Review Paper on Secure & Effective Environment Using Graphical Password Authentication Scheme

Akshima Sharma[1], Aditi Kushwaha[2], Suman Nehra[3]

ECE Department, Rajasthan College of Engineering for Women, Jaipur

sharmaakshima796@gmail.com

aditikushwaha275@gmail.com

sumannehra15891@gmail.com

***Abstract*- Authentication, authorization and audit are the most important issues of security in data communication. In particular, authentication is the life of individual essential close friend. The security of user authentication depends on the strength of the password. A strong password is generally random, bizarre, very long and difficult to remember. For most users, these irregular remember passwords are very difficult. To easily remember and security are two sides of a coin. In this paper, a new protocol of graphical password authentication is proposed to solve this problem. The graphical password authentication technology is the use of Click on the image to replace the entrance to some characters. The GUI can help users easily create and remember your passwords. However, in the system of graphical passwords based on images you can provide an alternate password, but too many images will be a great database to the issuance of the store. All information can be steganography to achieve our scheme to solve the problem of database storage. Moreover, the technique of steganography tabular can achieve our plan to solve the problem of intelligence information during data transmission. Our system of modified graphical passwords can help users friendly and easy to store your password without losing any security authentication. Chosen user input is hidden in an image using steganography technology, and will be transferred to the server security without any problem of hacking. And then, our authentication server only needs only store a secret key for decryption rather than the overall database password.**

Keywords: Graphical password authentication, Security, Steganography, Protocol, hack, network security.

I. INTRODUCTION

Network environment today is full of dangerous attackers, hackers, crackers, and spammers. Authentication, authorization and audit are the most important issues of security in data communication. Authentication is the process to allow users to confirm their identity to a Web application. Human factors are often considered the weakest link in computer security system. Point out there are three main areas where human-computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the problem of authentication. A password is a form of secret authentication data that is used to control access to a resource. The password is kept secret from those not allowed access, and those wishing to gain access are tested or know the password and are granted or denied access accordingly. The use of passwords goes back to ancient times. A person is only permitted if they knew the password. In modern times, passwords are used to control access to protected computer operating systems, mobile phones, ATM machines, etc. A typical computer user may require passwords for manypurposes: connections to computer accounts, retrieving e-mail server, access to files, databases, networks, and websites and even read the newspaper in the morning line.

The password authentication method is a very good and strong still used until now, but because of the breakthrough in computer use in many applications such as data transfer, data exchange, accessing e-mail or Internet, some drawbacks of conventional password appears as stolen password, forgotten password, password week, etc. so a great need is required strong way to ensure all our possible application authentication, making out with some research. They called advanced graphical password where they tried to improve security and avoid weakness of conventional password. Graphical password have been proposed as a possible alternative to text based, motivated mainly by the fact that humans can remember images better than text. Psychological studies have shown that people can remember things better than the text (RN Shepard, 1987) images. The pictures are usually easier to be remembered and acknowledged that the text, especially photos, which are even easier to remember than random images.

II. RELATED WORK

Graphical password authentication protocol is first described in Blonder [7]. Blonder proposes a new idea, he lets users use mouse or stylus by themselves to click the picture on presetting correct regions for replacing the traditional text input password. After that, graphical password systems are popular and several different issues are developed [2].Graphical password authentication is an image-based authentication technique which can be divided into two categories [2]. We describe these two categories, recognition-based authentication technique and recall-based authentication technique as follows.

2.1. Recognition Based

Recognition-based technique is a kind of graphical password authentication techniques which need to choose those correct pictures from many pictures. Dhamija and Perrig [18] propose a scheme which can use Hash Visualization technique [1] to support recognition-based graphical password authentication. Kotadia [16] proposes a new recognition-based graphical password authentication that is a multi-image technique with one step for authentication. In Dhamija and Perrig‟s system, the system shows some random generated images and the users are asked to select a certain number of images for the authentication in the graphical interface [18], as shown in Fig. 1. Before use, the user needs to set in advance through the authentication sever to identify images. However, the average log-in time is longer than input alphanumeric password, but the result showed that 90% of all participants succeeded and the text-based password with PINS only 70% in the result [27]. The scheme proposed by Dhamija and Perrig was not really secure because the passwords need to store in database and that is easy to see.

