Fuzzy identity based encryption", In Eurocrypt 2005 , 2005.
[28] K. Jaroslav, J.David, and K.Radek , " Implementation of an Advanced Authentication Method within Microsoft Active Directory Network Services ", 2010 Sixth International Conference on Wireless and Mobile Communications, 2010.
[29] R. K. Banyal **,** V. K. Jain **and** Pragya Jain , " Dynamic Trust Based Access Control Framework for Securing Multi-Cloud Environment" , ICTCS '14 Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies , ACM New York, NY, USA ©2014.
[30] T.Lakshmi Praveena , V.Ramachandran and CH. Rupa, " Attribute based Multifactor Authentication for Cloud Applications" , International Journal of Computer Applications (0975 –8887) Volume 80 –No 17, October 2013.
[31] U.Sultan, X.Zheng and F. Zhou , " TCLOUD: A Multi –Factor Access Control Framework for Cloud Computing " , International Journal of Security and Its Applications Vol. 7 ,No. 2, March , 2013.

BIOGRAPHY

Dr. Ayman A. Rahim A. Rahman, Jerash University- Jordan. PhD,MSc,BSC. He has completed Master degree in Information Technology, and his PhD in Computer Information System, and presently working as Assistant Professor in Jerash Uiversity -Jordan.

DOI 10.17148/IJARCCE.2016.5563