Control Techniques for the Common Password Attacks

Madhu Meghana Talasila
Computer Science Department
Arizona State University
Tempe, United States of America
mtalasil@asu.edu

Abstract: *As the technology progress, lots of information has been produced over and over. The key issue is to protect data from the malicious user. Passwords, are used to protect data. But they form the weakest chain in the system as passwords are maintained by the user. Number of ways have been proposed to protect passwords from the malicious users. The three possible attacks that are discussed in this paper are hacking attack, phishing attack and weak passwords. This paper explains the hacking attack and the ways to overcome the hacking attack by using Noisy password schemes, dynamic password authentication and security and poly password hasher. Then paper explains the other possible attack phishing - PhishTank(2009) shows that there a number of active phishing sites which can retrieve username and password, thus making the system vulnerable. The solutions that are discussed to protect the system from this kind of attack is One Time Password (OTP) using reliable security channel. The other possibility is user choosing weak passwords based on a number of reasons such as interference with "Long Term Memory". This paper explains the blonder's mechanism of graphical passwords as an alternative to weak passwords. Finally, this papers explains the pros and cons with each of the discussed solutions and identifies OTP using Instant Messaging as a better alternative.*

Key words: Authentication, Authorization, Cross-site scripting, Hacker

I. INTRODUCTION

With the increase in technology, computer became a one stop for all the needs from extremely important transactions like online-banking to regular grocery shopping can be done online. For which user has to maintain an account with vendor/ system. The Password is the best way to get access to the system. Hence, malicious users are targeting the passwords and trying to get lot of information. The possible attacks on passwords range from simple dictionary attack to social engineering. This paper deals with the attacks on passwords like hacking attack, phishing attack and weak passwords. Explains few of the approaches that deals with these attacks and identifies the better possible alternative among them by analyzing various factors like cost, query run time, effectiveness and by security analysis.

II. HACKING ATTACK

Hacking attack is to gain unauthorized access to the system by "bypassing" the security of the system. Examples of hacking attacks are shoulder surfing, dictionary attack, password theft etc. The possible solutions for hacking attack are discussed below [1].

1. Noisy Password Scheme

In contrast to the original password, in this along with the password some noise is also added. Software is available which takes the passwords, encrypts the password during registration and decrypts the password during authentication. Noisy password P = <S, V, X, F> consists of 4 parts safeguard S, variable alpha numeric value V, fixed alpha numeric value F and a terminator X. [2] During user registration uses has to enter the variable alphanumeric password, fixed alpha numeric password which acts as noise to construct the encrypted password, terminator which cannot be in the set of values V that user selects and an alpha numeric Text of length S, which acts as safeguard. In this mechanism user has to remember the original password and the terminator. This technique proves to the best when used by people who have knowledge of the technique. The fixed part and terminator forms the backbone of the scheme as they are hard to crack and at the same time once cracked, it is very easy to get access to the system. [3]

2. Noisy Password with Patterns

This is similar to the Noisy Password scheme. In this user has to enter the password and the pattern

which dynamically changes the password and then encrypted by the software which makes the password more secure and difficult to crack by the attackers. This mechanism can be applied on character based passwords and digit based passwords. This is more resistant to dictionary attack as the variable length changes every time and shoulder surfing is impossible [4][5].

3. *Dynamic password authentication and security system using grid analysis (DPASS):*

In this paper, I studied "DPASS – Dynamic Password Authentication and Security System using Grid Analysis" by Balaji R and Roopak V. This system makes use of dynamically generated grid and dynamically generated one time password. The grid consists of alphabets, symbols and numbers. User can select any of these and any number of times to form the password. Grid is generated based on the capacity of the server. The values that are selected in the grid are used as passwords. [2]

The scheme is dynamic and the pattern that the user enters also changes every time. The advantage with this system is user can choose a character as his complex character which exponentially increases the number of combinations.[6]

PolyPasswordHasher

PolyPasswordHasher is another scheme proposed by Justin cappos. This system is more resistant to hacking attacks especially for files in database. The author assumes a threat model and describes the paper on the grounds of those assumptions. It uses SHA 256 with salt and shamir secret sharing scheme to divide the hashed passwords and to separately store the individual shares. This system is robust and work well password files because even if the hacker got access to the system it remains useless until all the shares in the password file are known correctly [7].