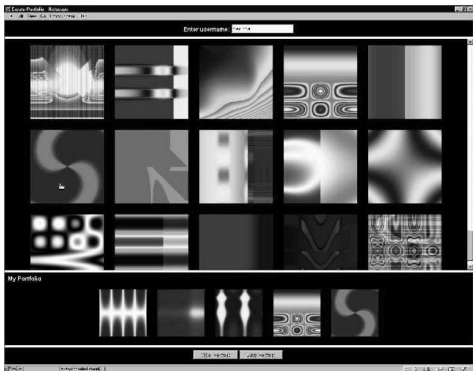
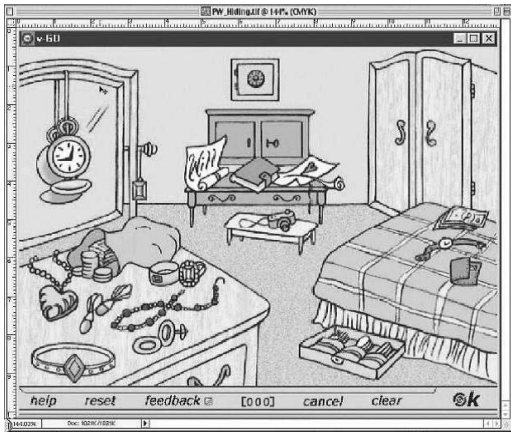


Fig. 1. Random images select used by Dhamija and Perrig [18]

After that, Akula and Devisettys proposed algorithm is similar to Dhamija and Perrig‟s, the different is that it uses hash function SHA-1 rather than Hash Visualization technique. Their scheme can be more secure and require less memory than Dhamija and Perrig‟s . “Pass face” is still a multi-image technique developed by Real User Corporation. Users will be asked to choose four face images to be the password. In authentication step, the users see a grid of nine faces, as illustrated in Fig. 2, and only one face was correct image.

2.2. Recall Based

Another image-based authentication technique is recall-based authentication technique. “Draw-a-Secret” (DAS) is a famous recall based technique which proposed by Jermyn, et al. [11]. DAS technique allows users to draw their passwords on the interface, as shown in Fig. 3. A user will be asked to draw a simple picture and the picture will be store for authentication. During authentication, the user is asked to draw their unique password. User should draw the same grids in the same sequence, and then the authentication will be success. DAS technique can let users draw by themselves, but need more time then alphanumeric-based password [6], and if the users draw in the middle of two sequences, the system will be error. It is difficult that users should draw their password correct and always be same with the first time. Passlogix [17] has developed a graphical password system which is based on a designated image. In this scheme, user should click different items on an image in order to be authenticated, as illustrated in Fig. 4. User should recall the various items that combined their password and choose these correct items. This scheme is not flexible, but certainty provides more security. Passpoints is a kind of single-images based graphical password scheme and this scheme provide more password space to support more security than textual passwords technique. Passpoints scheme also needs one picture to be the interface and allows users to click anywhere in this designated picture to be the user password. Passpoints provide large password space [10] to ensure the secure and provide more flexible interface for user. In addition, Birget et al. [10] proposed a new scheme that is based on the discretization method. Passpoints is our main subject and we will introduce and improve in next subsection.



IJSER

Fig. 2.A recall-based graphical password system

2.3. Passpoints

Passpoints is a graphical password scheme similar to Blonders scheme [7]. Passpoints allows any images to be used and users can click on this designated image to complete their password authentication. A rich and colourful image can be divided into hundreds or more squares. The system of Passpoints includes both graphical and alphanumeric interfaces, but we only discussed the graphical interface. The graphical interface includes a rich picture and several buttons, as shown in Fig. 5. The size of the picture is 451 x 331 pixels and the grid square around a click point is set to 20 x 20 pixels. The special buttons of graphical interface is the "See My Password" button, and it allows users to view their password when they are clicking for ensuring the correct password. Users choose sequence of these memorable points to be the password and it can be hashed that means more security of this graphical password system.

