The Knowledge Based Authentication Attacks

Farnaz Towhidi[1], Azizah Abdul Manaf[1], Salwani Mohd Daud[1], Arash Habibi Lashkari[1]

[1]Advanced Informatics School, Universiti Technologi Malaysia (UTM), Kuala Lumpur, Kuala Lumpur, Malaysia

Abstract - *Knowledge Based authentication is still the most widely used and accepted technique for securing resources from unauthorized access for its simplicity, ease of revocation and legacy deployment which divides to textual and graphical password. Over the last decade several attacks records for stealing user's identity and confidential information using a single or combination of attacks. In this paper the attacks pattern of textual and graphical password describes according to CAPEC standard, following describing their effects on both conventional and image password. More over some categories lacks from detail research which highlighted and will select as future work.*

Keywords: Authentication Attack, Graphical Password Attacks, Knowledge Based Attacks, Recognition Based Attacks, Recall based Attacks.

1 Introduction

The tradeoff between security and usability of knowledge based authentication schemes was always a topic for experts. Although textual password is still use as an entrance in most secure environments, graphical password has been selected as an alternative due to the drawbacks of textual password. The image password is classified into three categories: Recognition Based; Pure Recall Based and Cued Recall Based [1].

These recognition categories provide a gallery of faces, objects, random arts or icons for users and some of them can be selected as the user's password. In pure recall based or draw based [2], the user needs to draw a shape or signature in an empty grid as password. For the other category, cued recall based or click based, the system provides user special facilities to remember his password, for instance in Passpoint algorithm, the user is given a chance to select some points in the background image as his passwords. [2-4].

The Common Attack Pattern Enumeration Classification's (CAPEC) Release 1.6, defines and describes the common attack pattern along with the observation of the Department of Homeland Security, which will be used to help users find the subset pattern of enumeration. In this paper, the attack pattern of knowledge based authentication are as follow:

2 Password Brute Force

Also known as exhaustive search or guessing attack, it uses "Probabilistic Techniques" as a method of attack. Probabilistic technique shows that when one object is selected randomly from a class of objects, the probability that the result would be the same as the desired result is more than zero, so password brute forcing works by an attacker who uses trial and error method to explore all possible passwords of the user [5].

In textual password brute forcing, the attacker should trying millions of passwords by testing every combination of letters, digits, special symbols and punctuation symbol until a password is found. So, an attacker will require years, and in some cases hundreds or thousands of years, to completely reveal a password. In the recognition category of graphical password, when the attacker physically accesses the database of pictures, this attack is possible using the trial and error using stolen images. In draw based, an attack can be launched using smart programs to automatically generate accurate mouse motion to imitate human [2].

To prevent successful attacks, password management policies can force user to change his password before a brute force attack managed to check all possible combinations. This attack has two different versions which use brute force as a method for attacking, namely "Dictionary Based Password Attack" and "Rainbow Table Password Attack" with the following description [5].

2.1 Dictionary Based Password Attack

This is one of the branches of brute force attack which the attacker creates a dictionary of textual or graphical possible password, and then tries to compromise an account with one user name and the passwords in the created dictionary [5].

In textual password, the attacker creates a dictionary of memorable words like dates of birth as passwords. On the other hand, there are also several free wordlists or software tools that automate dictionary attacks [6]. In click based graphical password, the attacker creates a dictionary of popular spots of image or points which can attract the user. There are several algorithms which show the visual attention of user like "Bottom up" and "Top down". In Bottom up, the human attention goes towards "hotspots" or "salient" which are recognizable shapes, bright colors, or objects that are more likely to be selected [7-9]. In top down visual search,

humans control his attention by searching for a specific thing in a picture [9-10]. When the dictionary is created, attacker uses software to check the login page for one username and hundreds of password in the dictionary.

To prevent this attack, a mechanism named CAPTCHA needs to identify whether the password is entered by the user or by an automated program. The Captcha is a challenge response program that generates a test to identify whether the third party is a human or a system. This test can be solved easily by the user but hard to bypass by a system [11].

