User Authentication Methods and Techniques by Graphical Password: A Survey

Swetha Sathish
Dept. of ISE, Sambhram Institute of Technology (VTU), Bangalore

Asha B Joshi
Dept. of ISE, Sambhram Institute of Technology (VTU), Bangalore

Ganeshayya I Shidaganti
Lecturer, Dept. of ISE, SaIT, Bangalore

ABSTRACT

The most commonly and widely used authentication method is the traditional "Username" and "Password". For such authentication generally text (alphanumeric) is used. This method has been shown to have significant drawbacks. For example, users tend to use passwords that are easy for attackers to crack. On the other hand, if a password is hard to guess, then it is often hard to remember. To address these problems, some researchers have developed authentication methods that use pictures as passwords. The goal of authentication systems is to support users in selecting better passwords, thus increasing security, usability and expanding the effective password space. In this paper we make a comprehensive survey of the basic authentication and its techniques. The techniques of authentication can be broadly classified as token based, biometric based and knowledge based. We also discuss the strengths and limitations of each method. This survey will be useful to find an alternative to text based authentication methods.

KEYWORDS

Graphical password Authentication, Security, Usability, Password space.

1. INTRODUCTION

Human factors are often considered the weakest link in a computer security system [1]. There are three major areas where human-computer interaction is important: authentication, security operations, and developing secure systems [2]. Authentication is any protocol or process that permits one entity to establish the identity of another entity [3]. Humans have used three methods for authentication [3]. These methods are:

- Something you know (the password)
- Something you have (credit card, university ID card)
- Something you are (face, voice, signature, fingerprints, DNA, iris)

Today, these methods are called the three factors of authentication [4]. They are

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

Token based techniques such as credit 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 [5]. Tokens have their own weaknesses, however because tokens are simple and cheap to produce, they are also simple and cheap to reproduce. This makes them vulnerable to being counterfeiting. Also, because they are typically a physical object or device, carrying token all the times is inconvenient for users. They can also be stolen more easily than passwords. For this reason, tokens are typically used with another method, such as a PIN code, to reduce their usefulness if stolen [3].

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 [5].

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords [1].

Text based passwords are not very secure. The problems with text based passwords are:-

1) Passwords should be easy to remember and the 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.

Satisfying these requirements is virtually impossible for users. Consequently, users ignore the requirements, leading to poor password practices. This problem has led to innovations to improve passwords.

One innovation is graphical passwords, i.e., passwords that are based on images rather than alphanumeric strings. The basic idea is that using images will lead to greater memorability and decrease the tendency to choose insecure passwords.

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).

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 [1].

2. CLASSIFICATION OF AUTHENTICATION METHODS

Table 1. Classification of different authentication methods

	TOKEN BASED AUTHENTICATION METHOD	BIOMETRIC BASED AUTHENTICATION METHOD	KNOWLEDGE BASED AUTHENTICATION METHOD
Meaning	Token-based authentication is a security technique that authenticates the users who attempt to log in to a server, a network, or some other secure system, using a security token provided by the server	Biometric based authentication[http://en.wikipedia.org/wiki/Biometrics - cite_note-1](http://en.wikipedia.org/wiki/Biometrics) refers to the identification of humans by their characteristics or traits. Biometrics is used in computer science as a form of identification and access control	Knowledge-based authentication is a method of authentication which seeks to prove the identity of someone accessing a service, such as a website
What is it also known as?	Proof by possession techniques (Something you have)	Proof by property techniques (Something you are)	Proof by knowledge techniques (Something you know)
Where is it used?	One time passwords, Smart cards, Soft tokens, Dongles	Fingerprint, Palm print, DNA, Face recognition, Voice, Gait, and Speaking rhythm or diction	Personal Identification Number, Text based passwords, Picture based passwords
Benefits	• It increases security compared to passwords	• Highest level of security • Positive and accurate identification • Safe and user friendly	• Pictures are easier to remember • Graphical passwords are hard to guess by the attacker • Easy to communicate
Limitations	• Can be lost or stolen • Observable and possible to replicate • Accessibility	• Susceptible to replay-capture of data and reuse • Biometric systems are expensive • Unreliable • Perceived privacy threats	• Prone to dictionary attacks, brute force attacks, observation attacks • Difficult to remember • Easily predictable

Most commonly, computers use passwords, the "something you know" factor, for basic authentication. Passwords are the simplest authentication model to implement, and that is why password models are so common. Unfortunately, password models are also the weakest authentication model because passwords are guessed or stolen relatively easily. Users often choose weak passwords.

