ISSN No. 0976-5697

Volume 4, No. 6, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

CASE STUDY AND REPORT

Available Online at www.ijarcs.info

# A Secure Authentication Using Graphical Password Authentication System: GPAS

Nikhil Arun Pogale
Department of Information Technology
Jawaharlal Darda Institute of Engineering
and technology Lohara,Yavatmal
Npogale009@gmail.com

Deepak Ganpatrao Rasekar
Department of Information Technology
Jawaharlal Darda Institute of Engineering
and technology Lohara,Yavatmal
Deepakrasekar9404@gmail.com

Prof. Aditya P. Bakshi
Department of Information Technology
Jawaharlal Darda Institute of Engineering
and Technology Lohara, Yavatmal

***Abstract:*** Now a days majority of computer systems, passwords are the method of choice for authenticating users. A process by which a system verifies the identity of a user is known as 'Authentication'. Authentication may also be generalized by saying that "to authenticate" means "to authorize". Authentication is the first line of defense against compromising confidentiality and integrity. The most widely and commonly used authentication is traditional "Username" and "Password". For such authentication generally text (alphanumeric) is used. It is well-known, however, that passwords are susceptible to attack: users tend to choose passwords that are easy to remember, and often this means that they are also easy for an attacker to obtain by searching for candidate passwords . Token and biometric based authentication systems were introduced as an alternative for that schemes. However, these schemes are very costy . Thus, Graphical scheme was introduced as a variation to the login/password scheme. In this paper we explore an approach to user authentication that generalizes the notion of a textual password and that, in many cases, improves the security of user authentication over that provided by textual passwords. In this proposed system we have used a new technique for authentication. It is a variation to the login/password scheme using graphical password used in an graphical manner. We have introduced a framework of our proposed Graphical Password Authentication System (GPAS), which is immune to the common attacks suffered by other authentication schemes**.** We try to answer most important question "Are graphical passwords as secure and easy to use as text-based passwords"? Nowadays with the use of mobile phones, users can access any information including banking and corporate database. In this proposed work, we specifically target the mobile banking domain and propose a new and intelligent authentication scheme. However, our proposal can also be used in other domains where confidentiality and integrity are the major security requirements.

***Keywords***: Authentication, security, Graphical password, mobile banking.

## I. 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 simply an object running in a device. Authentication process assures the basic security goals, i.e. confidentiality and integrity. The first line of defense for protecting any resource is Authentication. For secure authentication it is necessary that the same authentication technique may not be used in every scenario. For example, accessing a "chat server" a less authentication security technique is used as compared to accessing a corporate database. 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. Because, Most of the existing authentication schemes require processing both at the client and the server end. Due to the proliferation of mobile and hand-held devices the resource requirement has become a major factor.

Now a days users can access any information including banking and corporate database, by using mobile phones. For banking we propose our Authentication System using Graphical Password, in which the scheme allows any image to be used and it does not need artificial predefined click regions with well-marked boundaries. Graphical Password can be formed in the combination of Image Icons or Pictures. In other words, 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). For this reason, the graphical-password approach is sometimes called graphical password authentication system(GPAS). In GPAS, the server has password at the time of authentication and at the time of registration, the user give this information to the server in an graphical form at the time of registration and login.

Computer and Information security is very much dependent on password for the authentication of the users and are common in practice. There are several authentication schemes available in the literature. They can be broadly classified as: Knowledge based authentication, Token based authentication and Biometric based authentication. An example of the "Knowledge based authentication" is the traditional username/password or PIN based authentication scheme. An examples of "Token based authentication" are Smartcards or electronic tokens nd finally biometric based authentication schemes are examples of the "Biometric based authentication" type of authentication. Some authentication systems may use a combination of the above schemes. In



CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

GPAS, we focus only on "Knowledge based authentication" types of authentication.

## II. LITERATURE REVIEW

Text method is most widely used, since it is easy to implement and use. One of the main pitfalls in text-based password is the difficulty of remembering it. There were lot of problems in using traditional alphanumeric password such as vulnerable to guessing, dictionary attack, key-logger, forget password, shoulder-surfing and social engineering, although they are widely used. Studies have shown that users tend to pick short and easy passwords that can be used by them easily. But, these passwords can also be easily guessed or broken. Text based password scheme is lacking the above essential points mostly. Generally the text based passwords follow the following guidelines:

a. At least 8 characters long and alphanumeric.
b. Should not be easy to relate to the user (e.g. last name, phonenwnber, birth year).
c. Should not be a word that can be found in a dictionary or public dictionary.
d. Should combine upper and lower case letters and digits.

The biometric system was introduced *et al.*[2], As an alternative to the traditional password based scheme. This relies upon unique features unchanged during the life time of a human, such as finger prints, iris etc. the high cost of additional devices needed for identification process *et al.*[2] is the major problem of biometric as an authentication scheme. if The devices are not robust the false-positive and false negative rate may also be high. 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.By introducing token-based authentication schemes, recent developments have attempted to overcome biometric shortcomings.

