International Journal of Cryptography and Security
ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-27-31.
Available online at http://www.bioinfo.in/contents.php?id=115

GRAPHICAL PASSWORD AUTHENTICATION SYSTEM IN AN IMPLICIT MANNER

SUCHITA SAWLA*, ASHVINI FULKAR, ZUBIN KHAN AND SARANG SOLANKI

Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India.
*Corresponding Author: Email- suchita.sawla@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- Authentication is a process by which a system verifies the identity of a user. Authentication may also be generalized by saying that "to authenticate" means "to authorize". For example, users tend to pick passwords that can be easily guessed, on the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem some researchers have developed authentication methods that use pictures as passwords, known as graphical passwords. We classify these techniques into two categories: recognition-based and recall-based approaches which are discussed in this paper along with the strengths and limitations of each method. We have proposed a new technique for authentication. It is a variation to the login/password scheme using graphical passwords used in an implicit manner. This Graphical Password Authentication System in an Implicit Manner is immune to the common attacks suffered by other authentication schemes.

Keywords- Authentication, Graphical Password.

Citation: Suchita Sawla, et al. (2012) Graphical password authentication system in an implicit manner. International Journal of Cryptography and Security, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, pp.-27-31.

Introduction

Authentication deals with the security as an act of showing the belongings to its owner only. Various authentication schemes are available these days. But out of these entire how many are truly secure? To answer it lets go through the background of graphical passwords. We deal with graphical passwords because graphical password schemes act as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text [10]. Pictures are generally easier to be remembered or recognized than text. In addition, if the number of possible pictures is sufficiently large, the possibility of password space exceeds than that of text-based schemes and thus offers better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password. Authentication is a process by which a system verifies the identity of a user. It is a process of determining whether a particular individual or a device should be allowed to access a system or an application or merely an object running in a device [15]. Also, adequate authentication is the initial step of defense for protecting any resource. Authentication may also be generalized by saying that "to authenticate" means "to authorize" or provide authorization to the user. It is important that the same authentication technique may not be used in every scenario. For example, a less sophisticated approach may be used for accessing a "chat server" compared to accessing a corporate database [15]. Most of the existing authentication schemes require processing both at the client and the server end. Thus, the acceptability of any authentication scheme greatly depends on its robustness against attacks as well as its resource requirement both at the client and at the server end. Here specifically the mobile banking domain is targeted and a new and intelligent authentication scheme is proposed.

In this paper, we conduct a study of the existing graphical password techniques. We will discuss the strengths and limitations of each method. The rest of the paper is organized as follows: 2. specifies various graphical password techniques, 3. deals with various authentication schemes, 4. Proposed Graphical Password Authentication System in an Implicit Manner along with its strengths and weaknesses compared with the existing schemes, 5. deals with conclusion and future directions.

Various Graphical Password Techniques

In general, the graphical password techniques can be classified into two categories: recognition-based and recall-based graphical techniques [10].

Recognition Based System

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. There are many graphical password authentication schemes which designed by using recognition-based techniques. We only introduce two typical schemes. The first one is PassFaces which was developed by Real User Corporation [10]. The user will be asked to choose four or more images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight cheat faces (figure 1). The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures.

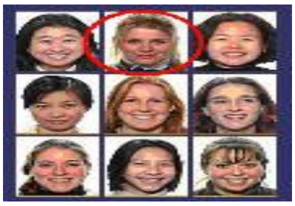

Fig. 1- An example of Passfaces

Also a survey concluded that user's password selection is affected by race and gender. This makes the Passfaces's password somewhat predictable.

Another recognition-based scheme is Pass-Objects which was developed by Sobrado and Birget [6]. The system will display a number of pass-objects among many other objects. Then, to authenticate, the program shows a variety of similar objects on the screen, and the user is asked to click inside the area that the selected objects make. For instance, if you chose three Pass-Objects, when those three objects are displayed on the screen, it will form a triangle. What a user will then do is click inside of this newly formed invisible triangle for authentication. It will then ask for the same action again, but with the icons on the screen in different positions. Figure 2 is an example of this method. Sobrado and Birget suggested using 1000 icons and ten attempts. This will yield 2.6×1023 combinations of possible Pass-Objects. This is a greater combination than a 15 character alphanumeric password used today.

