Review of Password-Based Authentication Schemes

Anushree Ghag[1], Ami Mistry[2], Apurva Shinde[3], Priyadarshini Banpatte[4]
[1,2,3,4] Student, Department of Information Technology
Padmabhushan Vasantdada Patil Pratishthan's College of Engineering, Sion Mumbai
[1]anughag77@gmail.com, [2]amymistry97@gmail.com, [3]apoorvas.shinde1287@gmail.com, [4]banpattepriyadarshani11@gmail.com

Abstract: The most dominant authentication method, text based passwords are mainly prone to various attacks like dictionary attack, brute force attack and many more. Passwords are hacked in a variety of ways and for variety of reasons. For computer security and privacy, authentications based on password are widely used. Weak passwords are vulnerable to attacks. In this paper, we analyze various authentication schemes proposed by researchers. We have also proposed the system to resist the shoulder surfing attack and dictionary attack.

Keywords - Dictionary attack, brute force attack.

I. INTRODUCTION

The simplest form of user authentication available to us particularly on the Web, is the password authentication protocol. This method of authentication compels us to remember username and password combinations to access the user accounts. Once user enters data, the system authenticates users via database and grants access to the user. Such type of technique protects users' data and allows only the authenticated users to access the system. However, this technique is vulnerable to many attacks such as shoulder-surfing, key-loggers, brute force attacks etc. Textual passwords are one of the weakest password schemes. Because some passwords are easy to remember, but also easy to guess. Other passwords are secure but are difficult to remember. Graphical passwords are easy to recall and recognize. Graphical passwords are prone to shoulder surfing. To make graphical passwords resistant to shoulder surfing, Passpoint matrix [13] concept is introduced. Virtual passwords give different results for each run. Virtual password is a combination of string part and mathematical part. The string part is the original password and the mathematical part is the random salt. Graphical and virtual passwords are introduced because users usually tend to keep their passwords short and simple and are vulnerable to attacks. In this paper, we present the review of various password based authentication schemes proposed by various authors. We also propose a system where graphical and virtual passwords are used together to authenticate the user. The paper is organized as follows. Section I shows an introduction. We present the state of art of authentication attacks in section II. We present our proposed system in section III. Section IV concludes the paper and also focuses on the future work.

II. LITERATURE SURVEY

In today's world, passwords based on text which include lowercase, uppercase letters along with numbers has become common practice for the authentication process. But these passwords are quite difficult to remember, memorize and recollect. Hence, user either chooses a shorter password or the password that he/she could not easily forget. Majority of the users tend to keep same password for multiple websites, which can be easily hacked. Various methods are proposed and implemented to overcome brute force attack or dictionary attack, the two most popular password attacks. The most popular approach to avoid brute force is One Time Password (OTP). To address the limitations of text based password approach, various authentication schemes based on graphical password methods are developed. However, graphical password authentication approach is also susceptible to shoulder surfing attack which is the most common attack and is difficult to overcome. To overcome this attack, Draw a Secret (DAS) [1] method authentication, Pass point method [13] authentication scheme, Fake Pointer scheme [13] and Pass-matrix scheme [2] were proposed. Below we explain various approaches of password based authentication schemes proposed by researchers.

A. Schemes based on graphical password

H.Gao et al [1] proposed a shoulder-surfing resistant scheme, Contains DAS and Story, (CDS). CDS is based on recognition, an easier memory task and suggests users to create a story for sequence retrieval. As an input, CDS requires that users should draw a curve across their password images (pass- images) in order. The purpose of CDS is to overcome the drawback of recall-based systems by erasing the drawing trace and introduces the drawing method with the help of Story to resist against shoulder-surfing.
Shums Tabrez et al [2] proposed a pass-matrix authentication system. The Passpoint method [13] of authentication involved remembering n squares in single image as password, which made it prone to shoulder surfing. In the pass-matrix method, users choose one square per image for a sequence of n images rather than n squares in one image making it resistant to shoulder surfing. However, the drawbacks of pass-matrix authentication are, it is difficult for the user to remember pass points and also it is not completely resistant to shoulder surfing attack. The main purpose of pass-matrix authentication system is to eliminate text based passwords attacks.

