International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 5, May - 2013

A Secured Graphical Password Authentication System

M. Mathuri Pandi
PG Student,Department of computer Applications,
Bharathidasan Institute Of Technolog,
Anna University Regional Center,
Trichy.

Dr. A. Valarmathi,
AP,Dapartment Of Computer Applications,
Bharathidasan Institute Of Technology,
Anna University Regional Center,
Trichy.

Abstract

Information and computer security is supported largely by passwords which are the principle part of the authentication process. The most common computer authentication method is to use alphanumerical username and password which has significant drawbacks. Authentication is one of the essential security features in network communication. Authentication process ascertains the legitimacy of the communicating partners in communication. In authentication process, the originator of the communication and the respondent transacts some identification codes of each other prior to start of the message transaction. Several methods have been proposed regarding the authentication process from time to time. Though traditional login/password based schemes are easy to implement, they have been subjected to several attacks. As an alternative, token and biometric based authentication systems were introduced. However, they have not improved substantially to justify the investment. In this paper, we introduce a framework of our proposed (SGPAS) Secured Graphical Password Authentication System, which is immune to the common attacks suffered by other authentication schemes.

Keywords-- ***Graphical Password; Security; Passwords; Graphical Authentication. Network Security.***

1. Introduction

Authentication 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. This is an important process which assures the basic security goals, viz. *confidentiality and integrity.*

Also**,** adequate authentication is the first line of defense for protecting any resource. It is important that the same authentication technique may not be used in every scenario.

Graphical passwords can be created during user registration or after registration (for users registered before Two Step was implemented), and be changed any time after creation. A graphical password policy, which may be set by the site operator or the user, influences its presentation and security. Example policy attributes are: *number of rounds of verification*; *display layout*, e.g., 6×6, defining how images are presented to the user, and the total number of images displayed in each round; *number of images* to be selected in each round; and *ordered* or *unordered* image selection, defining whether order of image selection matters.

After a graphical password policy is defined, users choose images as their graphical passwords. For each round of verification, the specified numbers of images are randomly selected by the system from a database to form an image portfolio. A user then chooses a specified number of images from the portfolio as her graphical password components. This process repeats for the specified number of rounds. If the user does not like a particular image portfolio, she may request a new one or upload her own images to be included in a portfolio. An accepted image portfolio remains unchanged until the user changes her graphical password. To facilitate recognition, images within a portfolio are assembled to be sufficiently distinguishable.

There are several authentication schemes available in the literature. They can be broadly classified as follows:

_ What you know
_ What you have and
_ What you are

The traditional *username/password* or *PIN* based authentication scheme is an example of the "what you know type". Smartcards or electronic tokens are examples of "what you have type of authentication" and finally biometric based authentication schemes are examples of the "what you are" type of authentication. Some authentication systems may use a

combination of the above schemes. In this paper, we focus only on "what you know" types of authentication.

Although traditional alphanumeric passwords are used widely, they have problems such as being hard to remember, vulnerable to guessing, dictionary attack, key-logger, shoulder-surfing and social engineering [1].

In addition to these types of attacks, a user may tend to choose a weak password or record his password. This may further weaken the authentication schemes. As an alternative to the traditional password based scheme, the biometric system was introduced. This relies upon unique features unchanged during the life time of a human, such as finger prints, iris etc. The major problem of biometric as an authentication scheme is the high cost of additional devices needed for identification process [2].

The false-positive and false negative rate may also be high if the devices are not robust. Biometric systems are vulnerable to replay attack (by the use of sticky residue left by finger on the devices), which reduces the security and usability levels. Thus, recent developments have attempted to overcome biometric shortcomings by introducing *token-based* authentication schemes.

Token based systems rely on the use of a physical device such as smartcards or electronic-key for authentication purpose. This may also be used in conjunction with the traditional password based system. Token based systems are vulnerable to man-in-the middle attacks where an intruder intercepts the user's session and records the credentials by acting as a proxy between the user and the authentication device without the knowledge of the user [3]. Thus as an alternative, *graphical based passwords* are introduced to resolve security and usability limitations mentioned in the above schemes.

