The International Journal of Multi-Disciplinary Research
ISSN: 3471-7102

3 Level Password Authentication

(Conference ID: CFP/306/2017)

Authors Name: Mwendabai Malambo Chinyonga
Department: School of Engineering
Information and Communications University
Lusaka City, Zambia
Email: mwendaveli@gmail.com

***Abstract*—**
Managing security is a problem that has existed since Internet and Web Development came into existence. Text based passwords are the most common but they are not enough to counter such problems and they are an anachronistic approach. Therefore, there is need for something more secure and user-friendly. This paper proposes a system that requires three levels of security before access is granted to the user.

Keywords: *Managing security, Text based passwords, three levels of security.*

I. INTRODUCTION

The vulnerabilities of the textual password have been well known. Users tend to pick short passwords that are easy to remember. This makes the password vulnerable to attackers. Furthermore, textual passwords are vulnerable to shoulder-surfing, hidden camera, spyware, key loggers and brute force attack. Graphical password schemes have been proposed as a possible alternative to text-based schemes. However, they are mostly vulnerable to shoulder surfing and key loggers. There is a need for solving the above stated problem.

Materials / Methods / Design/methodology

Existing system

In today's world, hackers break into our accounts and collect our personal documents. These attacks are mostly targeted at our bank details, office details

and personal mail. The current security methods have failed to safeguard our data because most applications are vulnerable to attack. Our username identifies us and the password validates us. But textual passwords have some weaknesses: they are easier to guess or work out and are often easily forgotten.

Proposed system

In this paper, I present a 3 Level authentication System. Access to each new level is only secured upon passing the preceding level. Security at the first level has been imposed by using Text based password (with alpha-numeric and special characters). The second level of security involves a Pattern based authentication, where the user needs to remember pattern based images and arrange them in order.

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 their mobile phone.

A successful attack that reaches the second level will falter at the third security level unless the hacker has access to the user's mobile device too.

The figure below shows the block diagram showing the various stages of three level security systems.

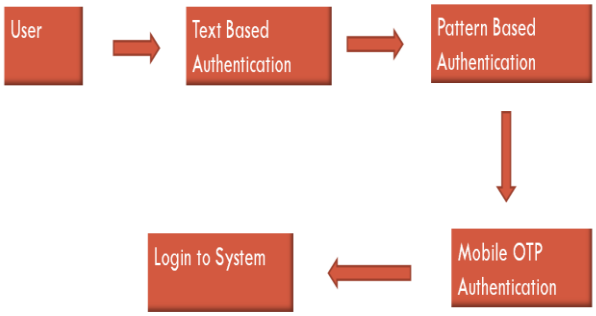

Fig.1: Architecture Diagram

1st Level - Text based authentication

Text based authentication is also known as alphanumeric password. This is the most popular technique which involves strings of letters and digits. Users tend to use short and simple passwords such as personal names of family members, phone numbers, dictionary words, birth-date etc. which are easy to remember. In today's world, users require passwords for personal computers, social networks, email, company applications and more. Because it is difficult to remember different passwords for different applications and devices, users tend to employ one password for all. Password security researchers realized that the user's independent password is vulnerable to various attacks such as dictionary attacks, easy to guess, brute force attacks, packet sniffing, key loggers, shoulder surfing, spyware attacks, social engineering, hidden camera etc.

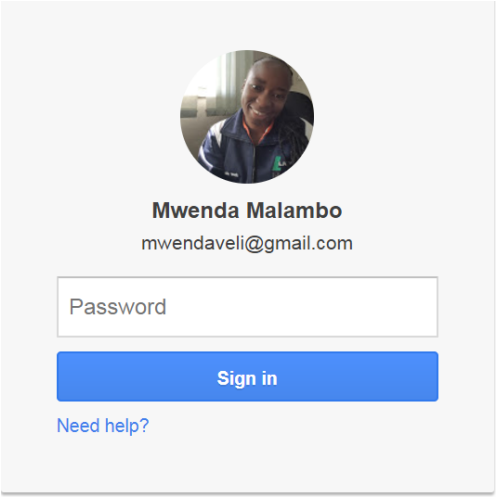

Fig.2: text password

2nd Level - Pattern based authentication

The second level of security is a pattern or image based authentication. From many studies and experiments performed by Neuroscientists, a popular theory called dual coding (Paivio, 1969, 1983, 1986) emerged which states that graphical objects such as pictures, images or shapes are better remembered than words or number sequences. This authentication system uses end user's visual memory.

Image ordering- Image ordering simply means the selection of previously set images in the same order. From a sequence of images, the user can select few images at random. The images provided are commonly used, user friendly and easy to remember. For instance, we can set a maximum count to three images. During authentication phase, the sequence of images will be given in a shuffled order, from which the user selects the same set of images chosen during registration phase in the same order. In case of any invalid selection of images, the system will be locked automatically after few trials based on the count given.