Some authentication systems commonly use tokens, which is any device or object that can authenticate a user. In the previous example, we referred to the general's ring or seal. These are examples of tokens. Common modern examples include physical keys, proximity cards, credit cards, or ATM cards. Tokens are good because they're simple. Physical keys, for example, are widely supported and cheap to produce and use. Tokens have their own weaknesses, however. Because tokens are simple and cheap to produce, they are also simple and cheap to reproduce. This makes them vulnerable to being counterfeiting. Also, because they are typically a physical object or device, they can be stolen more easily than passwords.

Humans have specific physical attributes that are unique to specific individuals. Humans are conditioned to recognize these characteristics and use them for authentication. However, it is more difficult for computers, which think in digital ones and zeros, to recognize "analog" characteristics such as faces or voices. We call the systems that do this processing for authentication biometric systems. The problem with biometric systems is that it is very expensive and not

very reliable. It is susceptible to possible threats like the information could be regenerated and misused.

3. TAXONOMY OF AUTHENTICATION METHODS

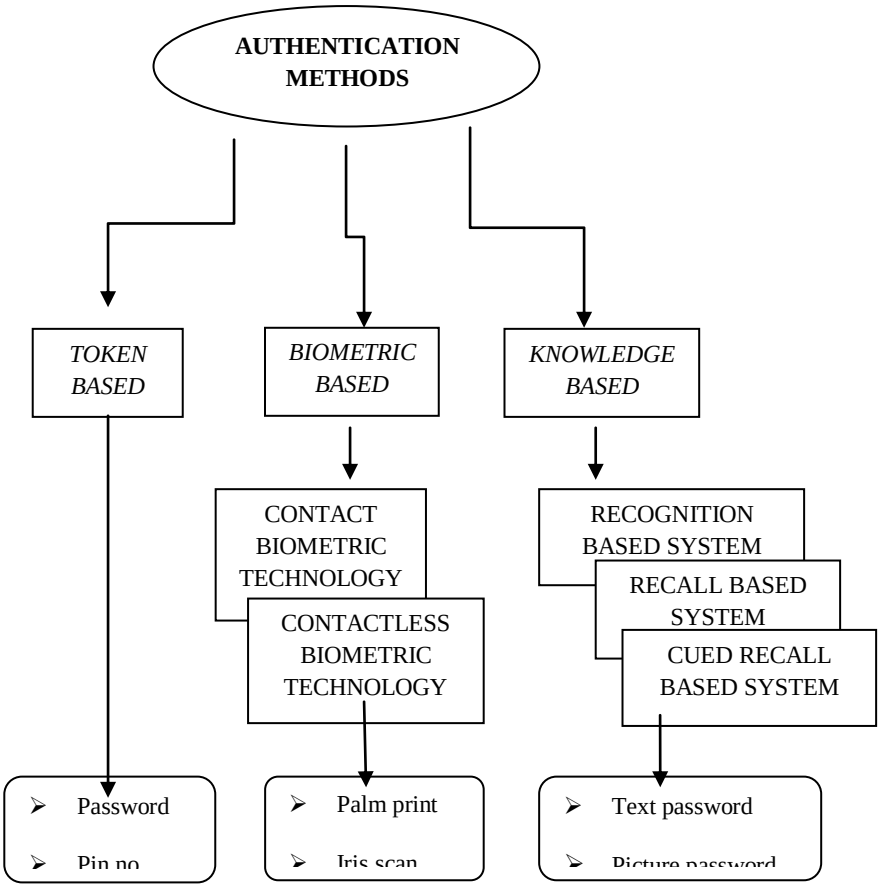

Figure 1. Taxonomy of different authentication methods

4. KNOWLEDGE BASED AUTHENTICATION

Knowledge based authentication system is an authentication system which requires the user to know something for getting the access into the system [6].