2. Classification of Current Authentication Methods

Due to recent events of thefts and terrorism, authentication has become more important for an organization to provide an accurate and reliable means of authentication [4]. Currently the authentication methods can be broadly divided into three main areas. Token based (two factor), Biometric based (three factor), and Knowledge based (single factor) authentication [5], also shown in the Figure 1.

2.1. Token Based Authentication

It is based on "Something You Possess". For example Smart Cards, a driver's license, credit card, a university ID card etc. It allows users to enter their username and password in order to obtain a token which allows them to fetch a specific resource - without using their username and password. Once their token has been obtained, the user can offer the token - which offers access to a specific resource for a time period - to the remote site[6]. Many token based authentication systems also use knowledge based techniques to enhance security [7].

2.2. Biometric Based Authentication

Biometrics (ancient Greek: bios ="life", metron ="measure") is the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits [9]. It is based on "Something You Are" [8]. It uses physiological or behavioral characteristics like fingerprint or facial scans and iris or voice recognition to identify users. A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. The classification of authentication will be shown in figure 1.

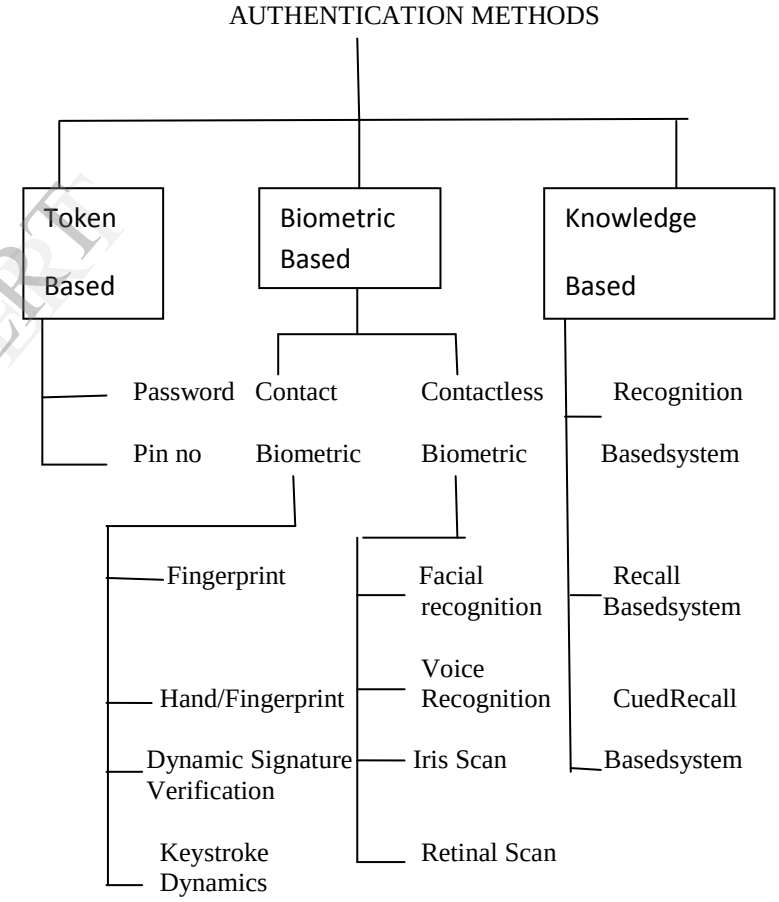

Figure 1.

A biometric-based authentication system may deploy one or more of the biometric technologies: voice recognition, fingerprints, face recognition, iris scan, infrared facial and hand vein thermo grams, retinal scan, hand and finger geometry, signature, gait, and keystroke dynamics [10]. Biometric identification depends on computer algorithms to make a yes/no

decision. It enhances user service by providing quick and easy identification [11].

2.3. Knowledge Based Authentication

Knowledge based techniques are the most extensively used authentication techniques and include both text based and picture based passwords [12]. Knowledge-based authentication (KBA) is based on “Something You Know” to identify you For Example a Personal Identification Number (PIN), password or pass phrase. It is an authentication scheme in which the user is asked to answer at least one "secret" question [13]. KBA is often used as a component in multifactor authentication (MFA) and for self-service password retrieval. Knowledge based authentication (KBA) offers several advantages to traditional (conventional) forms of e-authentication like passwords, PKI and biometrics [14].