2.2 Rainbow Table Password Attack

Nowadays administrators try to save the password of users in hash form. If the attackers want to find the plain text of hash value, he has two choices. One is to calculate the hash value of many plain texts to find the same hash which might take a long time. Or the other choice is pre computing the hash of billions of passwords and store them in a Rainbow table in order to find the correct password [12]. These tables take a very long time and uses large space to generate, but once the attacker has the tables, it facilitates attacks by cracking a large number of passwords in a second. The main idea of the rainbow table is using chain of hashing and reduction function. A hash function maps the plaintexts to hashes, and the reduction function reduces the length of hash function to a fix value. The chain of rainbow table starts with a plaintext and finishes with a hash value.

To prevent the risk of Rainbow table, the administrators adds a random character named salt before hashing. The salt value is stored in the database for each user. During every authentication, a new challenge is generated by the server, the Rainbow tables need to either include all the salt combinations which would make them unmanageably large, or recalculate the table every time which makes them similar in terms of efficiency to brute force attacks [12]. In this situation, the attacker needs to find the correct salt for each of his hashing which makes the process much too long. If the selected salt key is long enough, compromising the password would be much harder for the attacker [12-13].

3 Sniffing Attack

Sniffing uses the weakness found in design of application to reveal more information to the intruder than what it intends to show by using sniffer to monitor and eavesdropping the input or output data [5, 14-15]. In textual password, the user starts to send “Towhidi7958F” as his password which transferred in sequence of packets. The packets go up and down through network along with the packet’s destination address to show which computer is permitted to accept it. At the same time the attacker uses a sniffer software to change the configuration of his Network Interface Card to a promiscuous mode to collect all these packets [14]. In Recognition based Graphical Password, the attacker can sniff the ID of image password. This ID is usable only if user can attack the image gallery at the same time. No research has found the impact of sniffing attacks on click based and draw based algorithms.

To protect from password sniffing attacks, sensitive information must be properly encrypted [16], another choice is using “IP Security Protocol (IPsec)” that secure data in the network layer by authenticating and encrypting each packet in communication [17].

4 Spoofing Attack

The attacker uses various techniques like Action Spoofing, Content Spoofing, or Identity Spoofing to masquerade his message as a legitimate one in order to trick user. In “Action Spoofing” the attacker changes the mechanism of actions to lead victim to a wrong way. For instance the user thinks by clicking on the return button of the page, he will redirect to the home page but in return, an executable file is run by attacker. In “Content Spoofing”, the attacker changes the contents of one page to show his messages rather than the original one. For instance in the bank portal, the attacker change the account number of bank to his. In the “Identity Spoofing”, the attacker impersonates a legitimate user.

A computer may be protected from this attack by restricting the IP addresses that sends data. A router may have a list of IP numbers and it allows only data from these numbers to enter the computer. So if the attacker gains the IP list, he can start sending data that appears to come from a legitimate IP address. But when the attacker do not have the list, he starts to send packets with consecutive IP numbers until a packet gain one of allowed IP in the list, which in this case the packet gains access to computer [15]. Identity Spoofing have several subsets like “Man in the Middle Attack” and “Phishing Attack” as follow [5].

4.1 Man in the Middle Attack

Derive from basketball, when two player want to pass a ball to each other, another player interrupts the passing ball without prior knowledge [18]. In the man in the middle attack (MITM), the intruder uses spoofing method by sitting somewhere between the client and the server and starts sniffing packets or even alter message from first party and send the changed message to the second, so although the two parties thought they are directly talking to each other, the attackers actually control all the conversation without any sign [5, 19]. In case of successful MITM, the attacker can have several consequences like DNS poisoning, denial of service attack or even Https sniffing. In case of sniffing, any textual or graphical password can be observed by the intruder, especially when data transfer in TCP protocol as data are transferred without any encryption [18].