4.1 Recognition based system

Dhamija and Perrig [7] proposed a graphical authentication scheme based on the Hash Visualization technique [8]. 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 preselected images in order to be authenticated. 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. Akula and Devisetty's algorithm [9] is similar to the technique proposed by Dhamija and Perrig. The difference is that by using hash function SHA-1, which produces a 20 byte output, the authentication is secure and require less memory. The authors suggested a possible future improvement by providing persistent storage and this could be deployed on the Internet, cell phones and PDA's. Weinshall and Kirkpatrick [10] sketched several authentication schemes, such as picture recognition, object recognition, and pseudo word recognition, and conducted a number of user studies. In the picture recognition study, a user is trained to recognize a large set of images (100 – 200 images) selected from a database of 20,000 images. This study showed that pictures are the most effective among the three schemes tested.

. Sobrado and Birget [11] 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. The main drawback of these algorithms is that the log in process can be slow.

4.2 Recall Based Techniques

In this section we discuss two types of recall based techniques: reproducing a drawing and repeating a selection.

4.2.1 Reproduce a Drawing

Jermyn, et al. [12] 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.

4.2.2 Repeat a sequence of actions:-

Blonder [13] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password).

5. DESIGN AND IMPLEMENTATION CHALLENGES OF GRAPHICAL PASSWORD

The main design issue for recognition based techniques is how to make it easier for users to remember and recognize the images. A number of techniques have been proposed, such as grouping images by theme, using human face images, or allowing users to register their own images.

The major design issue for recall-based methods is the reliability and accuracy of user input recognition. This is a typical pattern recognition problem. In this type of methods, the tolerances of error have to be set carefully – overly high tolerances may lead to lots of false positives while overly low tolerances may lead to lots of false negatives.

In the above section, we have briefly examined the security issues with graphical passwords. Maintaining a large password space is a major design issue for both recognition based and recall-based methods. A large password space is necessary to defend against guess-based attacks. For recognition-based methods, one solution is to have several rounds of verifications. But this will make the log-in process longer and tedious. Another solution is to deploy large number of decoy-images. Some proposed methods involve hundreds of decoy-images. This would also slow down the log-in process. In addition, this solution is not suitable for mobile devices due to very limited user interface space.

For "reproduce-a-drawing" methods, possible solutions include maintaining a large canvas, reducing the tolerance of error, and requiring users to draw complex pictures. However, this may result in sophisticated and perhaps overly sensitive recognition programs that generate lots of false negatives. For "repeat-a-sequence" methods, the solution is to use a highly detailed image and provide large number of potential click-points. Users are also required to click on many points in order to generate a long password. The drawback, however, is that users may have difficulty to memorize the long sequence of clicks.

Shoulder-surfing resistance is an important design consideration. 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. Graphical passwords require much more storage space than text based passwords. Tens of thousands of pictures 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 hundreds of pictures may need to be displayed for each round of verification [5].

6. CONCLUSION

Authentication methods and techniques are currently available in plenty but each has its own benefits and shortcomings. A neat comparison of different authentication methods is presented in the table shown above. Though the main discussion for graphical based passwords is that people are better at remembering picture passwords than text based passwords, our preliminary analysis suggests that it is very complicated to break graphical passwords using techniques such as brute force search, dictionary attack, spyware etc which are known to be the traditional attack methods. Much research on graphical password techniques have to be done to reach higher levels of usefulness. To conclude, we need our authentication systems to be more reliable, robust and secure as there is always a place for improvement.

7. REFERENCES

[1] Suo, Xiaoyuan, "A Design and Analysis of Graphical
[2] Password" (2006). Computer Science Theses. Paper 27. A. C. L. Andrew S. Patrick, Scott Flinn, "HCI and Security Systems," in CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.
[3] "Authentication Methods and Techniques", Christopher Mallow.
[4] "A Graphical Password Based System for Small Mobile Devices", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011, Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang.
[5] "Graphical Passwords: A Survey", Xiaoyuan Suo, Ying Zhu, G. Scott, Owen, Department of Computer Science, Georgia State University.
[6] "Enhanced Knowledge Based Authentication Using Iterative Session Parameters", Ali Alkhalifah, Geoff D.Skinner, World Academy of Science, Engineering and Technology 47 2010
[7] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
[8] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*, 1999.
[9] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings of Midwest Instruction and Computing Symposium*, 2004.
[10] 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.
[11] L. Sobrado and J.-C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002
[12] 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.
[13] G. E. Blonder, "Graphical passwords," in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996