Token based systems rely on the use of a physical device such as smartcards or electronic-key for authentication purpose *et al.*[9]. The traditional password based system may also be used in Token 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 *et al.*[9].

Graphical based passwords are introduced as an alternative to above schemes to resolve security and usability limitations mentioned in these schemes. Graphical-based password techniques have been introduced as a potential alternative to text-based techniques, due to by the fact that humans can remember images better than text *et al.*[8]. Psychologists also proved that images are more memorable than text. Therefore, graphical-based authentication schemes have higher usability than other authentication techniques. On the other hand, it is also difficult to break graphical passwords using normal attacks such as dictionary attack, brute force and spyware which have been affecting text-based and token-based authentication. So, there were higher sequrity in graphical based authentication scheme than other authentication schemes. In general, the graphical password techniques can be classified into two categories: recognition-based and recall based graphical technique *et al.*[1].In recognition-based systems, a group of images are displayed to the user and he has to clicked or touched a correct image in a particular order for accept authentication. Some examples of recognition-based system are Awase-E system, AuthentiGraph, and Pass faces system. Even though Awase-E system has a higher usability, due to the storage space needed for images and also the system cannot tolerate replay attack it is difficult to implement. The commercial system Pass faces *et al.*[1] uses images of human faces.

Davis, *et al.*[3] worked on such a scheme and concluded that user's password selection is affected by race and gender. This makes the Passfaces's password somewhat predictable. Although a recognition-based graphical password seems to be easy to remember, which increases the usability, it is not completely secure. It needs several rounds of image recognition for authentication to provide a reasonably large password space, which is tedious *et al.*[3]. 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, we consider these drawbacks in our proposed system, which overcomes the problems of recall based schemes too.

## III. ANALYSIS OF PROBLEM

As we know the biometric system was introduced, as an alternative to the text-base password scheme. But because of it's high cost, it is not eassy to implement. So token based scheme was introduced. Token based systems rely on the use of a physical device such as smartcards or electronic-key for authentication purpose. Graphical-based password techniques is introdused as an potential alternative to text-based technique because we know the fact that humans can remember images better than text. In general, the graphical password techniques can be classified into two categories: recall based and recognition-based graphical techniques. In recall-based systems, the user is asked to reproduce something that he/she created or selected earlier during the registration phase. In recognition-based systems, 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, but there are some drawbacks of these systems, such as:

a. Alphanumeric passwords have problems such as user may forgot the password, dictionary attack, key-logger, vulnerable to guessing, shoulder-surfing and social engineering.
b. The major problem of biometric as an authentication scheme is the high cost of additional devices needed for identification process.
**c.** Although a recognition-based graphical password seems to be easy to remember, which increases the usability, it is not completely secure. It needs several rounds of image recognition for authentication to provide very large password space, which is tedious.

In this proposed work, we specially focus only on "Knowledge based authentication" types of authentication. GPAS is similar to the Pass Point scheme with some finer



CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

differences. In every "Knowledge based authentication 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 GPAS for banking, we consider the piece of information i.e. password as a known to the server at the time of registration and at the time of authentication, the user give this information in an graphical form that can be understood only by the server. The strength of GPAS depends greatly on how effectively the authentication information is embedded graphicaly in an image and it should be easy to decrypt for a legitimate user and highly fuzzy for a non-legitimate user. The authentication information is conveyed graphicaly, that's why No password information is exchanged between the client and the server in GPAS.

## IV. WORKING OF GPAS

In this scheme, we proposed a new Graphical password authentication system where the authentication information graphicaly given to the user. If the user 'click' the graphical images in same seqence he/she given to the server at the time of authentication, the user graphicaly authenticated. No password and information exchange between client and server in GPAS. The shoulder sufering and screen dump attack by which all schemes are suffer, the GPAS can tolerate these attack. As comapaired to other user the GPAS give us a secure authentication because GPAS required human-interaction and careful selection of images and 'click' region.

### *A. An Graphical Password Authentication System:*

An graphical password authentication scheme is siltly similar to pass point scheme .The GPAS is based on "Knowledge based authentication" type of authentication scheme. And in "Knowledge based authentication "type of authenticaton scheme the server give a task to youse by reqesting him/her to reproduse same fact or select a same seqence of images which he/she giveen to the server at the time of registration. Here the password given by user is conciderd as a pice of information give to the server at the time of registration and at the time of authentication. It is explained through a Mobile Banking domain.