To protect password against such attacks, hashing password, multi factor authentication, digital certificate, channel encryption, and integrity protection is recommended [20].

4.2 Phishing Attack

Phishing is the act of stealing a user's confidential information by pretending to be a legitimate entity. For example, an attacker design a fake website exactly like a bank's portal, then starts to send out a spam e-mails to a large random number of users trying to convinces the user to visit the cracked website and enter their account number and password. The method of convincing user can done by social engineering techniques like telephone call, SMS, and so on. [20-22].

In graphical password under the click based category, phishing is possible by creating a faked login page and simulating the area for drawing password. Once the user draws his password, the sketch can be used in the legitimate website. During recognition, the username is retrieved by the faked website, and then it will be passed to the legitimate website for retrieving the correct image gallery. Again this gallery is shown to the user in the faked website which causes the user to select the password [2]. Even click based can be simulate in phishing website, for instance the attacker can include the background images in the login page, when the user starts to click on special point of picture as his password, the area of password is revealed to the attacker.

Using "List Based" technique is recommended for mitigating this attack which divides to black list and white list. The black list contains the list of all phishing website which gathered by web crawlers or list maintainers but these list are helpful only if their data is accurate and fresh. The white list on the other hand includes the list of all trusted domains. So by visiting any website that does not record in white list, an alert message will be shown to the user [22].

5 Exploitation of Authentication

In the case that user does not have username and passwords; there are several methods for exploitating authentication like "Authentication Bypass" and "Exploitation of Session Variables, Resource IDs and other Trusted Credentials". The description of these two password attacks are as a follows:

5.1 Authentication Bypass

In this attack the attacker can gain access to resources, application, service and credential information with the privilege of an authorized person [5]. For instance an intruder can firstly gain physical access to local computer and then change the setting to administrator privilege. This privilege bypass all authentication for accessing files and folders [6]. In web application, most financial systems have authentication page as the heart for entering secure transactions. In some cases, the attacker bypasses the authentication page and directly type the URL of the page which will show after authentication.

5.2 Exploitation of Session Variables, Resource IDs

"Session Side Jacking" is a sort of Exploitation of Authentication by exploiting session variable and resource ID [5]. This attack controls the communication channel of two endpoints. When the user establishes a new session and authenticate successfully, the attacker can assume the identity of this user, and then install a Trojan horse on the target's computer to watch the activity and records user names and textual or graphical password. If the data transfer is in a "Secure Socket Layer", the attacker cannot intercept the data, otherwise the data can be captured and then "Session Replay" by the attacker [15].

In "Session Replay" or "Authentication Replay" the user steals a valid session ID or password and reused it again to gain privilege. Authentication replay is mostly used when the user uses encrypted password. For instance, suppose one client usually sends an encrypted string to the server that provides for user authentication, this encrypted string can be captured by the attacker and presented to the server by the attacker. Authentication schemes that use static authentication parameters are susceptible to password replay attacks.

Many authentication protocols uses a challenge-response mechanisms for user authentication like when the authenticator generates a random string and present it as a challenge to the supplicant. The supplicant will typically manipulate the server challenge in some way and will typically encrypt it using the user password or a derivative as the key, or generate a hash based on the challenge and the user password. In any case, the user plaintext password will be used by the client to generate a response to the server challenge. If an attacker manages to capture a challenge-response authentication session, he may be able to see the encrypted supplicant response that depend on the server-provided challenge.

6 Social Engineering Attacks

This is one of the oldest attacks that simply involves psychological and technical methods of tricking the user into believing that he needs to provide his confidential information.

Text based password can be easily described or written down on a paper or even describe verbally, so social engineering can easily lunch in this sort of authentication [2]. For graphical password, describing password by telephone or email is harder than conventional passwords because verbalizing a click points in a picture or even drawing shape is very hard. For instance in Passpoint scheme, explaining the exact click point of a user is very hard since there are millions of available spots in a picture. A research on Passface

graphical password shows although the algorithm is vulnerable to description attack, a wise choice of decoy pictures can increase or decrease its vulnerabilities [23].