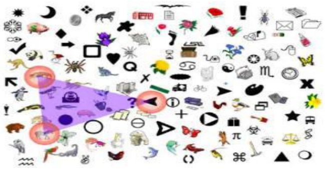

Fig. 2- An example of Pass-Objects

A group of images are displayed to the user and an accepted authentication requires a correct image being clicked or touched in a particular order in this recognition-based systems. Some examples of recognition-based system are explained below.

An image password called Awase-E [7] is a new system which enables users to use their favorite image instead of a text password for authentication purpose. Even though Awase-E system has a higher usability, the system cannot tolerate replay attack. Adding to this, a user may always tend to choose a well-known (or associated with the user through some relation, like son, wife or a place visited etc.) image which may be prone to guessing attacks. Weinshall and Kirkpatrick [14] studied a recognition-based scheme and concluded that users can still remember their graphical password with 90% accuracy even after one or two months. Their study supports the theory that human remember images better than text.

Although a recognition-based graphical password seems to be easy to remember, which increases the usability, it is not completely secure. Also, it is obvious that recognition based systems are vulnerable to replay attack and mouse tracking because of the use of a fixed image as a password. Thus, these drawbacks are considered in the proposed system, which overcomes the problems of recall based schemes too.

Recall-based System

In recall-based systems, the user is asked to reproduce something that he/she created or selected earlier during the registration phase. Recall based schemes can be broadly classified into two groups, viz: pure recall-based technique and cued recall-based technique.

Pure Recall-based Techniques

In this group, users need to reproduce their passwords without any help or reminder by the system. Draw-A-Secret technique [8], Grid selection [3], and Passdoodle [5] are common examples of pure recall-based techniques.

DAS (Draw-A-Secret) scheme is the one in which the password is a shape drawn on a two-dimensional grid of size G * G as in Figure 3. Each cell in this grid is represented by distinct rectangular coordinates (x, y). The values of touch grids are stored in temporal order of the drawing. If exact coordinates are crossed with the same registered sequence, then the user is authenticated. As with other pure recall-based techniques, DAS has many drawbacks. In 2002, a survey concluded that most users forget their stroke order and they can remember text passwords easier than DAS. Also, the password chosen by users are vulnerable to graphical dictionary attacks and replay attack.

In 2004, the Grid selection technique was proposed by Thorpe and Van Oorschot [3] to enhance the password space of DAS. To improve the DAS security level, they suggested the "Grid Selection" technique, where the selection grid is large at the beginning, a fine grained grid from which the person selects a drawing grid, a rectangular area to zoom in on, in which they may enter their

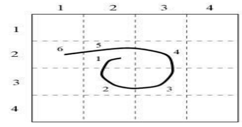

Fig. 3- Example of DAS

password as shown in Figure 4. This technique would increase the password space of DAS, which improves the security level at the same time. Actually, this technique only improves the password space of DAS but still carries over DAS weaknesses

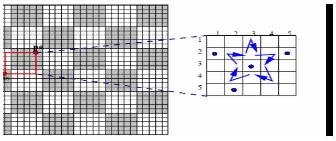

Fig. 4- Example of Grid Selection Model

Passdoodle, is a graphical password of handwritten drawing or text, normally sketched with a stylus over a touch sensitive screen as shown in Figure 5. Goldberg et. al have shown that users were able to recognize a complete doodle password as accurately as text-based passwords. Unfortunately, the Passdoodle scheme has many drawbacks. Users were fascinated by other users' drawn doodles, and usually entered other users' password merely to a different doodles from their own. It is concluded that the Passdoodle scheme is vulnerable to several attacks such as guessing, spyware, key-logger, and shoulder surfing.

Fig. 5- Example of Passdoodle

Cued Recall-based Techniques

In this technique, the system gives some hints which help users to reproduce their passwords with high accuracy. These hints will be presented as hot spots (regions) within an image. The user has to choose some of these regions to register as their password and they have to choose the same region following the same order to log into the system. The user must remember the "chosen click spots" and keep them secret. There are many implementations, such as Blonder scheme [1] and PassPoint scheme [6].

