Security Analysis of Graphical Passwords Over the Textual Passwords for Authentication

S. B. Dandin
Dean (Dept. of CS/IT) BKBIET
Pilani, Rajasthan, India

Manwinderkaur
Dept. of JOINT MASTER'S
PROGRAMME, BKBIET
Pilani, Rajasthan, India

Akanksha Tiwari
Dept. of JOINT MASTER'S
PROGRAMME, BKBIET
Pilani, Rajasthan, India

***Abstract:-* Securityis the state of being free from danger or threat or errors.In case of computers and workstation, security is applied or measured through passwords. So far, we are using textual passwords. Textual passwords are string of characters (which may include numbers or special characters). These textual passwords are widely and mostly used. But they are not totally or fully secured. Therefore, we face security issues by using this scheme of textual passwords.**

In our paper, a security Analysis of Graphical Passwords over the Textual Passwords through various schemes of graphical user authentication is analyzed.

Here proposed graphical authentication scheme is implemented as an alternateto text-based authentication systems, various analysesare made and also severalchallenges in graphical authentication are discussed.

Index Terms: Textual Passwords, Graphical Password, Issues, Security.

I. INTRODUCTION

PASSWORDS provide security mechanism forauthentication and protectionservices against unwanted access to resource.The most common approach forauthentication is

text passwords. Text password is simply a string of letters and digits. They are versatile and easy to implement and use. Textualpasswords are required to satisfy two contradictory requirements. They have to be easily remembered by auser, while they have to be hard to guess by impostor[1]. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary andbrute-forced attacks [2,3]. Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-rememberpasswords on sticky notes exposing them to direct theft [4]. Patrick, et al. [5]pointed out three major areas where human-computer interaction is important authentication, developing secure systems and security operations.According to a news article on Computerworld, a network password cracker was run by a security team at a large company and within 30 seconds, they were able to identify about 80% of the passwords [6]. Studies showed that since user can only remember a limited amount of different passwords, they tend to use the same passwords for different accounts or write them down [7]. To counter the inherent problems with traditional username/password authentication, various alternative authentication methods, such as biometrics, have been used. In this paper, however, we focus on graphical user authentication which is nothing but utilizing images as passwords. Graphical authentication schemes have been proposed as a possible alternative to replace the traditional username/password authentication schemes. It is motivated partially by the fact that humans are capable of remembering pictures or images better than texts; even psychologicalstudies supports such assumption [8]. Pictures orimages are generally much easier to be remembered or recognized than that of textual objects. In addition to memorability, if the number of possible pictures or images is significantly large, then the possible password space of a graphical password scheme may exceed that of text based schemes and thus might be able offer better resistance to dictionary attacks than text based schemes.

II. TEXTUAL AUTHENTICATION

The most common computer authentication method is to use alphanumerical username and passwords. Textual-based password authentication scheme tend to more vulnerable to attacks such as shoulder-surfing and hidden camera. To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text-based scheme. Because simply adopting graphical password authentication also has some drawbacks.

The main drawback of passwords is what we call the password problem, namely the fact that passwords are expected to comply with two conflicting requirements:

(1) Password should be easy to remember, and user authentication protocol should be executable quickly and easily by humans.

(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.

III.GRAPHICAL PASSWORD

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). Graphical passwords may be a solution to the ***password problem***. The idea of graphical passwords, first described by Greg Blonder [G. Blonder, Graphical Passwords, United States Patent 5559961 (1996)], is to let the user click (with a mouse or a stylus) on a few chosen regions in an image that appears on the screen. To log in, the user has to click in the same regions again.

