European Journal of Computer Science and Information Technology
Vol.3, No.5, pp.1-7, November 2015
Published by European Centre for Research Training and Development UK (www.eajournals.org)

THREE – LEVEL PASSWORD AUTHENTICATION

Mughele Ese Sophia

Department of Computer Science, Delta State School of Marine Technology Burutu P.M.B. 1060 Warri, Delta State Nigeria.

ABSTRACT: *Authentication is one of the most important security service provided to system by the different authentication schemes or algorithms which must be provided so that only authorized persons can have right to use or handle that system and data related to that information system securely. Techniques used include token based, biometric based as well as knowledge based. Despite these, no single mechanism is efficient and effective to provide adequate security for computing resources such as programs, files, messages, printers, internet, etc. A 3 – level authentication is proposed in this paper that is more confidential for ensuring adequate security.*

KEYWORDS: Authentication, Authentication Techniques, Information systems, Security

INTRODUCTION

Authentication is the proper validation and rights management of the user for accessing the resources of any information system. It is now beyond any doubt that user authentication is the most critical element in the field of Information Security (Manjunath et. al., 2013). Authentication is one of the most important security service provided to system by the different authentication schemes or algorithms. To protect any system, authentication must be provided so that only authorized persons can have right to use or handle that system and data related to that system securely (Vishal et. al., 2013). Authentication processes may vary from simple password based authentication system to costly and computation intensified authentication systems (Nagesh and Dharani, 2014). One of the approaches normally in use is the common authentication procedure in which a user needs only a user name and password, in other to make use of an authentication and authorization system in which every client has the right to access the data and applications which are only appropriate to his or her job (Savage, 2012).

A password is a secret word or phrase that gives users access to computer resources such as programs, files, messages, printers, internet, etc (Akinwale and Ibharalu, 2009). Passwords are more than just a key. They ensure our privacy, keeping our sensitive information secure. They also enforce non repudiation, preventing us from later rejecting the validity of transactions authenticated with our passwords. Our username identifies us and the password validates us (Nagesh and Dharani, 2014). Often, individuals tend to use key that can easily be remembered. This is one reason it is relatively easy to break into most computer systems (Hassan, 2005). Likewise, these passwords can also be easily guessed or broken. Gilhooly (2005), noted that the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. Therefore, it is pivotal to use a mechanism that is more confidential to ensure adequate security for computer resources. This is the impetus of this paper.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

This paper proposes an extremely secured system which employs 3 levels of security which includes textual password, pattern lock and biometrics. The 3-level password authentication system is an authentication scheme which combines the benefits of authentication schemes in existence to form the 3-levels of security. The proposed system in this paper would provide more secure authentication technique than existing one, overcome the drawbacks and limitations of previously existing systems (such as textual password, graphical password. etc) and combine more than one authentication techniques.

Survey of Authentication Techniques

Generally, authentication methods are classified into three categories (Manjunath et. al., 2013)(Suo et. al., 2005).

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based authentication

Token based means what you have (Vishal et. al., 2013). Token based techniques, use tokens such as key cards, bank cards and smart cards that are widely used by everyone (Varghese et. al., 2014). Others include a badge and a passport. Just as when a person loses a key, he would not be able to open the lock, a user who loses his token would not be able to login, as such the token based authentication category is quite vulnerable to fraud, theft or loss of the token itself (Manjunath et. al., 2013).

Biometric based authentication

Biometrics means what you are (Vishal et. al., 2013). The Inherent Based Authentication category which is also known as Biometric Authentication, as the name is the automated method/s of identity verification or identification based on measurable physiological or behavioral characteristics such as fingerprints, palm prints, hand geometry, face recognition, voice recognition and such other similar methods. Biometric characteristics are neither duplicable nor transferable. They are constant and immutable. Thus it is near impossible to alter such characteristics or fake them. Furthermore such characteristics cannot be transferred to other users nor be stolen as happens with tokens, keys and cards (Manjunath et. al., 2013).

Knowledge based authentication

Knowledge based means what you know (Vishal et. al., 2013). The most widely used authentication technique is the knowledge based techniques and it includes both text-based and picture-based passwords (Grover and Narang, 2012).True textual authentication which uses a username and password has inherent weaknesses and drawbacks.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

Proposed 3-Level Authentication

The paper proposes 3-level authentication which is a combination of many other authentication techniques/methods. The researcher proposes 3 levels of security. The 1st level employs the textual password, the 2nd employs the pattern lock and the 3rd level employs the biometrics which will provide more secure authentication (as shown in Fig. 1).

Figure 1: 3 -Level password authentication

1st Level – Textual Password

A password is a secret word or phrase that gives users access to computer resources such as programs, files, messages, printers, internet, etc (Akinwale and Ibharalu, 2009). Passwords are more than just a key. They ensure our privacy, keeping our sensitive information secure. There are mainly two types of password (Himika et. al., 2012):

- Static password
- Dynamic Password

Static password is the traditional password which is usually changed only when it is necessary: it is changed when the user has to reset the password, i.e., either the user has forgotten the password or the password has expired. While dynamic password, also known as One Time Password (OTP), is a password which changes every time the user logs in. An OTP is a set of characters that can act as a form identity for one time only. Once the password is used, it is no longer used for any further authentication. Moreover, the 1st level employs the static password due to the complexity of the One Time Password (OTP).