Countermeasure of this attack is very hard because it does not relate to any bugs or weakness in the system. Since the weakest link in any security system is humans, using users awareness training and security policies and procedures is highly recommended [24-25].

7 Physical Security Attacks

When an attacker has physical access to a computer, there is a chance of bypassing authentication and easily get access to resources even without authenticating. In case of physical attack of textual or even graphical password, an attacker can steal the password database from the server and launch offline attacks against it. For instance in the recognition category, the image password of the user is stored in the database, so anyone who gain access to the password bank can retrieve the credential information [5].

Although preventing security attack is hard, cryptography may be the solution to mitigate the risks of such attacks by encrypting password in database using a key. The key should be stored in a different computer to prevent an attacker from accessing information.

8 Shoulder Surfing Attack

The attacker tries to use direct observation like looking over the user's shoulder, using binoculars or even closed-circuit television cameras for capturing user's credential. For instance, this attack happens when user try to enter his password using the keyboard, mouse or even touch screen [26]. Graphical password schemes are more vulnerable to shoulder surfing than textual passwords [27]. In the recognition category, some of the algorithms design a challenge response method to resist this attack which forces the user to not clicking directly on password. For instance, the triangle algorithm , CDS Algorithm [28], DWT algorithm [29] and color login algorithm [30]. In the click based category, the attacker needs to capture exactly the position clicked by mouse in the image. Also in the draw based scheme, the process of drawing password is entirely visible to the attacker to memorize or even record [31]

To prevent this attack, users should make sure that no one is looking behind them when they are typing their passwords or even shielding the keypad from view by using their body or cupping their hands. [6].

9 Conclusion

Nowadays security of authentication remains an issue of paramount importance to verify the identity of person or process. Among various methods of authentication like biometric, smartcards and password authentication, textual and graphical password have been used for centuries and still remain the most popular mechanism. This paper reviews the common attacks of knowledge base authentication and the reflection in textual and graphical password.

On the other hand the limitation of human memory on memorizing strong and secure textual password led to focusing more on the security of graphical password. In the future the attacks on graphical password will describe in detail.

10 Acknowledgement

This paper is supported by project UTM-J-13-01/25.10/3/02H07(1) from Research University Grant (RUG) of University Technology Malaysia (UTM).

11 References

[1] Farmand, S. and O.B. Zakaria, Impro Passwving Graphicalord Resistant to Shoulder-Surfing Using 4-way Recognition-Based Sequence Reproduction (RBSR4), in The 2nd IEEE International Conference on Information Management and Engineering. 2010: Chengdu, China.

[2] Biddle, R., S. Chiasson, and P.C.v. Oorschot, Graphical Passwords: Learning from the First Generation. 2009: Ottawa, Canada.

[3] Towhidi, F. and M. Masrom, A Survey on Recognition-Based Graphical User Authentication Algorithms. International Journal of Computer Science and Information Security (IJCSIS) 2009. 6(2).

[4] Masrom, M., F. Towhidi, and A.H. Lashkari, Pure and Cued Recall-Based Graphical User Authentication, in The 3rd International Conference on Application of Information and Communication Technologies (AICT2009). 2009: Azerbaijan, Baku.

[5] CAPEC-Release1.6, Common attack Pattern Enumeration and Classification: http://capec.mitre.org.

[6] Todorov, D., Mechanics of User Identification and Authentication. 2007: Taylor & Francis Group.

[7] Oorschot, P.C.v., A. Salehi-Abari, and J. Thorpe, Purely Automated Attacks on PassPoints-Style Graphical Passwords. IEEE Transactions on Information Forensics and Security, 2010. 5(3): p. 393 - 405

[8] Thorpe, J. and P.C.v. Oorschot. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. in 16th USENIX Security Symposium on USENIX Security. 2007. CA, USA.