In Blonder-style graphical passwords, onlypre-processed images can be used. The click regions can only be chosen from certain pre-designed regions in the image. This implies that the users cannot provide images of their own for making passwords, and users cannot choose click places that are not among the preselected ones. Our design allows the use of any images (including the users own images, digital photos of landscapes, paintings, etc.). Moreover, we let users choose any places that attract them as click regions; such places are easier to remember. However, allowing arbitrary click locations lead to a stability problem, which we had to overcome. The problem is that we cannot expect users to click always on exactly the same location (when they intend to). So we discretize the image, by using a square grid. But that leads to border problems: If the chosen click location is near the edge of a grid-square, the user will sometimes click in one square, sometimes in a neighboring square. We devised a multi-grid method, which we call robust discretization, and which leads to a stable output for the user's clicking actions. An approximation parameter r is used; as long as the user clicks within distance r of the originally chosen click location, the output of the clicking will be the same (e.g., r=2 mm).It is important to have stable output, because the output of the discretized clicking will undergo a secure hash (“password encryption”) for security reasons, we do not store the actual graphical password in the computer, just the hash value. So, the system does not know the graphical password explicitly and hence cannot check whether a user's clicks are “approximately correct”. The hashing of passwords leads to the requirement that the user's clicks at login must always be in the same multi-grid squares; hence, we need a robust discretization.

Figure: Displaying Click-Points

We have implemented the graphical password system described in the above paper; the implemented version is called PassPoints. For passwords, human aspects (usability of the system, learnability and long-term memorability of the passwords, avoidance of unsafe practices, and user satisfaction) are of crucial importance.

III.SECURITY ANALYSIS FOR GRAPHICAL PASSWORD

Enough research is yet to be undertaken to study the difficulty of cracking graphical passwords. As graphical passwords are still not widely used in real world applications, there is no report on real cases of breaking graphical passwords. Here we briefly examine some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

A. Brute force search:

Brute-force attacks are simple to understand. An attacker has an encrypted file say, yourLastPass or KeePass passworddatabase.

They know that this file contains data they want to see, and they know that there’s an encryption key that unlocks it. To decrypt it, they can begin to try every single possible password and see if that results in a decrypted file.They do this automatically with a computer program, so the speed at which someone can brute-force encryption increases as available computer hardware becomes faster and faster, capable of doing more calculations per second. The brute-force attack would likely start at one-digit passwords before moving to two-digit passwords and so on, trying all possible combinations until one works.

The main defense measure against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94N, where N is the length of the password, 94 is the number of printable characters (shift and non-shift keys excluding SPACE) on a standard keyboard. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords [9]. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs needto automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, in terms of brute force attacks, it is believed that a graphical password has less vulnerability than a text-based password.

B. Dictionary attacks:

A “dictionary attack” is similar and tries words in a dictionary or a list of common passwords instead of all possible passwords. This can be very effective, as many people use such weak and common passwords.

It is impractical to carry out dictionary attacksagainst graphical passwords as recognition based graphical passwords involve mouse input instead of keyboard input. For some recall based graphical passwords [10], it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More researchis needed in this area. However, it is evident that graphical password has less vulnerability to dictionary attacks than text-based passwords.

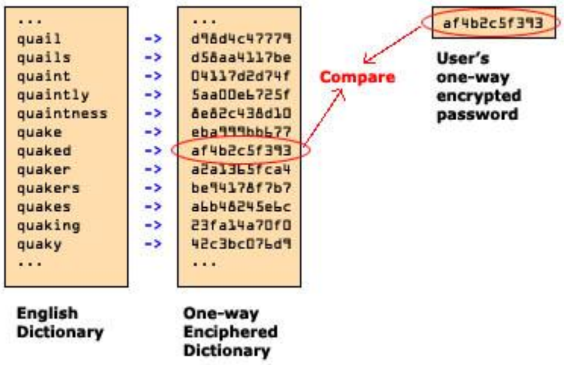
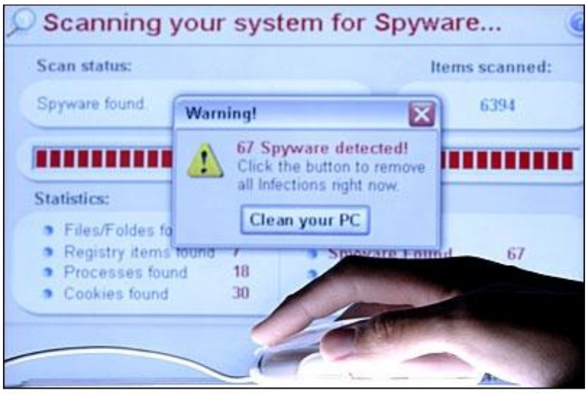