2.4. Security of Passpoints

The graphical password authentication security is based on the "password space". We carefully compared the Passpoints graphical password with the alphanumeric password. In Table 1, we show that the password space between graphical password and alphanumeric password. For example, a 64 character alphabet which includes 10 digits, 26 lower-case letters, 26 upper-case letters, underscore, and dot. If a user chooses alphanumeric password length eight over 64 character alphabets, then the entire number of guessing possible password is 648 = 2.8 x 1014. In graphical password system, there is an image size 451 x 331 = 149,281 and grid square size 20 x 20 = 400, there are about 149281 / 400 = 373 grid squares. If a user chooses 5 click points for the password and the entire number of possible is 3735 = 7.2 x 1012. The image size 451 x 331 is a small password space, but with a big image and more click points will increase the password space, we show the comparison in Table 1. "Passpoints" is secure and have enough password space, but needs to save more pictures for user to use.

III. Improve Database Storage

Recognition based graphical password techniques has a big problem that is to store many images for users. The password database needs to store ID, password table, images and other information which server need. In the premise, server needs enough space to store many sorts of information, especially the images. It will cause equipment burden. In our scheme, we successfully overcome this problem that database does not have to store the large data instead the secret key x. No matter how many users use the system, server just needs to pass the secret key x and key x is only for server using. Although in our scheme also need to store some images but when the user member increases, our scheme will still be a very effectual scheme.

3.1. Security Policy

In graphical password system, shoulder-surfing is a big problem but many researches can solve this problem. Shoulder-surfing means a person who stands on the back of user and wants to see the password when user inputs their passwords. We introduce some schemes and our policy to prevent shoulder-surfing problem. First scheme is developed by Sobrado and Birget [14] and which system displays a number of pass-objects among many different objects. User needs to recognize pass-objects to be authenticated. Second scheme is developed by Man, et al. [22], user needs to select a number of pictures as pass-object, but each pass-object has several variants and each variant is unique code. Third scheme is developed by Hong, et al. [5], and this scheme still uses pass-object, but allows user to assign their own codes to pass-object variant. Shoulder-surfing is a problem, but we propose a simple scheme to prevent this problem. In traditional authentication phase, User uses mouse to click their correct passwords on the interface which uses the left-button of mouse. Our improved scheme is that we can use the right-button of mouse to confuse the person who wants to see the password input. Any person wants to see the password but will not know which clicks are correct. We can set our system to accept only left-button, but let right-button of mouse to click and display. User can use left-button or right-button of mouse, but only the designated-button will be accept and authenticated.

3.2. Usability of Graphical Password

The usability is very important of graphical password and number of existing graphical password schemes available on the internet. We discuss about the usability and explain why the "Passpoints" can really use in the future. We show the usability features of graphical password which is made by Hafiz, et al. [28] and there are 12 schemes in the table to compare with their usability. The Passpoints scheme is the best of these 12 schemes in compare with each usability feature. The Passpoints scheme is the only scheme that can be considered as an efficient scheme. The input reliability andaccuracy are one of the features which can provide the usability and users can easily remember their graphical password. Even we use nine grids but do not spend many times and we believe that our modified Passpoints still can keep

IJSER

efficient. For user to use our system, user clicking one of nine pictures is just like to choose one of the correct points in Passpoints. Although this is easy but can really improve the security and also can keep efficient. If the users forget their setting points or images, they can redo the setting phase by the certified phase that same as the traditional alphanumeric password certified phase.