B. Schemes based on Virtual passwords

P.Umadevi et al [3] has proposed a virtual password scheme based on virtual password. Their proposed scheme provides differentiated security scheme through Virtual Password Function (VPF) and VPF via helper application [11]. In differentiated security mechanism, the system allows users to choose a registration scheme ranging from simplest one to complex one. In helper application user inputs random salt number into helper application, which generates virtual password so that he/she can authenticate to the system. These schemes have been proven to be secured and provides protection against shoulder surfing and phishing attacks.

Yang Xiao et al [8] has introduced differentiated virtual password scheme in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security. Their proposed scheme requires a small amount of human computing for securing user passwords. The authors also introduced several functions serving as system recommended functions and provided a security analysis. Their proposed scheme defends against phishing, key-logger and shoulder-surfing attacks.

N. R. Rekha et al [4] proposed an enhanced Key Life in Online Authentication Systems Using Virtual Password. The authors proposed a new virtual password authentication scheme based on secret string, secret number and secret operations to register a user. This scheme requires human computational skills, which ensures strong security. The purpose of this paper is to secure user's password in online environments by shoulder surfing and key loggers attacks through virtual password authentication.

Biswas Gurung et al [5] proposed an Enhanced Virtual Password Authentication (EVPA). EVPA is designed to implement a virtual password scheme. This scheme introduces pass pattern concept. Pass pattern concept is used to generate random values in a user defined pattern. User selects secret strings, secret numbers, pass pattern and mathematical operations during registration. These parameters are further used to evaluate virtual password. EVPA is resistant to shoulder-surfing.

C. Schemes based on salt hashing

E M Wasifur Rahman Chowdhury et al [6] introduced Salty Secret, a novel authentication system which resists the shoulder surfing attack and enables use of arbitrary characters in user specified parts of password. Salty Secret enables non-determinism in the passwords, hence provides strong resistance against shoulder surfing.

P. Gauravaram [7] presents detailed security analysis on salt with password hashing. The author shows that functions based on compression are easily susceptible to offline birthday attacks [10]. The author also shows how the prefix- salt and suffix-salt are prone to attacks and how hashes computed using Davies-Meyer hash function [12] are not susceptible to this attack.

D. Schemes based on Password Memorability and Security

Jeff Yan et al [9] have proposed a new scheme for creating password. The authors suggested users to create a simple sentence of 8 words and choose letters from the words to make up a password. Their proposed scheme works as follows: i) Take the initial or final letters ii) Put some letters in upper case to make the password harder to guess, iii)Minimum one number and/or special character should be inserted. The purpose of this scheme of password was to enhance memorability and security in authentication.

From the survey presented above we observed that the existing schemes are susceptible to various attacks like phishing attack, dictionary attack, shoulder surfing attack and many more. To overcome these attacks, we have proposed an improved authentication scheme. Our proposed scheme combines graphical and virtual password authentication approach and hence will result in stronger authentication system.

III. PROPOSED SYSTEM: AN IMPROVED AUTHENTICATION SCHEME

Authentication is a process of identifying an individual, usually based on a login credentials such as username and password. Password plays a vital role for authenticating a user and giving access to the system. Users tend to choose passwords that are easy to remember even though alphanumeric characters are used, it is still prone to several attacks. Hence, a new scheme is required which can overcome these security issues faced by existing system.

Below we present the details of our proposed scheme.

A. Methodology

System Architecture

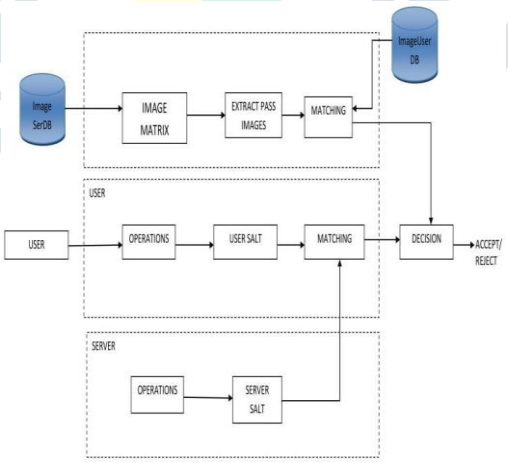

Figure 1: System architecture

The System Architecture shown in figure 1, represents the proposed authentication procedure. The purpose of ImageSerDB (Image Server Database) is to provide images for generation of image matrix. The images in matrix consist of *Pass images* (password images) along with random images. The user will draw a curve across his/her pass- images along with random images from the given image matrix which will avoid shoulder surfing. The *Pass images* (password images) are extracted from the curve images and compared with those stored in ImageUserDB during login phase. If the pass images match with the ones registered in ImageUserDB, then user is authenticated for next step. In second step, the user computes the salt by performing arithmetic operations on secret password and image ID. If both, the user computed and server computed salt matches then the user is authenticated.