Fig: Dictionary Attack

C. Spyware:

Spyware is infiltration software that secretly monitors unsuspecting users. It can enable a hacker to obtain sensitive information, such as passwords, from the user's computer. Spyware exploits user and application vulnerabilities and is often attached to free online software downloads or to links that are clicked by users.

Except for few cases, key listening or key logging spyware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spyware will be an effective tool against graphical passwords. However, motion of the mouse alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window location, its position and size, as well as desktop resolution and size also matters.


Scanning your system for Spyware...

Scan status: Items scanned:

Spyware found 6394

Warning!

67 Spyware detected!
Click the button to remove all infections right now.

Clean your PC

Statistics:

- Files/Foldes fo
- Registry items found 7 Spyware Found 67
- Processes found 18
- Cookies found 30

Bertrand Bechard/Maxppp/ZUMA Press

Fig: Spyware Attack

D. Shoulder surfing:

Shoulder surfing refers to a direct observation, such as looking over a person's shoulder, to obtain information. In some cases **ShoulderSurfing** is done for no reason other than to get an answer, but in other instances it may constitute a security breach as the person behind may be gleaning private information such as your PIN at a bank machine, or Credit card information as you enter it into a webbased shopping cart check-out.

Like text based passwords, most of the graphical authentication methods are vulnerable to shoulder surfing. Until now, only a few recognition-based methods claim to resist shoulder-surfing. None of the recall-based based methods are considered shoulder-surfing resistant.

Fig:Shoulder-Surfing Attacks

E. Social engineering:

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

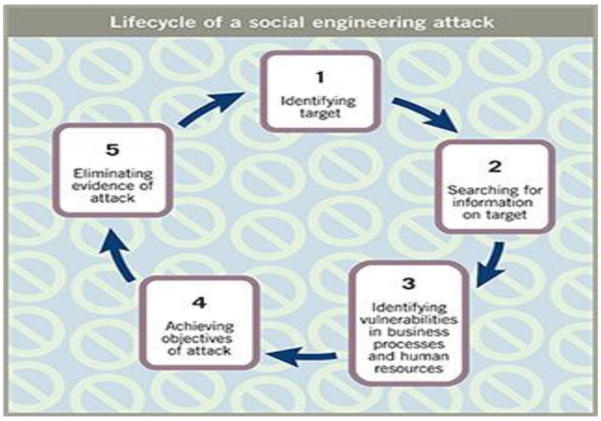

Lifecycle of a social engineering attack
1 Identifying target
2 Searching for information on target
3 Identifying vulnerabilities in business processes and human resources
4 Achieving objectives of attack
5 Eliminating evidence of attack

Fig: Social Engineering

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).It is less convenient for a user to give away graphical passwords to another person as compared to text based passwords. For instance, to tell a graphical password to others over the phone would be very difficult. Even if an attacker isto set up a phishing website so as to obtain graphical passwords from targeted users, it would be more time consuming to set up such sites. Overall, it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and spy-ware. As graphical passwords are still not widely deployed, an in-depth research and studies that investigates possible attack methods are still needed.

IV. DESIGN AND IMPLEMENTATION ISSUES OF GRAPHICAL PASSWORDS

- *Security:*

Security is the state of being free from danger or threat or errors. Graphical passwords are way more secure than textual passwords. Since, Graphical passwords are not widely used in real world hence enough research is yet to be done in field of graphical passwords.
We have briefly examined the security issues with graphical passwords alreadyin the above section.

