Three Level Password Security

Omkar Poojary[1] Ankitkumar Vaishya[2] Shreyas Yadav[3] Manas Pandey[4]
[1,2,3,4]Student
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Thakur Polytechnic, Thakur Complex, Maharashtra, India

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.

Key words: Authentication, Authentication Techniques, Information Systems, Security

I. 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. 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.

II. Survey Authentication Techniques

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

- Text based authentication
- Biometric based authentication
- Image based authentication

A. *Text Based Authentication:*

Security at this level has been imposed by using Text based password (with special characters), which is a usual and now an anachronistic approach. Security at Level 1, at the client side is ensured by the use of text password, and that text password has to be entered by ensuring employment of special characters. Therefore, security at level1 is ensured by use of text password which is a usual approach, and now an anachronistic approach

B. *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).

C. *Image Based Authentication*

At this level the safety has been obligatory mistreatment Image based mostly Authentication (IBA), wherever the user is going to be asked to pick from the 2 problem levels. Each of the degree is going to be having 3 distinctive Image grids, from wherever the user should choose 3 pictures, from grids. The IBA security level is split into a pair of problem levels. The security of the system will be compromised if we tend to don't choose correct pictures for the image set. Conjointly we've to stay in mind that a user needs to be ready to bear in mind his image simply. Another vital side about image set is however these pictures square measure organized once conferred to a user.

Fig. 1: color based Authentication

We use a random show of pictures inside a picture set i.e. inside a picture set, pictures square measure organized willy-nilly associate degreed their position is not any wherever associated with previous image set that was generated at an earlier purpose of your time, i.e. throughout the previous signup or login method. By doing this, the system protects itself from several security attacks (to be mentioned later on) particularly from associate degree hearer trying from behind. Keystroke work is one among the key attacks tried by a hacker in authentication systems. It is most typical once text based passwords square measure used to demonstrate users. The aggressor observes the key strokes of a user and later will have access to the system.

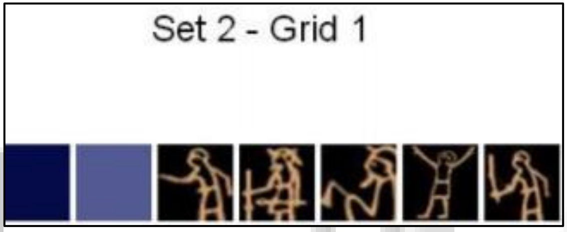

Fig. 2: Image Grid Authentication

III. 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).

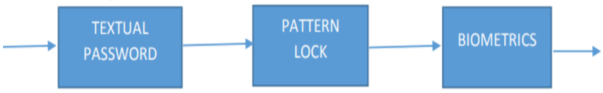

Fig. 3: 3-Level Password Authentication

A. 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:

1) Static password
2) 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).

B. 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. Hence, this locking feature is the most widely used by the general public.

C. 3rd Level

Biometrics (Retinal recognition) Biometrics establishes identity by recognizing an individual's physiological characteristics. Physiological or behavioural 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, 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. 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. 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.

IV. 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.

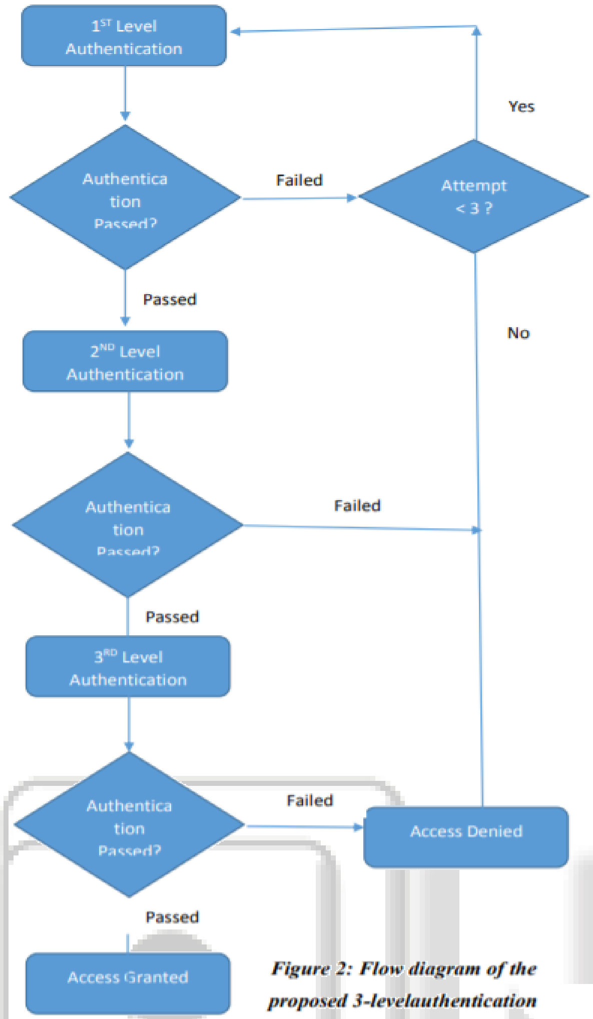

Fig. 2: Flow Diagram of the Proposed 3-level Authentication

V. EXISTING SYSTEM

Now days many hackers are hack our accounts and share all the details or collect the documents. Hackers are mostly hack our bank details, office details and personal mail. Now many security methods are used, But most of all failure process. Because all the applications have some easy way to hack. Our username identifies us and the password validates us. But passwords have some weaknesses: more than one person can possess its knowledge at one time. Moreover, there is a constant threat of losing your password to someone else with venomous intent. 3.

VI. PROPOSED SYSTEM

This unique and user-friendly 3-Level Security System is involving three levels of security. Where the preceding level must be passed in order to proceed to next level.Security at this level has been imposed by using Text based password (with special characters), which is a usual and now an anachronistic approach.At this level the security has been imposed using Image based authentication (IBA), where the user is asking to select from the two difficulty levels. Both the levels will be having three unique Image grids, from where the user has to select three images, one from each grid.After the successful clearance of the above two levels, the 3-Level security system will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his signed up email-id. Any hacker if in the extreme case, suppose (although difficult) will cross through the above two mentioned security levels, will definitely not be able to cross the third security level, unless he has access to the original user's email-id.

VII. ADVANTAGES

- This system use only security purpose, it uses to all security place.
- Hackers are not very easily to hack the security, because three levels are more useful this concept.
- Any hacker if in the extreme case, suppose (although difficult) will cross through the above two mentioned security levels, will definitely not be able to cross the third security level, unless he has access to the original user's email id.
- The user will be authenticated as an authentic user, and will be awarded access to the stored information, only after crossing the three security levels (Security level1-Text password, Security level2-Image Based password, and Security level3- One-Time Automated password).

VIII. 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.

REFERENCES

[1] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, Senior Member, IEEE 2008 Three-Dimensional Password for More Secure Authentication

[2] X. Suo, Y. Zhu, and G. S. Owen, ―Graphical passwords: A survey,‖ in Proc. 21st Annu. Comput. Security Appl. Conf., Dec. 5–9, 2005, pp. 463–472Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] Sagar Acharya1, Apoorva Polawar2, P.Y.Pawar. Student, Information Technology, Sinhgad Academy of Engineering/ University of Pune. Two Factor Authentication Using Smartphone Generated One Time Password

[4] http://en.wikipedia.org/wiki/File:Merkle-Damgard_hash_big.svg