Id Wisdom through Click Based Graphical Password Authentication

Kamlesh Borkar, Ashish Damke, Bhakti Sawarkar, Prashnnaki Gedam, Akash Wankhede

Abstract— "ID Wisdom through Click Based Graphical password Authentication" is a click-based graphical password scheme, a cued-recall graphical password technique. Users Click on one point per image for a sequence of images. The next image is based on the previous click-point. Performance was very good in terms of speed, accuracy, and number of errors. Users preferred CCP to PassPoint, saying that selecting and remembering only one point per image was easier, and that seeing each image triggered their memory of where the corresponding point was located. Secure Web accessibility through Click Based Graphical password Authentication also provides greater security than PassPoints because the number of images increases the workload for attackers

Keyword: Graphical Passwords, Computer Security, Authentication, Web Access through Graphical Password, Secure Web Access.

I. INTRODUCTION

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

Human factors are often considered the weakest link in a computer security system. Patrick, et al. point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. The most common computer authentication method is for a user to submit a user name and and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken.

Manuscript received January 15, 2014.

Kamlesh Borkar , Information technology, RTMNU, Nagpur, India.
Ashish Damke, Information technology, RTMNU, Nagpur, India.
Bhakti Sawarkar, Information technology, RTMNU, Nagpur, India.
Prashnnaki Gedam, Information technology, RTMNU, Nagpur, India.
Akash Wankhede , Information technology, RTMNU, Nagpur, India.

According to a recent Computerworld news article, the security team at a large company ran a network password a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken.

According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts. To address the problems with traditional username password authentication, alternative authentication methods, such as biometrics, have been used.

In this project, however, we have focus on another alternative: using pictures as passwords. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer better resistance to dictionary attacks. Because of these (presumed) advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

In this project, we propose a new click-based graphical password scheme for accessing web accounts called ID Wisdom through Click Based Graphical password Authentication. It can be viewed as a combination of PassPoints and Passfaces. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. This method offers both improved usability and security.

1.BACKGROUND STUDY

Current authentication methods can be divided into three main areas:

- ⇨ Token based authentication
- ⇨ Biometric based authentication
- ⇨ Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge based techniques to enhance security.

Fig.-1 Token Based Authentication

For example, ATM cards are generally used together with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted.

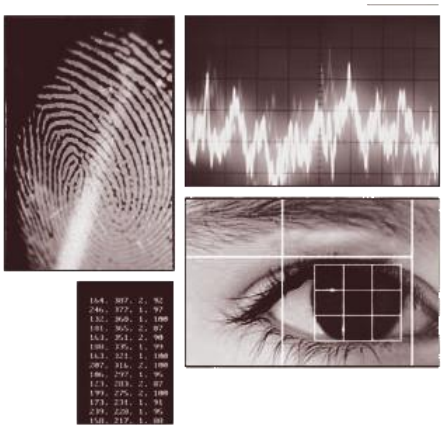

Fig-2 Biometric Authentication

The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security.

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories:

- ⇨ Recognition-based graphical techniques
- ⇨ Recall-based graphical techniques.

Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

2. Existing System

Dhamija and Perrig [1] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre-selected images for authentication from a set of images as shown in figure 1. This system is vulnerable to shoulder-surfing.

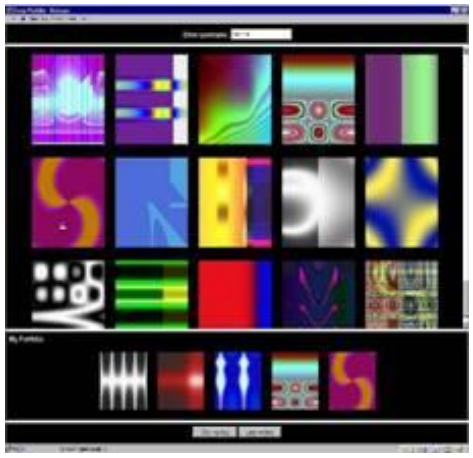

Fig-3: Random images used by Dhamija and Perrig

Passface [2] is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user as shown in figure 2. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. Since there are four user selected images it is done for four times

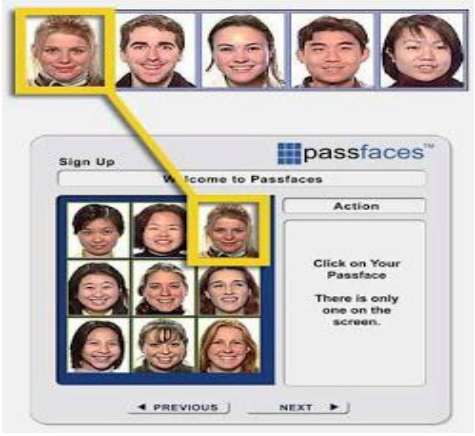

Fig-4: Example of Passfaces

Jermyn[3], proposed a new technique called "Draw- a-Secret" (DAS) as shown in figure 3 where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme is vulnerable to shoulder surfing