3. Classification of Graphical Password Based Systems

Graphical-based password techniques have been proposed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text.

Graphical based passwords schemes can be broadly classified into four main categories: First is **Recognition based Systems** which are also known as Cognometric Systems or Search metric Systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. Second is **Pure Recall based systems** which are also known as Drawn metric Systems. In pure recall-based methods the user has to reproduce something that he or she created or selected earlier during the registration stage. Third is **Cued Recall based** systems which are also called Icon metric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his his/her password. Fourth is **Hybrid systems** which are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes.

3.1. Recognition-Based Systems

. Recognition based systems which are also known as Cognometric Systems or Search metric Systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. The proposed works in this regards are summarized as below:

· Cognitive authentication (Weinshall 2006)
· Use your illusion (Hayashi 2008)
· Story (Davis 2004)
· Déjà vu (Dhamija 2000)
· PassFace (Realusr 2011, Passfaces 2011)
· VIP (Angeli 2005, Moncur 2007)
· Photographic authentication (Pering 2003)
· Convex Hull Click (Wiedenbeck 2006)
· GPI/GPS (Bicakci 2009)
· Picture Password (Jasen 2003)

Some examples of recognition-based system are Awase-E system ,AuthentiGraph , and Passfaces system.

An image password called Awase-E 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, it is difficult to implement due to the storage space needed for images and also 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.

3.2. Pure Recall based systems

which are also known as Drawn metric Systems. In pure recall-based methods the user has to reproduce something that he or she created or selected earlier during the registration stage. Few works are given below:

· Android screen unlock (Tafasa 2011)
· GrIDsure (Grid sure 2011)
· Pass Shapes (Weiss 2008)
· DAS (Jermyn 1999)
· BDAS (Dunphy 2007)
· PassGo (Tao 2006)
· YAGP (Gao 2008)
· Haptic Password (Orozco 2006)
· Pass doodle (Goldberg 2002, Varenhorst 2004)

3.3. Cued Recall based systems

Which are also called Icon metric Systems. In cued recall-based methods, a user is provided with a hint so that he or she can recall his his/her password. Several works are as below:

· Jiminy’s scheme (Renaud 2004, 2001)
· Suo’s scheme (Suo 2006)
· PassPoints (Wiedenbeck 2005, 2005, 2005)
· PassFace (Realusr 2011, Passfaces 2011)
· CCP (Chiasson 2007)
· PCCP (Chaisson 2008)
· Inkblot authentication (Stubblefield 2004)
· 3D scheme (Alsulaiman 2006)
· Passlogix (Passlogix 2011)

3.4. Hybrid systems

Which are typically the combinations of two or more schemes. Like recognition and recall based or textual with graphical password schemes. The scheme is studied by researches as below:

· CDS (Gao 2010)
· Two Step Authentication (Oorschot 2009)
· GP based systems for small mobile devices (Khan 2011)
· My proposed system: Ray's Scheme

4. PROBLEMS WITH THE EXISTING SCHEMES

Traditional alphanumeric passwords are always vulnerable to guessing and dictionary attack. There may even be a rogue program that may record the key strokes and publish it on a remote website. In order to overcome the key logger based attacks, newer systems may show a graphical keyboard and the user has to press the correct password using "mouse clicks".

Traditional alphanumeric passwords are used widely, they have problems such as being hard to remember, vulnerable to guessing, dictionary attack, key-logger, shoulder-surfing and social engineering.

In addition to these types of attacks, a user may tend to choose a weak password or record his password. This may further weaken the authentication schemes. As an alternative to the traditional password based scheme, the biometric system was introduced.

This relies upon unique features unchanged during the life time of a human, such as finger prints, iris etc. The major problem of biometric as an authentication scheme is the high cost of additional devices needed for identification process.

The false-positive and false-negative rate may also be high if the devices are not robust. Biometric systems are vulnerable to replay attack (by the use of sticky residue left by finger on the devices), which reduces the security and usability levels.

Thus, recent developments have attempted to overcome biometric shortcomings by introducing *token-based* authentication schemes. Token based systems rely on the use of a physical device such as smartcards or electronic-key for authentication purpose.