- *Usability:*

One of the major arguments for graphical authentication is that images are much easier to remember than text strings. Some research papers presented preliminary user studies to support this. However, a current user study involves only a small number of users and is still very limited. A major complaint among the users of graphical authentication procedure is that the registration process and log-in process take too much time, especially in recognition-based approaches. For instance, in the registration phase, a user has to pick few images from a larger number of image sets. Then in the authentication phase, a user has to identify a few pass-images by scanning through all the images displayed. Users may find this process long and tedious.

- *Reliability:*

The major design issue for recall-based methods is the reliability and accuracy of user input recognition. The error tolerances in graphical authentication schemes have to be set carefully if the tolerances are overly high then it may lead to many false positives. And if the tolerances are overly low, then again it may lead to many false negatives. In addition, if the program is more error tolerant, then it will be more vulnerable to attacks.

- *Communication and Storage:*

Graphical authentication schemes require much more space for storage than text based passwords. Huge numbers of images may have to be maintained in a centralized storage database. The delay in loading or transfer of images is also a concern for graphical authentication schemes. Especially for recognition-based techniques in which a large number of images are needed to be displayed for each round of verification in the authentication process.

Table 1: Comparison between different methods

Password Scheme	Password Input	Recapitulation Power	Processing Speed	Authentication
Text Based	Fast	Depend on length and type of character combination.	Fast; Complexity,N	Low
Birget	Fast Input	Low; when large number of objects involved	Slow; Complexity depends in size and type of pictures. Can be given as N! K! (N-K)! (N is the total number of picture objects; K is the number of pre-registered objects)	High
PassFace	Take longer than Text Based	Easier to remember, but, prediction.	N^K(K is the number of rounds of authentication, N is the total number of pictures at each round.)	High, but, chance of dictionary attack.
Glodberg	Draw with stylus on touch sensitive screen; time taking	Depends on drawing complicacy.	High Password Space	Guess dictionary attack
DAS	Depends on type of input; Draw with stylus on touch sensitive screen.	Depends on drawing complicacy.	Space consuming	Dictionary attack
User Authentication by Secured Graphical Password Implementation.	Depends on size of password.	Easy to remember	Minimum consumption due to digitization.	Totally secured; Handwritten Characters are varied from person to person Forgery Detection can be incorporated.

V. CONCLUSION

The alternative to textual passwords is graphical passwords. Graphical password are easy to remember as humans can remember picture better than text passwords Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as

Brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood. Much more research and user studies areneeded for graphical password techniques to reach higher levels of usefulness.

REFRENCES

[1] William Stallings and Lawrie Brown, "Computer Security: Principle and Practices". Pearson Education, 2008.

[2] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," 21st Annual Computer Security Applications Conference (ASCSAC 2005). Tucson, 2005.

[3] Md. AsrafulHaque, Babbar Imam, Nesar Ahmad, "2-Round Hybrid Password Scheme", International Journal of Computer Engineering and Technology (IJCET), Vol. 3, Issue 2, July-September (2012), page. 579- 587.

[4] D.Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399- 1402.

[5] A. S. Patrick, A. C. Long, and S. Flinn, HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA. 2003.

[6] A. Adams and M. A. Sasse, Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.

[7] K. Gilhooly, Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[8] R. Dhamija and A. Perrig, Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[9] R.N.Shepard, Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior", vol. 6, pp. 156-163, 1967.

[10] J.C. Birget, D. Hong, and N. Memon, Robust discretization, with an application to graphical passwords, "Cryptology ePrint archive 2003.

[11] I.Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, the Design and Analysis of Graphical Passwords, "in Proceedings of the 8th USENIX Security Symposium, 1999.

[12] HaichangGao, Xiyang Liu, Ruyi Dai, Design and Analysis of a Graphical Password Scheme, International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 675 678.

[13] Huanyu Zhao and Xiaolin Li, S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme, 21st International Conference on Advanced Information Networking and Applications Workshops, AINAW 07. Page(s): 467 472.

[14] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent-5559961, Ed. United States, 1996.

.