Below we explain the registration and login phase of our proposed system.

The Registration Phase

1) The user has choice to select utmost 4 images from set of images.
2) The user is asked to enter numbers (secret password) as much as images selected during previous step.
3) The user is given choice to select arithmetic operations (addition (+), subtraction (-), multiplication (*) and division (/)) he/she is comfortable with.

The Login Phase

1) The pass-images are shuffled and displayed with many other images on screen.
2) Each Image has an ID.
3) The user draws a curve such that pass-images are selected along with some more random images.
4) Using the Virtual Password Function, computations are performed at server end.
5) User performs the computations to enter the password
6) Comparison of user computed salt and server computed salt: If string matches then user is authenticated.

Password=[Secret Password][Operator][Temporary Image ID]

VI. CONCLUSION

Security is a vast and emerging field of research which faces many challenges such as hacking, password cracking and different attacks. In this paper we have presented and analyzed the survey of password based authentication schemes proposed by researchers. Also, we have proposed the graphical and virtual password scheme. Our proposed scheme will provide strong security to users and will provide resistance to attacks such as key logger, shoulder surfing, dictionary and brute-force attacks. However, the proposed scheme requires human computations, which increases the processing overhead of the users. Our future work is to analyze the proposed system by implementing it. Further, detailed survey and analysis is required to determine the effectiveness and time complexity of the system.

REFERENCES

[1] H. Gao, Z. Ren, X. Chang, X. Liu, and U. Aickelin, "A new graphical password scheme resistant to shoulder-surfing," in Cyberworlds (CW), 2010 International Conference on. IEEE, 2010, pp. 194-199.
[2] Shums Tabrez, D. JagadeeshSai, "Pass-Matrix authentication," in International Conference on Intelligent Computing and Control Systems (ICICCS), 2017
[3] P. Umadevi and V. Saranya, "Stronger authentication for password using virtual password and secret little functions," in Information Communication and Embedded Systems (ICICES), International Conference on. IEEE, 2014, pp.1-6.
[4] N. R. Rekha, Y. S. Rao, and K. Sarma, "Enhanced key life in online authentication systems using virtual password," in Information Technology: New Generations (ITNG), 2011 Eighth International Conference on. IEEE, 2011, pp. 366-369.
[5] BiswasGurung; P Prasad; Abeer Alsadoon; Amr Elchouemi, "Enhanced Virtual Password Authentication Scheme Resistant to Shoulder Surfing," in 2015 Second International Conference on Soft Computing and Machine Intelligence (ISCMI), IEEE 2015.
[6] E M Wasifur Rahman Chowdhury, M Saifur Rahman, A. B. M. Alim Al Islam M SohelRahman, "Salty Secret: Let us secretly salt the secret," in 2017 International Conference on Networking, Systems and Security (NSysS) in Jan. 2017
[7] P. Gauravaram, "Security analysis of salt- password hashes,", in Advanced Computer Science Applications and Technologies (ACSAT) 2012 International Conference on, pp. 25-30, 2012
[8] Yang Xiao, Chung-Chih Li, Ming Lei, and Susan V. Vrbsky "Differentiated Virtual Passwords, Secret Little Functions, and Codebooks for Protecting Users From Password Theft," in IEEE Systems Journal, Volume: 8 , Issue: 2 , June 2014. Pp. 406 - 416
[9] J. Yan, A. Blackwell, R. Anderson and A. Grant, "Password Memorability and Security: Empirical Results," in IEEE Security & Privacy, Vol. 2 No. 5, 2004.
[10] https://danielmiessler.com/study/birthday_attack/
[11] https://www.techopedia.com/definition/23519/helper-application
[12] https://en.wikipedia.org/wiki/One-way_compression_function
[13] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System", IEEE Transactions on Dependable and Secure Computing (Volume: 15, March-April 1 2018)