Image password schemes provide a way of making more user-friendly passwords.

Fig.3: Image pattern

3rd Level – Mobile OTP Authentication

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTP generation algorithms typically make use of pseudo randomness. This is done in order to prevent future predictions of OTPs by observing previous ones.

The first requirement is to register your phone number. After passing the second level image pattern authentication, an SMS with a unique 6 digit code is sent to your mobile phone. You then have to enter this number when you log in.

This password is generated and verified using Hash Functions and Secured Cryptographic Algorithm such as SHA-1 (Secure Hash Algorithm (SHA).

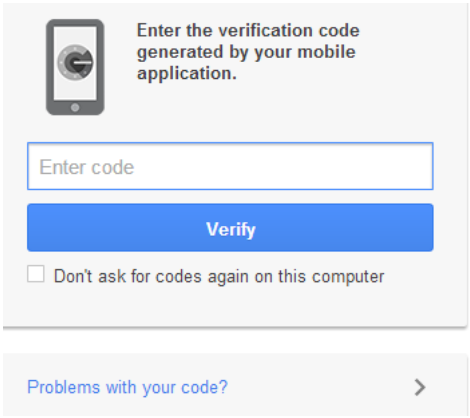

Fig.4: OTP authentication

- Time-synchronization – used between the authentication server and the client providing the password, OTPs are valid only for a short period of time.
- Mathematical algorithm – used to generate a new password based on the previous password, OTPs are effectively a chain and must be used in a predefined order.
- Mathematical algorithm - the new password is based on a challenge such as a random number chosen by the authentication server or transaction details and/or a counter.

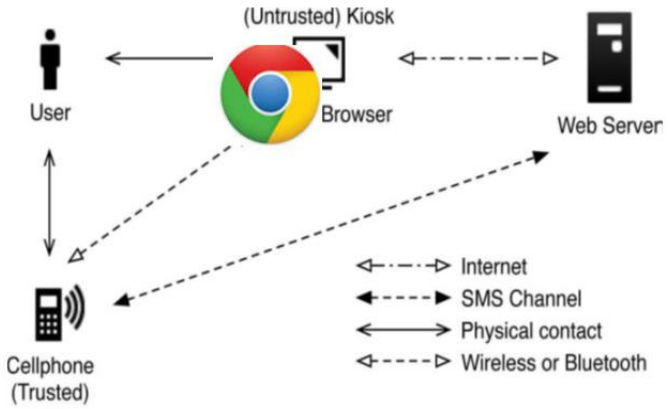

Fig. 4: OTP

A time-synchronized OTP is usually related to a piece of hardware called a security token. A user is given a personal token that generates a one-time password. Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server. On these OTP systems, time is an important part of the password algorithm, since the generation of new passwords is based on the current time rather than, or in addition to, the previous password or a secret key.

ADVANTAGES

• The system is user friendly

• It provides strong security against bot attacks or hackers.

• The user will be authenticated and will be awarded access to the stored information, only after crossing all three security levels.

DISADVANTAGES

• The first two levels have some vulnerabilities

• Man in middle attacks and dictionary attacks are possible.

• One needs to remember a series of passwords.

• It is also a time consuming process considering every person needs to give multiple authentications at various stages in the organization.

CONCLUSION

Text based authentication has major drawbacks and very vulnerable. The 3-level password (Password authentication, image based authentication and OTP) is a multifactor authentication scheme that combines the features of various authentication schemes. This system above makes it highly secure along with being more user friendly.

The Limitation of this paper is that it may be time consuming for the user to cross multiple levels to login successfully.

This system is not suitable solution for general security purposes, where time complexity will be an issue. But it will definitely be a boon in areas where high security is the main issue, and time complexity is secondary.

FUTURE WORKS

One of the future works will be hiring of white hats to attempt to break the system which will lead to system improvement and will prove the complexity of breaking the system. A shoulder surfing attack is a limitation against the 3-level password system. Therefore, a field research would be a better methodology.

Acknowledgment

First of all I would like to express my sincere gratitude to my husband and my mother for their guidance. I would also like to express my sincere gratitude to my lecturers, guides, colleagues and all who have helped in the completion of this paper successfully.

REFERENCES

[1] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik Three-Dimensional Password for More Secure Authentication

[2] Sonia Chiasson, P.C. van Oorschot, and RobertBiddle, "Graphical Password Authentication UsingCued Click Points" ESORICS, LNCS 4734, pp.359-

[3] **M.Manjunath** pursuing M.Tech II-year in Computer Science and Engineering from G. Pulla Reddy Engineering College during 2011 – 2013.

[4] Website: www.ijetae.com (ISSN 2250-2459,ISO 9001:2008Certified Journal, Volume 3, Issue 8, August 2013)

[5] Verlag Berlin Heidelberg 2007I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[6] 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