Traditional system store password as "Username, salt, Hash(password+ salt)" but PolyPasswordHash saves the password as "Username, salt, share(share number) XOR hash(salt+password)". The advantage with this scheme is that it increases the search space of the hacker as one need to obtain threshold of shares to completely know the password. In the figure 1 [3][8] it is clear that as the K value increases, the time to crack the password is increasing exponentially and almost makes the password impossible to hack.

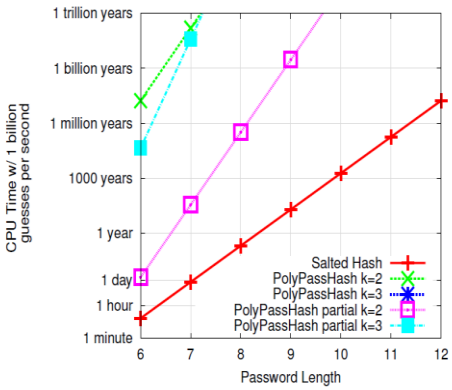

Figure 1Time to crack a password given 1 billion attempts per second [8]

III. PHISHING ATTACK

In the phishing Attack, phiser tricks the users and gain potential information from the users to retrieve the password. Because of increase in number of internet users, phishing attack gained its prominence. Some of the ways in which hackers can gain information from the user are by forwarding emails which contain malicious content, whenever user open the mail or acted as mentioned in the mail hacker can easily get access to the system[9] [4] and by claiming as the potential operator and gets necessary information to get password. The anti-phishing techniques are given below.

1. *Spam Filter*

Spam filters are used to spam the fraudulent mails based on the training data or filters. This makes the mails to be moved to spam and thereby avoids reading of fraudulent mails. Main disadvantage with this technique is that if the spam mails are not recognized by the filter then chances are more that user opens the mail [10].

2. *Anti-Phishing Toolbars*

These toolbars identifies the genuine websites from the fraudulent ones by making use of blacklist, whitelist and heuristics to identify the difference between the URLs. Examples of anti-phishing toolbars are McAfee site advisor, Google safe browsing, spoofgaurd, eBay Toolbar etc. [11][19]. Spoofgaurd relies on heuristics of URLs to verify the URL. The disadvantage with these are sometimes they report good URL as fraudulent and vice-versa. The disadvantage with these toolbars are they become impossible to maintain as whitelisted website can be many. Password protection Mechanisms are

1. PwdHash++

"V. Reddy, V. Radha and M. Jindal in their paper, 'Client Side protection from Phishing Attack', compared these various anti-phishing tools. They evaluated tools based of certain factors like application type, hashing algorithm, password strength, spoof proof, visibility to web page, visibility to user, and concluded Pwdhash as the most secure tool for passwords protection" [14]. The disadvantages with pwdHash are invisibility of running app to user, visibility of the activation of app to webpage. PwdHash++ was introduced to address this problem [12]. This method verifies the authentication of the website by checking the address of popup page and by verifying the custom image of the website which provider provides. Then user can login to the site and the password is hashed with the site domain name using MD5, which is irreversible and cannot be accessed through javascript.

2. Hashing with Salt Value

In this the password of the user is hashed after including the salt in the user's password. Which makes this technique more advanced than MD5. [14] Because it is easy for the hacker to get the domain name of the site than the salt which the user introduces.

3. Moody Keyboard

Moody Keyboard is a keyboard with multi-color LED lights and a help button which warns the user about one's activity when user tries to access the website which is not encrypted and also when using credit card details over unsecured network.