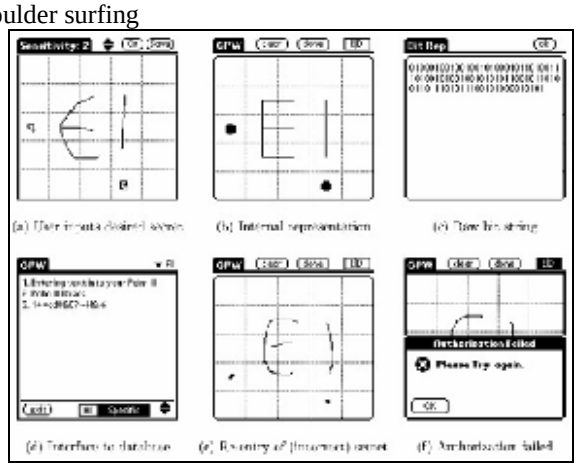

Fig-5: Example of Passfaces

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Haichang's [4] proposed a new shoulder-surfing resistant scheme as shown in figure 4 where the user is required to draw a curve across their password images orderly rather than clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user.

Fig-6: Haichang's shoulder-surfing technique

3. Attacks on Password

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

Brute force search

The main defence against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. 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 need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password.

Dictionary attacks

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, 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 research is needed in this area.

Overall, we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

This is the ingenious attack used word fond in the dictionary to check if any were used as passwords by the users. Many users' uses weak passwords which make it easier for attackers to guess the password using the graphical dictionary attack. Because of graphical password method of using mouse input type recognition, using dictionary attack on GUA would be a waste of time.

Guessing

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passfaces technique have shown that people often choose weak and predictable graphical passwords. Nali and Thorpe's study revealed similar predictability among the graphical passwords created with the DAS technique. More research efforts are needed to understand the nature of graphical passwords created by real world users.

Spyware

Except for a few exceptions, key logging or key listening 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, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

This attack uses a small application installed on a user's computer to record sensitive data during mouse movement or key press. This form of malware secretly store these information and then reports back to the attackers system. With a few exceptions, these key-loggers and listening spywares are unproven in identifying mouse movement to crack graphical passwords. Even if the movement is recorded, it is still not accurate in identifying the graphicalpassword. Other information is needed for this type of attack namely window size and position as well as the timing

Shoulder surfing

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing. None of the recall-based based techniques are considered should-surfing resistant. As the name implies, passwords can be identified by looking over a person's shoulder. This kind of attack is more common in crowded areas where it is not uncommon for people to stand behind another queuing at ATM machines. There are also cases where ceiling and wall cameras placed near ATM machines are used to record keyed pin numbers. The best way to avoid pin numbers being recorded or remembered by attackers is to properly shield the keypad when entering the pin number.

Social engineering

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

Overall, we believe it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and spyware. There is a need for more in-depth research that investigates possible attack methods against graphical passwords

II. CONCLUSION

In information security, user authenticate is most and critical of all elements.Research shows that the people tend to remember the grapghical password than text-base or alphanumberic password.The proposed click based authentication scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over PassPoints in terms of usability. Being cued as each images shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. CCP offers a more secure alternative to PassPoints. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images.

ACKNOWLEDGMENT

There are many persons in RGCER College have supported me from the beginning of my B.E project work. Without them, the project would obviously not have looked the way it does now. The first person I would like to thank is my Project Mr Alok Chauhan**,** Professor of Information technology, RGCER , Nagpur . He has helped me in many ways. His enthusiastic engagements in my project work and his never-ending stream of ideas have been absolutely essential for the results, presented here. I am very grateful that he has spent so much time with me discussing different problems ranging from philosophical issues down to minute technical details

REFERENCES

1. R.Dhamija and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.
2. Real User Corporation: Passfaces. www.passfaces.com
3. Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin."The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.
4. Haichang Gao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing"
5. Pinkas, B. and T. Sander. Securing Passwords Against Dictionary Attacks. ACM CCS, 2002
6. Suo, X, Y. Zhu, and G.S. Owen. Graphical Passwords: A Survey. Annual Computer Security Applications Conference, 2005.
7. Thorpe, J. and P.C. van Oorschot. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords.16th USENIX Security Symposium, 2007.
8. van Oorschot, P.C., S. Stubblebine. On Countering Online Dictionary Attacks with Login Histories and Humans-in-the-Loop.ACM Trans. Information and System Security 9(3), 235-258, 2006.
9. Weinshall, D. Cognitive Authentication Schemes Safe Against Spyware (Short Paper). IEEE Symposium on Security and Privacy, 2006.

AUTHORS PROFILE

Kamlesh Borkar, Student of RGCER Nagpur Pursuing the degree from RTMNU
Email id – kamles.borkar@gmail.com

Ashish Damke, Student of RGCER Nagpur Pursuing the degree from RTMNU Email id – ashish.g.damke@gmail.com

Bhakti Sawarkar, Student of RGCER Nagpur, Pursuing the degree from RTMNU, Email id – bhakti.sawarkar@gmail.com

Prashnnaki Gedam, Student of RGCER Nagpur Pursuing the degree from RTMNU Email id – prashgedam@gmail.com

Akash Wankhede, Student of RGCER Nagpur. Pursuing the degree from RTMNU Email id- akashwankhede48@gmail.com