In 1996, Blonder designed a method where a pre-determined image is shown to the user on a visual display and the user should "click" on some predefined positions on the image in a particular order to be authenticated as in Figure 6. This method was later modified and presented as Passpoint.

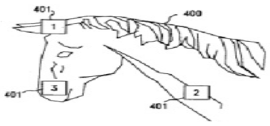

Fig. 6- Example of Blonder Scheme

In 2005, the PassPoint scheme was created to be similar to the Blonder's scheme while overcoming some of its main limitations. In Passpoint, the image can be an arbitrary photograph or paintings with many clickable regions as shown in Figure 7. This will increase the password space of Passpoint scheme which in turn will increase the security level. Another source of difference is that there is no predefined click area with clear boundaries like the Blonder scheme. The user password could contain any chosen sequence of points in the image, which increases the usability level of this scheme.

Fig. 7- Example of PassPoint System

Five or six click points on an image can produce more passwords than 8-character text-based passwords with standard 26-character alphabet. For more security, the Passpoint system stores the image password in a hashed form in the password file. In order to be authenticated, the user has to click close to the selected points, within some measured tolerance distance from the pass point. To log in, the user should click with the tolerance of such a click point.

Various Authentication Schemes

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. 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. 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 and 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. Using recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

Problems Faced by These Techniques

Traditional alphanumeric passwords are always vulnerable to guessing and dictionary attack. In order to overcome the key logger based attacks, newer systems using graphical keyboard may also be defeated if the attacker uses a screen capture mechanism, rather than using a key logger. An attacker may use a screen capture program and record a short video clip and send it to a remote server for publishing. So, as an alternative, a token based authentication method may be used either as a standalone authentication or used in addition to the traditional alphanumeric password.

Although image based authentication systems reviewed in this seminar address most of the threats, still they suffer from the following attacks: replay, Shoulder-surfing, and recording the screen. One may argue that replay attack can be prevented using encryption and tamper-proof time stamps, and physical shoulder-surfing may be known to the user as this process is invasive. However, due to the availability of high-bandwidth to mobile devices and light-weight, high-efficient video codecs, a rogue program may still capture and publish remotely. Since all the image based password schemes known to us use static passwords, the recorded movie may be replayed and with some human-interaction, the user's password may be decoded.

Graphical Password Authentication System In An Implicit Manner

The proposed Graphical Password Authentication System in an Implicit Manner is similar to the PassPoint scheme with some finer differences. In every "what you know type" authentication scheme, the server requests the user to reproduce the fact given to the server at the time of registration. Here the password is considered as a piece of information known to the server at the time of registration and at the time of authentication, the user give this information in an implicit form that can be understood only by the server. It is explained through a Mobile Banking example.

Mobile Banking

As an example mobile banking is considered. However, it may also be implemented in any client-server environment, where there is a need to authenticate a human as a client (it will not work in machine-to-machine authentication). It is also assumed that the server has enough hardware resources like RAM and CPU. The bank may have a database of 100 to 200 standard questions. During the time of registration, a user should pick 10-20 questions from the database (this number of questions depends upon the level of security required in the system) and provide answers to the selected questions.

For example, the user may choose the following questions:
1. Your favorite subject ?
2. What is the color of your eye?
3. Place of your birth?

For each question, the server may create an intelligent authentication space using images, where the answers to the particular question for various users are implicitly embedded into the images. During the time of authentication, the server may pick one or more questions selected by the users at the time of registration randomly (the number of questions depends on the level of service requested). For each chosen question, the server may choose an image randomly from the authentication space and present it to the user as a challenge. Along with the correct answer image the images which are incorrect are also shown to the user. Using the stylus or the mouse, the user needs to navigate the image and click the right answer. For example, the server may present the user with the images which are answer to other questions along with the image representing the correct answer. The user should correlate to Question 2. If blue is the color of the user's eye, he needs to click on the relevant image as shown in Figure 8.