This may also be used in conjunction with the traditional password based system. Token based systems are vulnerable to man-in-the middle attacks where an intruder intercepts the user's session and records the credentials by acting as a proxy between the user and the authentication device without the knowledge of the user.

5.PROPOSED SYSTEM

The proposed system overcomes the problems of the above mentioned systems by means of a graphical but implicit authentication mechanism that is safe from the shoulder surfing, screen capture or man in the middle attacks.

Here authentication is based on several questions instead of a single question so the question used for authentication of the user will not be repeated any sooner. Also the images associated with the user's authentication space will also be chosen randomly and thus the probability of the attacker guessing the password image is almost Zero.This mechanism does not involve the requirement of robust hardware like that of the bio-metric systems.

6. SECURED GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

In this section, we propose our Secured Graphical Password Authentication System. SGPAS is similar to the Pass Point scheme with some finer differences. In every "what you know type" authentication scheme we are aware of, the server requests the user to reproduce the fact given to the server at the time of registration. This is also true in graphical passwords such as Pass Point. In IPAS, we consider the password 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.

SGPAS may also be implemented in any client-server environment, where we need to authenticate a human as a client (SGPAS will not work in machine-to-machine authentication). We also assume that the server has enough hardware resources like RAM and CPU. This is not un-realistic as high-end servers are becoming cheaper day-by-day. Our System 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 (depending upon the level of security required) and provide answers to the selected questions. For example, the user may choose the following questions:

Who is your favorite leader?
The city you love to visit or visited?
Date of birth?
What is your favorite country?

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. 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 picture of the Globe. The user should correlate to Question 2. If Sydney is the city the user loves to visit or has **v**isited, he needs to click on to Australia. It will then enlarge Australia. Then in the map, the user needs to click Sydney as shown in Figure2.

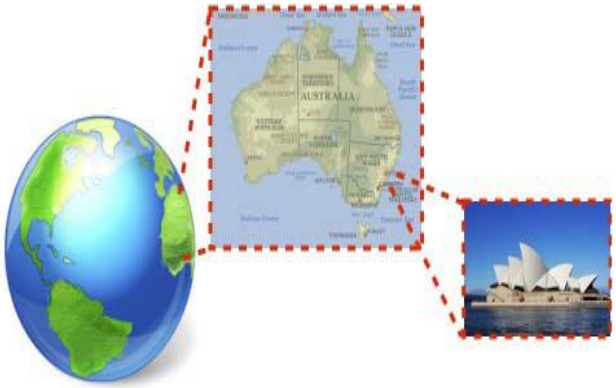

Figure 2.

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 image containing all famous buildings and monuments. The user needs to click on the "Sydney Opera house" to implicitly convey his answer. Since every time the server uses a different scenario and the answers are given implicitly, our 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 click "Opera house", it may even mean the "type of music user is interested to listen", or may represent his "place of birth", or "current residency" and so on.

7. SYSTEM IMPLEMENTATION

In this part, we will explain how the system is works. System is divided in to Registration module i.e user is require to register first of all. That is it requires filling all the necessary personal information such as full name, address, state, MobileNo. EmailID. And for as Proposed scheme the confidential details are as Username, Accountnumber, security level .The Accountnumber field is most important the user will remember the accountnumber after registration for future use. The Registration process is shown in Figure 3.

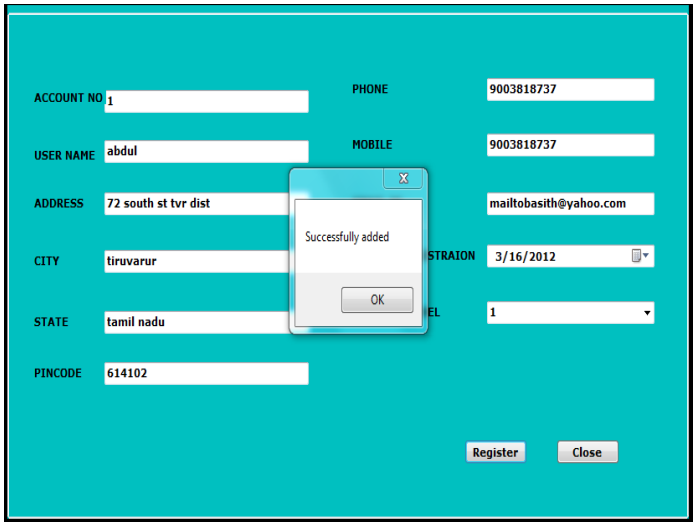

Figure 3.