2nd Level – Pattern lock

This authentication system uses end user's visual memory. Using nine points in a three-by-three grid, a user creates a drag pattern. This method belongs not only to the something you know category, which is based on memory, but also to the behavior pattern recognition category, since it utilizes finger motion memory. The number of available secret patterns in this system is 388,912 (Lee et al., 2014). However, the number of patterns provided is limited (Kim et al., 2013). Hence, this locking feature is the most widely used by the general public.

3rd Level – Biometrics (Retinal recognition)

Biometrics establishes identity by recognizing an individual's physiological characteristics (Brunelli, 2009). Physiological or behavioral characteristics which can form the basis of a biometrics scheme are fingerprints, other characteristics that are distinctive, persistent, collectable, and the ability of the method to deliver accurate results under varied environmental circumstances,

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

acceptability, and circumvention. Biometrics can be used for verification as well as for identification. The verification is referred to as "one to one" matching while identification is known as "one-to-many" matching (Rosenzweig, 2002).

Biometrics has various components, but there are at least eight types namely Fingerprint, Hand Geometry, Facial Recognition, Iris Scan, Retinal Scan, Voice Recognition, Dynamic Signature Verification, and Keystroke Dynamics (Akazue and Efozia, 2010). The kind of biometrics proposed is the retinal biometrics. The continuity of the retina pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high security option (Akazue and Efozia, 2010).

Although, all the individual techniques above have their draw back and limitation, the proposed 3 – level authentication combines all the benefits in to one to enhance security in information systems.

Procedure

As shown in Fig 2, the user enters his/her username and password (which is static in this case), which is the 1st level of authentication. The authentication system validates this and if passed, the user proceeds to the 2nd level of authentication for the pattern lock. Otherwise, the user is denied access after three attempts. Furthermore, the user draws the pattern in the 2nd level before proceeding to the third level once validated. For the user to be fully granted access to the information system, the biometrics (retinal recognition) which is the 3rd level authentication is validated. Otherwise, accessed to the system is denied.