4. One-Time Password (OTP)

OTP uses a reliable communication channel on the demand of the user. This method sends the password to the users via text message, mail, call etc., these passwords lasts only for a specified period of time. Delivering OTP using instant messaging is that password is delivered to the user via instant messaging and uses the already available web based methods to form a communication channel. Disadvantage is that it is not fully secured. With proper configuration and design this can be proved to be efficient [5]. It is a two-step process i.e, registration and authentication. OTP can be sent to the user in both of the steps and only for limited number of times in order to reduce the chances of security vulnerability. The registration is similar to the regular registration process but user has to login with anyone of IM service [15][23].

IV. INDIVIDUAL WORK – WEAK PASSWORDS

As the project work deals with the possible attacks on passwords and techniques used to solve them, I worked on analyzing the weak password. Studied papers on graphical password as an alternative to weak password. The main problem with the weak password is the Password Problem.

1. Password problem

Password are the easiest way for a hacker to get control of the system as they depend on the weakest link of the security chain "Human". The "password problem", as given by Birget in [25][24], arises because passwords are expected to comply with two conflicting requirements. They are:

1. "Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans" [25].
2. "Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text" [25].

While choosing alpha numeric passwords (min. of 8 characters and combination of lowercase, uppercase, digits and special characters) user tends to compromise one of the requirements which results in "weak passwords", prone to dictionary attack, brute force attack and soon. Some of the reasons why users tend to compromise are limitations to human's long term memory, users might be having a number of accounts, user might not be using account from long time and some accounts need password to be changed periodically for the sake of security. One of the solution to password problem is "Graphical Passwords".

2. Graphical Passwords

In graphical passwords user selects a series of images from the images displayed on series of screens in Graphical User Interface (GUI). This is also known as Graphical based user authentication. The displayed images might be most common objects like fruits, places, animals, human faces etc. Graphical passwords are easier and more secure than text passwords because they are easy to memorize and difficult for the hacker to hack them. Graphical passwords are vulnerable to Brute force attack, Dictionary attacks, Guessing, Spy-ware, Shoulder surfing and social engineering. Graphical Passwords are broadly classified into 4 categories:

1) *Recognition based Systems* – In this type of systems, user first selects a sequence of images during registration phase. In authentication phase user has to recognize the selected set of images in the same order [26].

Examples:

Déjà vu (Hash Visualization Technique) - During authentication, user has to select previously seen images.
Pass-Objects (Deals with shoulder surfing) - To be authenticated, user has to recognize pass-objects and click inside the convex hull formed by pass-objects.

2) *Pure Recall based Systems* – In this type of systems, user has to draw an image or a sketch on a grid. Grid points are stored into the database during registration. User has to redraw the image or sketch to get authenticated [26].

3) *Cued Recall based Systems* – Similar to Pure recall based systems but a clue can be selected during registration and can be used during authentication.
Examples:
Passlogix - During authentication, user has to draw password in the same grid and in same sequence
Draw-A-Secret (DAS) - To be authenticated, user has to draw the sketch in the grid as one did during registration phase in the same order.
PassPoints - To be authenticated user has to click on the region and in the same order as one did during registration [27].

4) *Hybrid Systems* – A combination of one or more of the above systems. Hybrid system is a combination recognition based system and recall based system. According to [30] hybrid system is an approach towards more reliable, secure, user-friendly, and robust authentication.

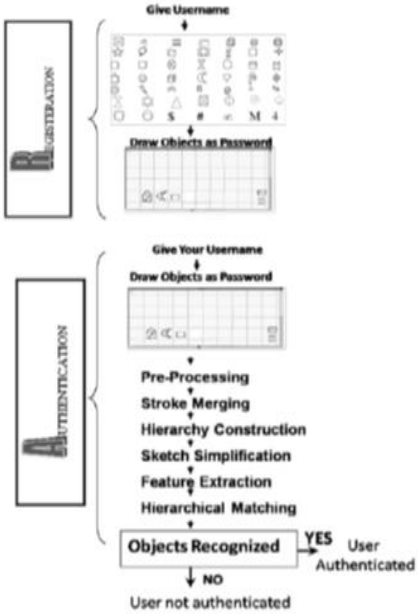

Figure 2 Graphical Representation of Hybrid system [30]

