IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

A Survey on Various Authentication Mechanisms using Graphical Passwords

Prof. D.T. Salunke[1], Mrunal Arak[1], Tanvi Merai[1], Pooja Sutar[1]

Information Technology, JSPM's Rajarshi Shahu College of Engineering, Pune, India[1]

Abstract: The severity of attacks to Textual and Graphical Passwords has become a major threat to security nowadays. The vulnerabilities of this method which may be eves dropping, dictionary attack, social engineering, shoulder surfing etc. are the most difficult problem to defend against internet security. The goal of this paper is to understand various techniques used for authentication in the field of security. It would be necessary to come up with the better solution to solve the stated problem using the combination of existing techniques.

Keywords: Textual Password, Graphical Passwords, attacks, security, vulnerabilities, authentication.

1. INTRODUCTION

Cryptography is actually the study of not revealing or hiding the user information. Cryptography make use of mathematical technique for authentication. It translates the data in the form that only intended or specified user can understand the transmitted contents. In today's world many transactions take place and cryptographic standards are used to protect the information. There are two basic approaches used to speed up the cryptographic information. One of the approaches is to design cryptography algorithms which have faster execution rate. The speed of the algorithm is based on the number of rounds, message and key size. The second one is to perform the operation in parallel with the help of hardware. Authentication is a process of providing credentials of authorized users to gain access to the resources.

The passwords play an important role in providing security and authentication of user so it is necessary that password selection should be appropriate. These passwords must be secured by encryption to enhance computer security for protecting it from attacks. The parameters of encryption and decryption process plays a vital role for speed that is key streams in onetime pad, DES algorithm's secret key etc. One of the techniques to encrypt the password is RSA. In RSA, the secret key is derived from the public key by choosing very large p and q. Even though the parameters of RSA are considered it is not fully secured due to use of ASCII character. The same cipher text will be produced if the same character is repeated in more than one place in the plain text.

Very common method for authentication is textual password. The issues related to this method are eves dropping, dictionary attack, social engineering and shoulder surfing. Variable and long passwords make the system more secure. Actually the main problem is the difficulty in remembering these passwords. Studies have shown that users always tend to use short passwords which are easy to remember. Unfortunately, these passwords are easily guessed or cracked. The other available techniques are graphical passwords and biometrics. These two techniques have some disadvantages. Biometrics, such as finger printing or iris scanning etc. have been introduced but not yet commonly used. The major drawback of biometrics is that it can be expensive and the process may beslow. Another approach similar to biometric is Keystroke Dynamics which is an automated method of recognizing the user in the way the user types on keyboard. There are many graphical password schemes that are proposed in last few years. But these passwords are suffering from shoulder surfing which is quite a big problem. Personal Digital Assistants are used by the people to store their personal and confidential information. Authentication should be provided in such a way that they make use of these devices too.

Some of the attacks on existing systems are Keyboard logger, Virtual Keyboard, Mouse Logger, Mouse logger with screenshot. Keystroke logging, often referred as key logging or keyboard capturing, is the action of recording the keys stroke on a keyboard, typically in a converted manner so that the person using the keyboard is not aware that their actions are being monitored. It has its use in the study of human–computer interaction. There are numerous key logging methods which are ranging from hardware and software based methods to acoustic analysis. A virtual keyboard is a software part that allows to enter characters. A virtual keyboard can be operated with many input devices like a touch screen, an actual computer keyboard and a computer mouse. The main aim of using virtual keyboard is to avoid keyboard logger attack. A mouse logger is a part of software that will record user actions for playback for later use. The advantage to use a macro recorder is because it allows to easily perform complex operations at much faster rate and with less effort without custom computer programming. This mouse logger software is same as to mouse logger as it captures mouse events and also screenshot of the computer. The screenshot can be used to find which character you have typed on the screen.

DOI 10.17148/IJARCCE.2016.51251

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

2. RELATED WORK

Existing Authentication scheme are prone to following Attacks:

1. Dictionary Attack:
These are attacks are directed towards textual passwords. In such attacks the hackers actually use the set of dictionary words and authenticate them word by word. The Dictionary attacks fails to authenticate systems because of session passwords which are used every time to login.

2. Shoulder Surfing:
These techniques are resistant to shoulder Surfing. In Pair based scheme, resistance is provided by secret pass created during registration which remains hidden so the session password is not enough to find secret pass. In hybrid textual scheme, the random colours are used to hide the password whereas the ratings decide the session password. Even by knowing session password, the complexity is 8^4 so we can say that these are resistant to shoulder surfing.

3. Guessing:
Guessing is not a threat to the pair based methods because it is hard to guess secret pass. The hybrid textual scheme is dependent on selection of the colours and the ratings by the user which changes every time.

Literature Survey [1]:-

Graphical Authentication by Dhamija and Perrig [1]:
Dhamija and Perrig proposed a technique for graphical passwords authentication where the user has to identify the defined images to prove their authenticity. In this, the user has to select set of images from a set of random images during registration and then during login the user has to identify those preselected images for authentication. This system is vulnerable to shoulder-surfing.

Literature Survey [2]:-

Draw - a - Secret By Jermyn, et al[8]:
Jermyn, et al. had proposed a method known as"Draw- a-Secret" (DAS) where the user has to re-draw the pre-defined picture on a 2D grid and if the drawn picture touches the same grids in the same sequence, then the user is said to be authenticated. But this DAS scheme is vulnerable to shoulder surfing too.

