Volume : 1 | Issue : 9 | September 2012 ISSN - 2250-1991

Research Paper Computer Science

Analysis & Design Graphical Password Authentication Using Cryptography Algorithms

*Mr.Pratik A Vanjara ** Dr. Kishor Atkotiya

* Department Of Computer Science & I.T., Shree. M & N Virani Science College, Rajkot

** Head, Department of Computer Science, J.H Bhalodia Women's College, Rajkot

ABSTRACT

The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. 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 using cryptography algorithms. In this paper, we conduct a comprehensive survey of the existing graphical password techniques. We classify these techniques into two categories: recognition-based and recall-based approaches. We discuss the strengths and limitations of each method and point out the future research directions in this area.

We also try to answer two important questions: "Are graphical passwords as secure as text-based passwords?"; "What are the major design and implementation issues for graphical passwords". In this paper, we are conducting a comprehensive survey of existing graphical image password authentication techniques. Also we are here proposing a new technique for graphical authentication using algorithms.

Introduction:

Human factors are often considered the weakest link in a computer security system. 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. 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 paper, however, we will 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 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 paper, we conduct a comprehensive survey of the existing graphical password techniques using cryptography algorithms. We will discuss the strengths and limitations of each method and also point out future research directions in this area. In this paper, we want to answer the following questions:

→ Are graphical passwords as secure as text passwords?
→ What are the major design and implementation issues for graphical passwords?

Overview of the Authentication Methods:

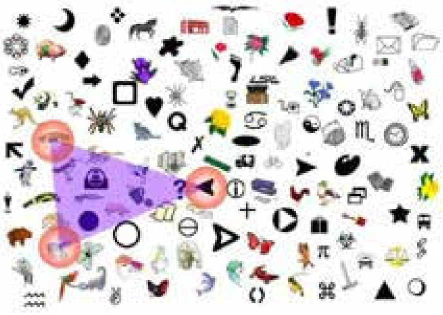
Current authentication methods can be divided into Three main areas:

→ 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.

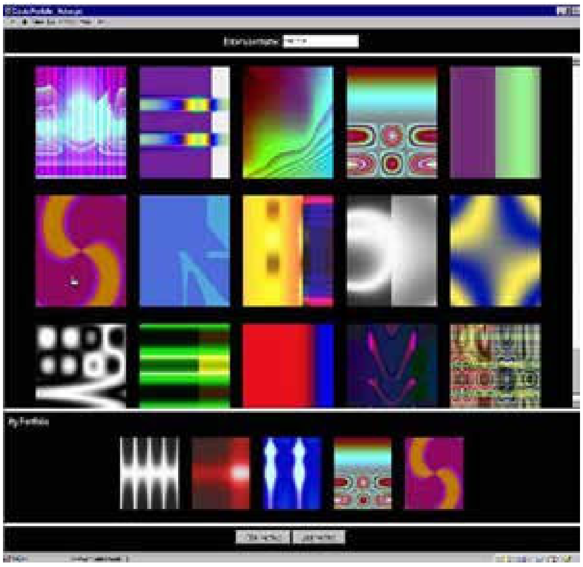
Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides he 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.

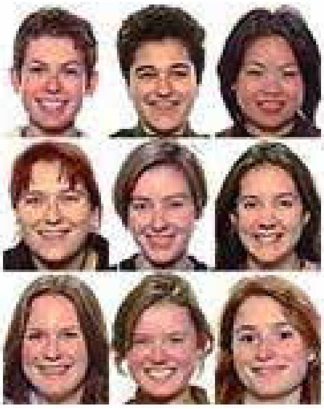


Recognition Based Techniques

Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the user will be required to identify the pre selected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

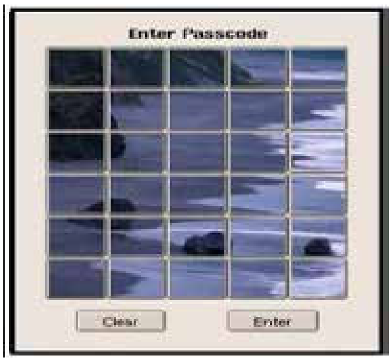


Sobrado and Birget developed a graphical password technique that deals with the shoulder-surfing problem. In the first scheme, the system will display a number of pass-objects (pre-selected by user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the convex hull formed by all the pass-objects.In order to make the password hard to guess, Sobrado and Birget suggested using 1000 objects, which makes the display very crowded and the objects almost indistinguishable, but using fewer objects may lead to a smaller password space, since the resulting convex hull can be large. In their second algorithm, a user moves a frame (and the objects within it) until the pass object on the frame lines up with the other two pass-objects. The authors also suggest repeating the process a few more times to minimize the likelihood of logging in by randomly clicking or rotating. The main drawback of these algorithms is that the log in process can be slow.