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

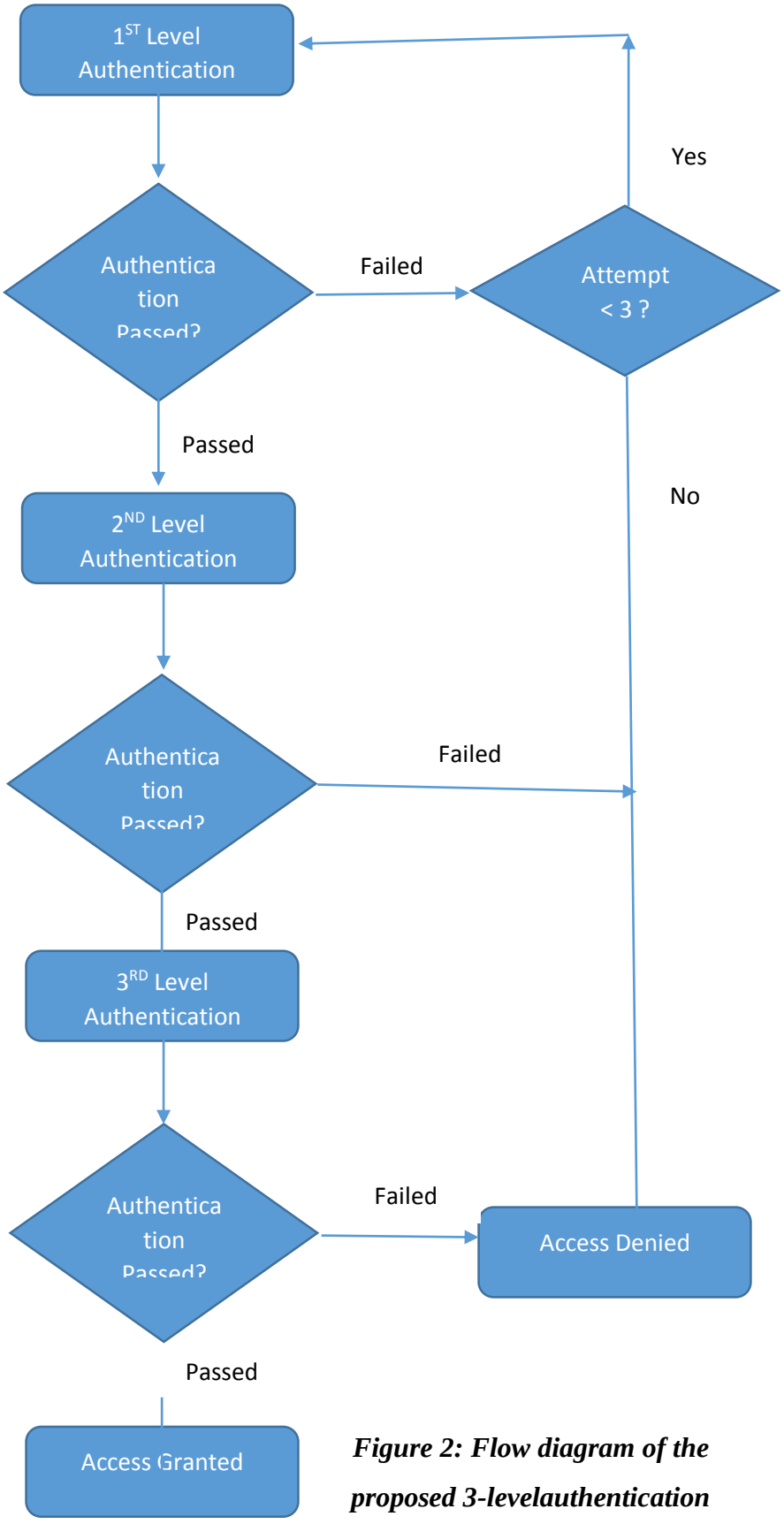

Figure 2: Flow diagram of the proposed 3-levelauthentication

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

CONCLUSION

Authentication is the proper validation and rights management of the user for accessing the resources of any information system and the most critical element in the field of Information Security. Yet, no single mechanism is efficient and effective to provide adequate security for computing resources such as programs, files, messages, printers, internet, etc. On that note, the paper proposes a 3 - level authentication technique which employs textual password, pattern lock and biometrics, hereby combining the benefit of the three techniques/methods to enhance the security of computer resources.

REFERENCE

A. A. Hassan (2005): Database security and auditing, protecting data integrity and accessibility. 1st edition, course technology

A. T. Akinwale and F. T. Ibharalu (2009): Password authentication scheme with secured log in interface. Annals. Computer Science series 7th tome 2nd Fasc.

Akazue M. 1 and Efozia, N. F. (2010): A Review Of Biometric Technique For Securing Corporate Stored Data

Bob Savage (2012): 'Science and Industry: Working Together for Economic Recovery', http://www. s i l i c o n r e p u b l i c . c o m / c l o u d / i t e m / 2 4 4 2 8 - c l o u d - most-significant-tranlast retrieved 02.08.2012.

Brunelli R.: Template Matching Technique in Computer Vision: Theory and practice. http://www.enterstageright. com (2009). Retrieved Sept. 2009.

Grover Aman and Narang Winnie (2012): 4-D Password: Strengthening the Authentication Scene. International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012 1 ISSN 2229-5518. IJSER © 2012 http://www .ijser.org

H.-W. Kim, J.-H. Kim, D. J. Ko, E.-H. Song, and Y.-S. Jeong, (2013): "8- Way lock for personal privacy of smart devices based on humancentric," in *Proceedings of the 40th Conference of the KIPS*, vol. 20, pp. 735–737, KIPS, November 2013.

Himika Parmar, Nancy Nainan and Sumaiya Thaseen (2012): Generation of secure one-time

Jae Dong Lee, Young-Sik Jeong, and Jong Hyuk Park (2014): A Rhythm-Based Authentication Scheme for Smart Media Devices. Hindawi Publishing Corporation, Scientific World Journal

K. Gilhooly (2005), "Biometrics: Getting Back to Business," in *Computerworld, May 09*, 2005.

Lalu Varghese, Nadiya Mathew, Sumy Saju, Vishnu K Prasad (2014): 3-Level Password Authentication System. International Journal of Recent Development in Engineering and Technology Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 4, April 2014)

M.Manjunath, K. Ishthaq Ahamed and Suchithra (2013): Security Implementation of 3-Level Security System Using Image Based Authentication. Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com Volume 2, Issue 2, March – April 2013

Nagesh.D Kamble and.Dharani J (2014): Implementation of Security System Using 3-Level Authentication. International Journal of Engineering Development and Research (www.ijedr.org) © 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)

Password based on image Authentication. pp. 195–206, 2012. © CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2417 Computer Science & Information Technology (CS & IT)

Rosenzweig P. (2002): Biometrics Technologies: security, legal and policy implication. Published by the Heritage Foundation. http;//www.fas.org/irp/congress/2002-rpt/911rept.pdf

Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod (2013): Secure Authentication with 3D Password. Certified International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013 ISSN: 2319-5967 ISO 9001:2008

Volume 2014, Article ID 781014, 9 pageshttp://dx.doi.org/10.1155/2014/781014

Xiaoyuan Suo Ying Zhu G. Scott. Owen (2005): Graphical Passwords: A Survey. Department of Computer Science Georgia State University xsuo@student.gsu.edu, yzhu@cs.gsu.edu, owen@siggraph.org. https://www.acsac.org/2005/papers/89.pdf

ISSN 2054-0957 (Print), ISSN 2054-0965 (Online)