*Working of Hybrid System: "*This system comprises of 9 steps. Steps1-3 are registration steps and steps 4-9 are the authentication steps. The first step is to type the user name and a textual password which are stored in the database. During authentication user has to give that specific user name and textual password in order to log in. In second step objects are displayed to user and he selects minimum of three objects from the set and there is no limit for maximum number of objects, by using one of the recognition based schemes. The selected objects are then drawn by user, which are stored in database with the specific username. Objects may be symbols, characters, auto shapes, simple daily seen objects etc. In third step during authentication, user draws pre-selected objects as his password on a touch sensitive screen with a mouse or a stylus. This will be done using the pure recall based methods. In fourth step, the system performs pre-processing. In fifth step, the system gets the input from user and merges strokes in the user drawn sketch. In sixth step, after stroke merging, system constructs the hierarchy. Seventh step is sketch simplification. In the eighth step three types of features are extracted from the sketch drawn by the user. The last step is called hierarchical matching". As shown in Figure 2 [30].

Security Analysis: "The hybrid system is less vulnerable to brute force attack as the password space is large. It is also less vulnerable to dictionary attack, as if user tends to maintain weak text password, the graphical password makes the password strong and cannot be guessed. It overcomes the problem of shoulder surfing as a combination of techniques are used, even one is compromised it is hard for the hacker to guess other one. Social Engineering also does not work with this method as images are used. User cannot note down the password or even cannot not share the password "[30].

Advantages: Hybrid system is resistant to all the possible attacks on graphical passwords. People who are face-blind can also use this method as objects are used as images.
Disadvantages: This system also suffers from inherent weakness of graphical passwords i.e., people with poor vision, poor motor control, and color blindness cannot use graphical passwords effectively. As other graphic password schemes, this method is also slow as it takes more time for normalization and matching.

V. CONCLUSION

As mentioned, passwords are the most important to access the system especially in this internet age. As there are a number of security measures to protect the system similarly there are a number of ways in which

one can hack the system. We discussed the mentioned three threats and counter measures for the threats. After analyzing the techniques for the phishing attack, hacking and weak passwords. The promising one among the counter techniques will be OTP via IM based on security analysis, resources like memory, time and usability.

REFERENCES

[1] Chun-Ying Huang; Shang-PinMa; Kuan-TaChen, Using one-time passwords to prevent password phishing attacks. Journal of Network and Computer Applications 34(2011)1292–1301.

[2] Justin Cappos. PolyPasswordHasher: Protecting Passwords In The Event Of A Password File Disclosure http://polypasswordhasher.github.io/PolyPasswordHasher/.

[3] K.Aravindhan; R.R.Karthiga, One-time Password: A Survey. International Journal of Emerging Trends in Engineering and Development. Issue 3, Vol.1 (January 2013). ISSN 2249-6149.

[4] http://www.phishtank.com/S. URL:/http://www.phishtank.com/S.

[5] DhamijaR, TygarJD, Hearst M. Why phishing works.In:CHI'06:proceedings of the SIGCHI conference on Human factors in computing systems. NewYork,NY, USA: ACM;2006.p.581–90.

[6] Khaled Alghathbar Hanan A. Mahmoud (hanan.hosni@coeia.edu.sa), Noisy Password Scheme: A New One Time Password System, Center of Excellence in Information Assurance, King Saud University, Riyadh, Kingdom of Saudi Arabia [2010].

[7] Minakshi Bhardwaj, G.P Singh, Types of Hacking Attack and their Counter Measures, International Journal of Education Planing& Administration, Volume 1, Number 1 (2011), pp. 43-53, Research India publications, http://www/ripublication.com/ijepa.htm.

[8] Adeka, M.; Shepherd, S.; Abd-Alhameed, R., "Resolving the password security purgatory in thecontexts of technology, security and human factors", Computer Applications Technology (ICCAT), 2013International Conference on DOI: 10.1109/ICCAT.2013.6522044, Publication Year: 2013, Page(s): 1-7. K

[9] Khaled Alghathbar (ghathbar@coeia.edu.sa), Hanan A. Mahmoud (hanan.hosni@coeia.edu.sa), Noisy Password Security Technique, Center of Excellence in Information Assurance, King Saud University, Riyadh, Kingdom of Saudi Arabia [2010].