The proposed system has a field security level. In this field has a security questions for user. Based on the security level the questions will be shown to the user. One security level have two security questions the register user will answer the questions.

If the user answers the security questions the different type of images will be shown depends upon the user answer. The user will see the images and remember the images for future use. After the security level questions are answered by user then the user will enter login module. The security question level will be shown in figure 4.

Figure 4.

The next module is Login. In this module it Require to fill the necessary information such as account number, After user click the show images button there are random color images are displayed the user will select the image that is the user had seen at the time of registration, if the selected color images at the login time is equal to the selected images at the time of registration then and then only the authentication is valid otherwise authentication is failed. The Login process is shown in fig5.

Figure 5.

8. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we have proposed a new Implicit Password Authentication System where the authentication information is implicitly presented to the user. If the user "clicks" the same grid-of-interest compared with the server, the user is implicitly authenticated. The strength of IPAS 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 our paper, IPAS may require human-interaction and careful selection of images and "click" regions.

9. REFERENCES

[1] Sabzevar, A.P. & Stavros, A., 2008," Universal Multi-Factor Authentication Using Graphical Passwords", IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS).

[2] Haichang, G., L. Xiyang, et al. (2009). "Design and Analysis of a Graphical Password Scheme", Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on Graphical Passwords.

[3] L.Sobrado and J.C. Birget, "Graphical Passwords", The Rutgers Schloar, An Electronic Bulletin for Undergraduate Research,vol4,2002,Http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm.

[4] Patric Elftmann, Diploma Thesis, "Secure Alternatives to Password-Based Authentication Mechanisms" Aachen, Germany October 2006

[5] Hai tao, ***"Pass-Go, a New Graphical Password Scheme"***, Master Thesis, University of Ottawa Canada, June 2006.

[6] Di Lin, Paul Dunphy, Patrick Olivier, Jeff Yan, 2007, 'Graphical passwords& qualitative spatial relations',Proceedings of the 3rd symposium on Usable privacy and security, ACM.

[7] Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd, 2007, 'Reducing shoulder-surfing by using gaze-based password entry',Proceedings of the 3rd symposium on Usable privacy and security, ACM.

[8] HAFIZ, M. D., ABDULLAH, A. H., ITHNIN, N. & MAMMI, H. K., 2008, „Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique" , Second Asia International Conference on Modeling & Simulation (AICMS).

[9] HAICHANG, G., XUEWU, G., XIAOPING, C., LIMING, W. & XIYANG, L., 2008, „YAGP: Yet Another Graphical Password Strategy" , Annual Computer Security Applications Conference.

[10] HUANYU, Z. & XIAOLIN, L., 2007, „S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme" , 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW).

[11] P. Golle and D. Wagner. Cryptanalysis of a Cognitive Authentication Schemes (Extended Abstract). In Proc. of the 2007 IEEE Symposium on Security and Privacy, May 2007.

[12] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter, and A. Rubin. The Design and Analysis of Graphical Passwords. In Proc. of the 8th USENIX Security Symposium, August 23-26 1999.

[13] M. Kumar, Tal Garfinkel, D. Boneh, and T. Winograd. Reducing Shoulder-surfing by Using Gaze-based Password Entry. In Proc. of SOUPS'07, July 2007.

[14] A. Rabkin. Personal Knowledge Questions for Fallback Authentication. In Proc. of the 2008 Symposium On Usable Privacy and Security (SOUPS), July 23-25 2008.

[15] D. Weinshall. Cognitive Authentication Schemes Safe Against Spyware (Short Paper). In Proc. of the 2006 IEEE Symposium on Security and Privacy, May 2006.

[16] Sigmund N. Porter. A password extension for improved human factors. Computers & Security, 1(1):54 – 56, 1982.

[17] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. Graphical passwords: A survey. In Proceedings of Annual Computer Security Applications Conference, pages 463–472, 2005.

[18] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63:128–152, July 2005.

[19] G. E. Blonder. Graphical password. U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill, NJ), August 1995.