A shoulder-surfing resistant graphical password scheme

Man, et al. proposed another shoulder-surfing resistant algorithm. In this algorithm, a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects (each in the form of a randomly chosen variant) and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass-objects in reference to a pair of eyes. The argument is that it is very hard to crack this kind of password even if the whole authentication process is recorded on video because where is no mouse click to give away the pass-object information. However, this method still requires users to memorize the alphanumeric code for each pass-object variant. Hong, et al. later extended this approach to allow the user to assign their own codes to pass-object variants. However, this method still forces the user to memorize many text strings and therefore suffer from the many drawbacks of text-based passwords.

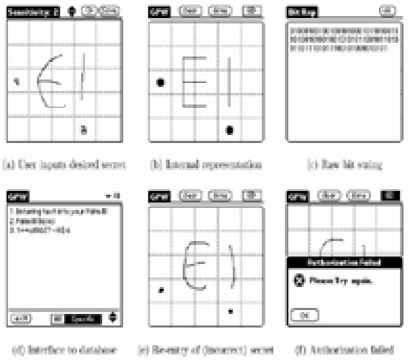


An example of Passfaces

Jansen et al proposed a graphical password mechanism for mobile device .during the enrollment stage, a user selects a theme (e.g. sea, cat, etc.) which consists of thumbnail. photos and then registers a sequence of images as a password .During the authentication, the user must enter the registered images in the correct sequence. One drawback of this technique is that since the number of thumb nail images is limited to 30, the password space is small. Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password. The result showed that the image sequence length was generally shorter than the textural password length. To address this problem, two pictures can be combined to compose a new alphabet element, thus expanding the image alphabet size.

RECALL BASED

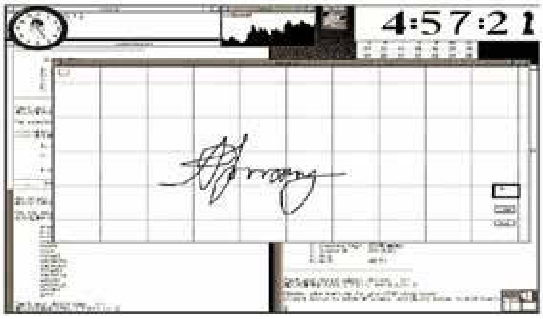
Reproduce a drawing:


(a) User inputs desired secret
(b) Internal representation
(c) Raw bit string
(d) Interface to database
(e) Re-entry of (incorrect) secret
(f) Authorization failed

A graphical password scheme proposed by Jansen, et al

Jermyn, et al. proposed a technique, called “Draw - a - secret (DAS)”, which allows the user to draw their unique password .A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space.