[9] LeBlanc, D., et al., Can Eye Gaze Reveal Graphical Passwords?, in ACM Symposium on Usable Privacy and Security (SOUPS). 2008, ACM: Pittsburgh, USA.

[10] Henry, P.T., Toward usable, robust memometric authentication: An evaluation of selected password generation assistance, in College of Information. 2007, Florida State University. p. 207.

[11] Wang, L., et al., Against Spyware Using CAPTCHA in Graphical Password Scheme. 2010.

[12] Thorpe, J., *On the predictability and security of user choice in password*, in *Computer Science*. 2008, CARLETON UNIVERSITY: Ottawa, Ontario. p. 197.

[13] S. H. Khayal, et al., *Analysis of Password Login Phishing Based Protocols for Security Improvements*, in *International Conference on Emerging Technologies, 2009. ICET 2009.* . 2009, IEEE. p. 368 - 371.

[14] Qadeer, M.A., et al., *Bottleneck analysis and traffic congestion avoidance*, in *Proceedings of the International Conference and Workshop on Emerging Trends in Technology*. 2010, ACM: Mumbai, Maharashtra, India. p. 273-278.

[15] Salomon, D., *Network Security*, in *Elements of Computer Security*. 2010, Springer London. p. 179-208.

[16] Spangler, R., *Packet Sniffer Detection with AntiSniff*. 2003.

[17] Yin, H. and H. Wang, *Building an application-aware IPsec policy system.* IEEE/ACM Trans. Netw., 2007. **15**(6): p. 1502-1513.

[18] Nayak, i.N. and S.G. Samaddar, *Different flavours of Man-In-The-Middle attack, consequences and feasible solutions*, in *3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)* 2010, IEEE: Chengdu p. 491 - 495

[19] YUAN, X., et al., *Visualization Tools for Teaching Computer Security*. 2010, ACM.

[20] Joshi, Y., D. Das, and S. Saha, *Mitigating Man in the Middle Attack over Secure Sockets Layer*. 2009.

[21] Butler, R., *A framework of anti-phishing measures aimed at protecting the online consumer's identity.* 2007.

[22] Huang, C.-Y., S. PinMaa, and K. TaChen, *Using one-time passwords to prevent password phishing attacks.* JournalbofbNetworkbandbComputer Applications, 2010.

[23] Dunphy, P., J. Nicholson, and P. Olivier, *Securing Passfaces for Description.* 2008.

[24] Sandouka, H., A. Cullen, and I. Mann, *Social Engineering Detection using Neural Networks*, in *2009 International Conference on CyberWorlds*. 2009, IEEE.

[25] al, A.A.G.e., *Network Attacks*, in *Network Intrusion Detection and Prevention: Concepts and Techniques*, Springer Science, Business Media.

[26] Kumar, M., et al., *Reducing Shoulder-surfing by Using Gaze-based Password Entry*, in *Symposium On Usable Privacy and Security (SOUPS)*. 2007: Pittsburgh, PA, USA.

[27] Tari, F., A.A. Ozok, and S.H. Holden, *A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords*, in *Symposium On Usable Privacy and Security (SOUPS)*. 2006: Pittsburgh, PA, USA.

[28] Gao, H., et al., *A New Graphical Password Scheme Resistant to Shoulder-Surfing*, in *International Conference on Cyberworlds*. 2010, IEEE: Singapore p. 194 - 199

[29] Hasegawa, M., Y. Tanaka, and S. Kato, *A Study on an Image Synthesis Method for Graphical Passwords*, in *International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2009)*. 2009.

[30] Gao, H., et al., *Analysis and Evaluation of the ColorLogin Graphical Password Scheme*, in *Fifth International Conference on Image and Graphics (ICIG)*. 2009, IEEE. p. 722 - 727

[31] Lashkari, A.H., et al., *Shoulder Surfing attack in graphical password authentication.* International Journal of Computer Science and Information Security, 2009. 6(9).