Literature Survey [3]:-

Passface Authentication [2]:
Passface [2] is a technique developed where the user has to see a grid of nine faces and selects one face previously chosen by them. The user chooses four images of human as their password and the users have to select their preselected image from eight other set of images. As there are four user pass images it is done for four times.

Literature Survey [4]:-

Convex Hull for Graphical Password Authentication byWiedenback [3]:
Wiedenback et al [8] has proposed a graphical password entry scheme using convex hull method against shoulder surfing attacks. User must be able to recognize pass objects and click inside the convex hull formed by these pass objects. If user wants to make the password hard to guess, large set of objects can be used but it will make the images look very crowded and the objects almost indistinguishable. Using fewer objects may lead to a smaller password space resulting convex hull to be large.

Literature Survey [5]:-

Graphical Authentication byBlonder [5]:
Blonder [5] has designed a graphical password scheme where the user has to click on the approximated areas of pre-defined locations on particular image. Passlogix [6] elaborated this scheme by allowing the user to click on various objects in correct and ordered sequence to prove their authenticity. Haichang et al [7] also proposed a new scheme which was resistant to shoulder surfing where the user needs to draw a curve across their password images sequentially instead of clicking them directly. The graphical scheme is combination of DAS and story schemes which provides authenticity to the user.

Literature Survey [6]:-

Authentication by Drawing Signature Using Mouse by Syukri [4]:
Syukri has designed a technique where in authentication is actually done by drawing digital signature using a mouse. The technique includes two stages, in stage one registration is to be done and the other stage is verification. During registration stage user draws his signature with a mouse, after which the system extracts the signature area. It takes the user signature as an input and performs the normalization process after which extraction of the parameters of the signature is done in the verification stage. The disadvantage in this technique is forgery of signatures. Drawing with mouse is not familiar to most of the people and it is also a bit difficult to draw the signature in the same perimeters during registration time.

Literature Survey [7]:-

A Scalable Shoulder-Surfing Resistant Text and Graphical Password Authentication Scheme [13, 14, 16]:
To avoid or to reduce threats of the shoulder-surfing problem, one technique was developed by Zhao and Li named as "S3PAS". The importance behind this scheme was that in the login stage, the original text passwords in the login image must be found out and clicked inside the invisible triangular region. The system has both graphical

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

and textual password scheme integrated in it and has high level security.

Man, et al [14] developed shoulder-surfing resistant technique in which a user chooses many images as pass objects. The pass objects have variants to which is assigned a unique code. The user must type the unique codes of the pass-objects variants in scenes provided by the system in the authentication stage. Scheme shows perfect results it requires the user to remember code along with the pass-object variants.

Zheng et al [16] designed a hybrid password scheme based on shape and text in last few years. The basic concept was to map shape to text with strokes of the shape and a grid of text. Even though the fact that communication is secured since centuries, the key management problem is being preventing it from using it as a common application.

TABLE 1 COMPARISON OF VARIOUS METHODS USED FOR AUTHENTICATION

Sr. No.	Method	Resistance To Attack	Security Level
1.	Graphical Password	Shoulder Surfing	Medium
2.	Biometrics	Shoulder Surfing, Key Logger, Phishing	High
3.	Keystroke Dynamics	Shoulder Surfing, Key Logger, Phishing	Medium

3. CONCLUSION

We discussed the different methods used for authentication. But these methods in some or the other way prove to be vulnerable to shoulder surfing, key logger, phishing, dictionary attacks etc. The graphical password schemes that have been designed since last few years which have been resistant to shoulder-surfing but they have certain disadvantages like usability issues or slow speed for user to login or having security levels. The biometrics scheme is resistant to key logger but it lacks in standardization. Key stroke dynamics also has certain disadvantages. So there is a need to come up with the collaborative approach by analyzing all the discussed methods and find the efficient solution to cope up with all the vulnerabilities that would provide better authenticity and Internet security.

REFERENCES

[1] R. Dhamija, A. Perrig paper based on Study Using Images for Authentication in 9th USENIX Security Symposium, 2000.
[2] Real User Corporation: Passfaces.
[3] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon study on Design evaluation of a graphical password system. International J. of Human-Computer Studies 63 (2005) 102-127.
[4] A. F. Syukri, E. Okamoto, and M. Mambo, User Identification System by Signature done with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Notes in Computer Science (1438), 1998.
[5] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[6] Passlogix, website:- http://www.passlogix.com.
[7] Haichang Ga, Xiuling Chang, Xiyang Liu Uwe Aickelin paper on Password Scheme which is Resistant to Shoulder-Surfing risk.
[8] JermynI, Mayer A., Monrose F., Reiter M. and Rubin. Study on Design analysis of graphical passwords in USENIX Security Symposium, August 1999.
[9] W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.
[10] W. Jansen on Authentication scheme of user using Handheld Devices in Canadian Information Technology Security Symposium, 2003.
[11] D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.
[12] J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstracts on Human Factors in Computer Systems, 2002.
[13] H. Zhao and X. Li, "A Scalable Shoulder-Surfing Resistant Text and Graphical Password Authentication Scheme," in 21st International Conference on AINAW 07 vol. 2. Canada, 2007, pp. 467-472.
[14] S. Man, D. Hong, and M. Mathews paper on shoulder surfing resistant to graphical password scheme in International conference on security and management. Las Vegas, NV, 2003.
[15] X. Suo, Y. Zhu and G. Owen, "Survey on graphical password" in ACSAC'05.
[16] Z. Zheng, X. Liu, L. Yin, Z. Liu study based on password authentication scheme using shape and text, Journal of Computers, vol.5, no.5 May 2010.