### *B. Mobile Banking domain:*

Here we consider mobile banking as our domain. GPAS may be implemented in any client-server environment,where client must be a human user because GPAS will not working machine-to-machine authentication. We also assume that the server has enough hardware resources like RAM and CPU. Here the bank database has a up to 200 questions.During the time of registration user have to give a answers of 10-20 questionds which are he/she selected from the database.The number of questions are depending upon the klevel of sequrity. For example, the user may choose the following questions:

a. What is your favoriet place?
b. What is your hobby?
c. Whaich food do you like to eat?

For each question user has to choose a answer which are provided by server. Server stored this information in to the database by creating a space for this. when user reqest for authentication, the srerver pick the questions from a questions selecterd by user at the time of registration randomly (the number of questions depends on the level of service requested). For each chosen question, the server presented the images as challenge to the user by selecting a images randomly from the authentication space. Using the mouse, the user needs to click the correct image and give a right answer to the server. For example, the server ask the question Which is your favoriet country? Then user has to choose a corect answer from a image provided by server which include right and wrong answers. If the answer is "Austrelia" then user has to choose it from the following image.

The other images may be answer of another questions. But this answer is not shown directly; it is represented by the image in an secrete way. let us conciderd the above example the answer is "Austrelia" but the answer is represented as any place from that country for example the "Austerlia" is represented by "Lotus House". Like that "Gate way of india" represent the country India and so on. Next time, if the same question is chosen by the server, the server may not be presented same group of images. For the next time, the server presentr the image with wrong and right answer and user has to click on "Great Barrier Reef" and so on. The user needs to click on this "Great Barrier Reef" image for correlating it to the answer Austrelia to graphicaly convey his answer. Since every time the server uses a different group of images and the answers are given secretly, the proposed system is immune to screen capture attack.

Figure 4.1 Example of the system

### *C. 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 the server provides their individual answer. For each question, the system then either creates an authentication space (the space that represents graphical answers for the questions using images) if it is not available or add the new user's answer to the existing authentication space.



CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

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 sys-tem 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 up to the user to correlate with the question the image shown on the screen. The proposed system consists of two modules as follows:

a. Web Admin Module
b. Customer Management Module

Web Admin Module: This module is developed for the administrator of the system. Who create and maintain the authentication space (the space that represents graphical answers for the questions using images) and also can change or update the authentication space means the number of questions and answers. Administrator adds the images for questions and then map's the images. Administrator also has to maintain login for individual user. In this module there are following sub modules:

a. Create authentication space using images
b. Change and update authentication space
c. Maintain Log for customers

Customer Management Module: This module is design for the user of the system. Using GPAS each user can create his/her account by filling the registration form. For authentication user has to choose the level of authentication and then depending on level of authentication, i.e. low, high or moderate user has to choose some questions and answers to that respective questions. The sub modules are as follows:

a. Create account using GPAS
b. Define level of authentication
c. Redirect to the services

We are using the concept of cloud sever for the storage of database. Where the administrator has to perform different storage service operations based on client users, such as total cloud storage, cloud rent, payment summary, pending payment, etc. The user has some functions to perform on cloud server, e.g. upload document, download document, total cloud usages, cloud rent, etc.

## V. REFERENCES


[1]. Xiaoyuan, S., Z. Ying, et al. (2005). "Graphical passwords: a survey", Computer Security Applications Conference, 21st Annual.

[2]. Pierce JD, Jason G. Wells, Matthew J. Warren, & David R. Mackay. (2003). "A Conceptual Model for Graphical Authentication", 1st Australian Information security Management Conference, 24 Sept. Perth, Western Australia, paper 16.

[3]. Dirik, A. E., N. Memon, et al. (2007). "Modeling user choice in the Pass Points graphical password scheme", Proceedings of the 3rdsymposium on Usable privacy and security. Pittsburgh, Pennsylvania, ACM.

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

[5]. Masrom, M., F. Towhidi, et al. (2009). "Pure and cued recall-based graphical user authentication", Application of Information and Communication Technologies, 2009. AICT 2009. International Conference.

[6]. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon,``PassPoints: Design and longitudinal evaluation of a graphical password system", International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63 (2005) 102-127.

[7]. Takada, T. and H. Koike (2003). "Awase-E: Image-Based Authentication for Mobile Phones Using User's Favorite Images", Human-Computer Interaction with Mobile Devices and Services, Springer Berlin / Heidelberg. 2795: 347-351.

[8]. Sadiq Almuairfi, Parakash Veeraraghavan and Naveen Chila-mkurti (2011) Workshops of International Conference on Ad-vanced Information Networking and Applications.

[9]. Ms.Prajakta, D.Kulkarni, Mr.C.S.Satsangi**,** Mr.Santhosh Easo. "Authorization using Graphical Password", IOSR Journal of Engineering (IOSRJEN) ISSN: 2250-3021 Volume 2, Issue 7(July 2012), PP 91-95.

[10]. Birget, J. C., H. Dawei, et al. (2006). "Graphical passwords based on robust discretization", Information Forensics and Security, IEEE Transactions on 1(3): 395-399.