The other images may be answer to other questions. But this answer is not shown directly, it is represented by the image in an implicit way. Here the other images like zebra-crossing may represent the answer zebra, the images of vegetables might represent vegetarian food which the user likes, and the image of milk represent the white color and so on. So the conclusion is that the answer is provided indirectly i.e. implicitly. Next time, if the same question is chosen by the server, the same scenario may not be presented. For the next time, the server may show an images among which the correct answer be shown by an image showing a blue ink pen and so on. The user needs to click on this blue ink pen image correlating it to the answer blue to implicitly convey his answer. Since every time the server uses a different scenario and the answers are given implicitly, the proposed system is immune to screen capture attack. Also, except for the server and the legitimate user, for others, the answers may look fuzzy. For example, if the user clicks "Blue Ink Pen", it may even mean the "type of writing tool the user likes the most", or may represent his "favorite color" and so on.

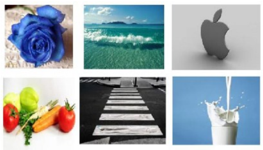

Fig. 8-Example of the system

Framework

The bank may have a set of 100 to 200 questions. Every user selects a set of 10 to 20 questions at the time of registration and provides their individual answer. For each question, the system then either creates an authentication space (the space that represents implicit answers for the questions using images) if it is not available or add the new user's answer to the existing authentication space. Once the authentication space is created, the system is ready for authenticating a user.

First, a user may request access to the system by presenting his user name and the level of access required. This may be sent as a plain text. Depending on the level of access required, the system might choose one or more questions registered by the user during the time of registration process. For each question, the server may choose random images from the authentication space that represents the correct answer. The chosen images will contain a correct answer along with incorrect answers. It is upto the user to correlate with the question the image shown on the screen.

Strength

As one can easily see, it is immune to shoulder surfing and screen -dump attacks. Also, the authentication information is presented to the user in an implicit form that can be understood and decoded only by the legitimate end-user. Traditional password based authentication schemes and PassPoint are special cases. The strength of this system depends greatly on how effectively the authentication information is embedded implicitly in an image and it should be easy to decrypt for a legitimate user and highly-fuzzy for a non-legitimate user.

Conclusion

people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. 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.

The proposed Graphical Password Authentication System in a Implicit Manner provides authentication information to be implicitly presented to the user. If the user “Clicks” the same grid-of-interest compared with the server, the user is implicitly authenticated. No password information is exchanged between the client and the server. Since the authentication information is conveyed implicitly, it can tolerate shoulder-surfing and screen dump attack, which none of the existing schemes can tolerate. The strength lies in creating a good authentication space with a sufficiently large collection of images to avoid short repeating cycles. Compared to other methods reviewed in this paper, it requires human-interaction and careful selection of images and “Click” regions. It may also need user training.

References

[1] Birget J.C.,Dawei H., et al. (2006), *Information Forensics and Security, IEEE Transactions on* 1(3),395-399.

[2] Dirik A. E., Memon N., et al. (2007). *3rd symposium on Usable privacy and security*.

[3] Haichang G., Xiyang L., et al. (2009).Fourth International Conference on Graphical Passwords.

[4] Lashkari A. H., Towhidi F., et al. (2009) *ICCEE '09. Second International Conference*.

[5] Masrom M.,Towhidi F., et al. (2009). *AICT 2009. International Conference*.

[6] Pierce J.D., Jason G. Wells, Matthew J. Warren, and David R. Mackay. (2003).*1st Australian Information security Management Conference*,

[7] Renaud K. (2009) *J. Vis. Lang. Comput*. 20(1),1-15.

[8] Wiedenbeck S.,Waters J.,Birget J.C.,Brodskiy A., Memon N. (2005) *Symposium on Usable Privacy and Security (SOUPS)*, 6-8

[9] Wiedenbeck S.,Waters J.,Birget J.C., Brodskiy A., Memon N. (2005) *International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security),* 63, 102-127.

[10]Sabzevar A.P. and Stavrou A. (2008) *IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS)*.

[11]Takada T. and Koike H. (2003) *Human-Computer Interaction with Mobile Devices and Services* 2795:,347-351.

[12] Wei-Chi K. and Maw-Jinn T. (2005) *Local Computer Networks*.

[13] Wells Jason, Hutchinson Damien and Pierce Justin *Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication, formation Security Management Conference*. 58.

[14] Xiaoyuan S., Ying Z., et al. (2005) Computer Security Applications Conference.

[15] Sadiq Almuairfi, Parakash Veeraraghavan and Naveen Chilamkurti (2011) *Workshops of International Conference on Advanced Information Networking and Applications.*