IV. CONCLUSION

This paper reviews the graphical password systems, in this we need the image big enough to ensure the security. Because of the large enough images can be cut into many enough sub-blocks to meet the users to set their passwords. In a small screen device, the problem is how to provide a large enough password space on a small image. The research of Passpoints suggested that user might be handled by magnification of any area of the chosen image. Our research suggests that user can move the image in small screen by mouse. In the screen, the system will show the given area and when user hold the left button of mouse then user can move the image in this area that means we can put a big image in a small screen device like PDA. The limitation of graphical password system has some important issues. First, the image should be colourful and rich enough, the image should be a big enough to provide large enough password space to keep the security. And when input password may click in the middle of two grids, the fault tolerance can be set to solve this problem. Second issue is efficiency; users to use the mouse to enter a password may be slower than the keyboard. However, graphical password still has value and possibility instead of alphanumeric password. The most important issue is the human memory. People should spend more time learning and practice the graphical password but user's thinking and feeling this kind of graphical password will be much easier than alphanumeric password. Finally, this paper reports a new scheme of graphical password and combines with another technology to improve database of server. In cryptography, security is based on the strength of password. Most passwords belong to alphanumeric password which is developed from symmetric cryptographic algorithm to asymmetric cryptographic algorithm. That shows the importance that saving password is in password table. We provide a new scheme of graphical password and prove that our scheme can solve the problem of database storage. All information can be steganography to achieve our scheme and can solve the problem of database storage. Furthermore, the information eavesdropping problem during data transmission can be overcome by our tabular steganography technique. Overall, our modified graphical password system can help user easy and friendly to memory their password and without loss of any security of authentication. User's chosen input will hide into image using steganography technology, and transfer to server security without any hacker problem. And then, our authentication server only needs to store a secret key X for decryption instead of large password database.

V. REFERENCES

[1]. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce. (1999)

[2]. Paivio, T. B. Rogers, P. C. Smythe, "Why are pictures easier to recall then words?" Psychonomic Science, Vol.11, No.4, pp.137–138. (1999)

[3]. C. Lee, M. S. Hwang, W. P. Yang, "A Flexible Remote User Authentication Scheme Using Smart Cards", ACM Operating Systems Review, Vol. 36, No. 3, PP. 46-52. (2002)

[4]. S. Tsai, C. C. Lee, M. S. Hwang, "Password Authentication Scheme: Current Status and Key Issues", International Journal of Network Security, Vol.3, No.2, pp.101115. (2006)

[5]. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware", Proceedings of International conference on security and management. Las Vergas, NV. (2004)

[6]. Weinshall, S. Kirkpatrick, "Passwords you"ll never forget, but can't recall", Proceedings of CHI 2004 ACM Press, New York, pp. 1399-1402. (2004)

[7]. E. Blonder, "Graphical password", United States Patent 5559961. (1996)

[8]. P. Bahrick, "Semantic memory content in permastore: fifty years of memory for Spanish learned in school", Journal of Verbal Learning and Verbal Behavior, Vol. 14, pp. 1-24. (1984)

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

[10]. J.C. Birget, D. Hong, and N. Memon. "Robust Discretization, with an Application to Graphical Passwords". IEEE Transactions on Information Forensics and Security, Vol. 1, pp. 395-399. (2006)

[11]. Scholtz, J. Johnson, "Interacting with identification technology: can it make us more secure?", Proceedings of the CHI 2002 Extended Abstracts, ACM Press New York, pp. 564– 565. (2002)

[12]. T. Wixted, "The psychology and neuroscience of forgetting", Annual Review of Psychology, Vol.55, pp. 235– 269. (2004)

[13]. Coventry, A. De Angeli, G. I. Johnson, "Usability and biometric verification", ATM interface, CHI 2003 Proceedings, pp. 153–160. (2003)

[14]. Sobrado and J. C. Birget, "Graphical passwords", The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4. (2002)

[15]. A. Sasse, S. Brostoff, D. Weirich, "Transforming the „weakest link"-a human/computer interaction approach to usable and effective security", BT Technical Journal Vol.19, pp.122–131. (2001).

IJSER