Draw-a-Secret (DAS) technique proposed by Jermyn, et al



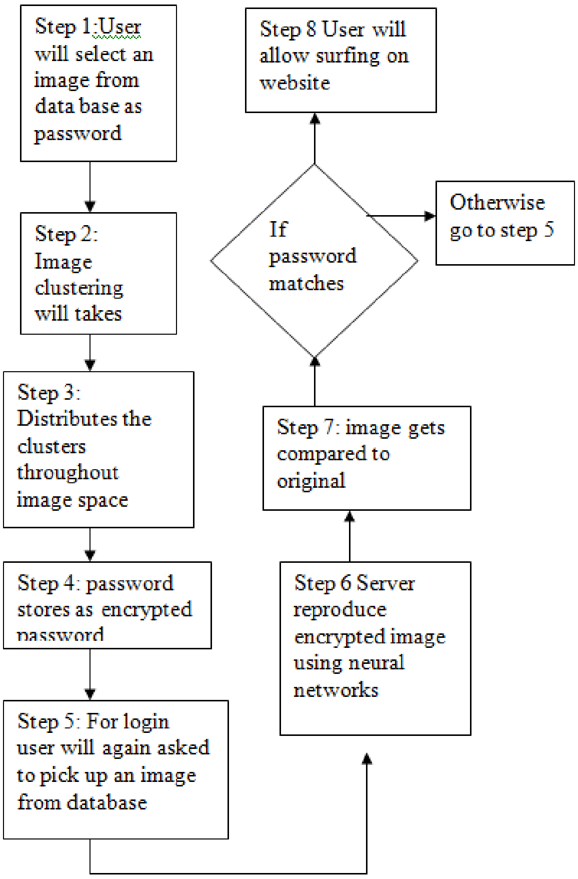
Nali and Thorpe conducted further analysis of the "Draw-A-Secret (DAS)" scheme. In their study, users were asked to draw a DAS password on paper in order to determine if there are predictable characteristics in the graphical passwords that people choose. The study did not find any predictability in the start and end points for DAS password strokes, but found that certain symmetries (e.g. crosses and rectangles), letters, and numbers were common. The "PassPoint" system by Wiedenbeck, et al. extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence. This technique is based on the discretization method proposed by Birget, et al. . Because any picture can be used and because a picture may contain hundreds to thousands of memorable points, the possible password space is Quite large.

An image used in the Pass point System,

New Technique For Graphical Password Authentication

. Here we are proposing a new algorithm of authentication using graphical images. when a ;user tries to register over a network we will ask him or her to select a theme or sequence of pictures from already given image frame. The local host downloads an image frame which contains various themes of sequence of pictures which act as passwords, these are given by server. Since any image is made of pixels we have its gray level concentration. In this way the image will be distorted and can't be in original form. so it is not easy for hacker to reproduce the original form of image.

The flow chart of the proposed technique is given below.


Step 1:User will select an image from data base as password
Step 2: Image clustering will takes
Step 3: Distributes the clusters throughout image space
Step 4: password stores as encrypted password
Step 5: For login user will again asked to pick up an image from database
Step 6 Server reproduce encrypted image using neural networks
Step 7: image gets compared to original
If password matches
Otherwise go to step 5
Step 8 User will allow surfing on website

Is a graphical password as secure as text-based 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 defense 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 basedgraphical 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.

Guessing

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passface 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.

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.

What are the major design and implementation issues of graphical passwords?

Security

In the above section, we have briefly examined the security issues with graphical passwords.

Usability

One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. Preliminary user studies presented in some research papers seem to support this. However, current user studies are still very limited, involving only a small number of users. We still do not have convincing evidence demonstrating that graphical passwords are easier to remember than text based passwords.

A major complaint among the users of graphical passwords is that the password registration and log-in process take too long, especially in recognition-based approaches. For example, during the registration stage,a user has to pick images from a large set of selections. During authentication stage, a user has to scan many images to identify a few pass-images.

Users may find this process long and tedious. Because of this and also because most users are not familiar with the graphical passwords, they often find graphical passwords less convenient than text based passwords.

Reliability

The major design issue for recall-based methods is the reliability and accuracy of user input recognition. In this type of method, the error tolerances have to be set carefully – overly high tolerances may lead to many false positives while overly low tolerances may lead to many false negatives. In addition, the more error tolerant the program, the more vulnerable it is to attacks.

Storage and communication

Graphical passwords require much more storage space than text based passwords. Tens of thousands of pictures may have to be maintained in a centralized database. Network transfer delay is also a concern for graphical passwords, especially for recognition-based techniques in which a large number of pictures may need to be displayed for each round of verification.

Conclusion:

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, we have conducted a comprehensive survey of existing graphical password techniques. The current graphical password techniques can be classified into two categories: recognition-based and recall-based techniques..

Although the main argument for graphical passwords is that 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. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood.

Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness.

REFERENCES

[1] A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003. [2] 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. [3] K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2000. [4] Websites browsed: www.crypto.com , www.cryptography.com, www.infosyssec.net, www.uow.edu.au, www.amazon.com, www.phptr.com, www.csrc.nist.gov