[10] Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd "Reducing Shoulder-surfing by Using Gaze-based Password Entry," Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.

[11] Reddy, V.P.; Radha, V.; Jindal, M. Client Side protection from Phishing attack. International Journal for Advanced Engineering Sciences and Technologies 3.1 (2011):39-45.

[12] Khayal, S.H.; Khan, A; Bibi, N.; Ashraf, T.Analysis of password login phishing based protocols for security improvements. Emerging Technologies, 2009. ICET 2009. International Conference, Serbia, 19-20 Oct. 2009.

[13] Ross, Blake, Collin Jackson, Nick Miyake, Dan Boneh, and John C. Mitchell. "Stronger Password Authentication Using Browser Extensions." 14th USENIX Security Symposium — Technical Paper. N.p., n.d. Web. 13 Oct. 2014.

[14] Luca A. D., Frauendienst B., Maurer M., Seifert J., Hausen D., Kammerer N., Hussmann H,. 2011. Does MoodyBoard make internet use more secure?Evaluating an ambient security visualization tool. In Proceedings of the 2011 annual conference on Human factors in computing systems (CHI '11). ACM, New York, NY, USA, 887-890.

[15] Agarwal, V. K.; Bharti, B. T.; Parihar, B. Password Authentication with Secured Login Interface at Application Layer. International Journal of Computer Science and Network Security 14.9(2014):82-85.

[16] Zeydan, H. Z.; Selamat, A.; Salleh, M. Study on Protection against Password Phishing. World Applied Sciences Journal 35:5 (2014):797-801.

[17] Gouda, M.G., Liu, A.X., Leung, L.M., Alam, M.A.; SPP: An anti-phishing Singlepassword protocol. Computer Networks 51(13), 3715–3726 (2007).

[18] Wu, Y.; Zhao, Z. "Enhancing the security of Online Transaction with CAPTCHA Keyboard". Information Security and Privacy Research 376(2012):531-536.

[19] Levenshtein Distance (n.d.). In Wikipedia. Retrieved November 5, 2014, from http://en.wikipedia.org/wiki/Levenshtein_distance

[20] Balaji. R, Roopak. V, "DPASS: Dynamic password authentication and security system using grid analysis", Electronics Computer Technology (ICECT), 2011 3rd International Conference on, vol.2, no., pp.250-253, 8-10 April 2011.

[21] http://cacm.acm.org/news/177328-new-protection-scheme-makes-weak-passwords-virtually-uncrackable/fulltext.

[22] Justin Cappos. PolyPasswordHasher: Protecting Passwords In The Event Of A Password File

Disclosure http://polypasswordhasher.github.io/PolyPasswordHasher/.
[23] http://engineering.nyu.edu/press-release/2014/07/29/crack-password-not-billion-years.
[24] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. Authentication using graphical passwords: Basic Results. Proc. Human-Computer Interaction International 2011, in press.
[25] Ahmad Almulhem, "A Graphical Password Authentication System", World Congress on Internet Security (WorldCIS-2011), London, UK, February 21-23, 2011.
[26] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing", 2010 International Conference on CyberWorlds, Singapore, 20-22 October 2010.
[27] Wei Hu,Xiaoping Wu, GuohengWei, "The Security Analysis of Graphical Passwords" International Conference on Communications & Intelligence Information Security, 2010.
[28] Elizabeth Stobert, Robert Biddle, "The Password Life Cycle:User Behavior in Managing Passwords".
[29] Wazir Zada Khan, Mohammed Y Aalsalemand Yang Xiang. "A Graphical Password Based System for Small Mobile Devices"IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011.
[30] MohdJali, Steven Furnell, and Paul Dowland, "Quantifying the Effect of Graphical Password Guidelinesfor Better Security"