ISSN No. 0976-5697

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

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

Cloud based Implicit Password Authentication System

Ms. Chaitali B. Khodani*, Ms. Namrata A. Khodke and Prof. Aditya Bakshi
JDIET, Yavatmal
chaitalikhodani@gmail.com*, namrata.khodke122@gmail.com, aaditya.bakshi009@yahoo.co.in

Abstract: There is increasing coverage in the literature emphasizing threats to online financial systems. Authentication is a process by which a system proves the identity of a individuals. Authentication may also be generalized by saying that "to authenticate" means "to authorize". Authentication is the first line of security against compromising confidentiality and integrity. 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 developed substantially to justify the investment. Thus, a variation to the login/password scheme, i.e. Graphical scheme was introduced.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 implicit manner. We have introduced a framework of our proposed Implicit Password Authentication System (IPAS), which is immune to the common attacks suffered by other authentication schemes**.** 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: Graphical password System, Security, Usability, Reliability, Authentication, mobile banking.

I. INTRODUCTION

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 is known as authentication. This is an important process which assures the basic security goals, i.e. 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. For example, a less sophisticated approach may be used for accessing a "chat server" compared to accessing a corporate database. 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. The resource requirement has become a major factor due to the proliferation of mobile and hand-held devices.

Nowadays with the use of mobile phones, users can access any information including banking and corporate database. We propose our Authentication System for banking using Implicit Password, in which the scheme allows any image to be used and it does not need artificial predefined click regions with well-marked boundaries. A password can be any arbitrarily chosen sequence of points in the image with some finer differences. In IPAS, the server has a piece of information i.e. password at the time of authentication and at the time of registration, the user give this information to the server in an implicit form. Implicit password is particularly suited for mobile phones and portable computers, although it may be implemented for any computer.

There are several authentication schemes available in the literature. They can be broadly classified as: What you know, what you have and what you are. The traditional username/passwordor 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 proposed work, we focus only on "what you know" types of authentication.

II. LITERATURE REVIEW

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. 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*et al.*[1]. 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*et al.*[1]. 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*et al.*[2].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*et al.*[2].

Thus as an alternative, graphical based passwords are introduced to resolve security and usability limitations

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

mentioned in the above schemes. 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*et al.*[3]. Psychologists have confirmed that in both recognition and recall scenarios, images are more memorable than 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. Thus the security level of graphical based authentication schemes is higher than other authentication techniques. In general, the graphical password techniques can be classified into two categories: recognition-based and recallbasedgraphical technique*et al.*[4]. 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. Some examples of recognition-based system are Awase-E system, Authenti Graph, and Pass faces system. 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.

The commercial system Pass faces *et al.*[4] uses images of human faces. Davis, *et al.*[5] 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.*[5]. 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

Earlier the biometric system was introduced, 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. Token based systems rely on the use of a physical device such as smartcards or electronic-key for authentication purpose. Graphical-based password techniques supported partially by the fact that humans can remember images better than text, which have been proposed as a potential alternative to text-based techniques. 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 being hard to remember, 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 "what you know" types of authentication. IPAS 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 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 implicit form that can be understood only by the server. The strength of IPAS 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. The authentication information is conveyed implicitly, that's why No password information is exchanged between the client and the server in IPAS.

IV. PROPOSED WORK

In this proposed work, 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 administrator server, the user is implicitly authenticated. No password information is exchanged between the client and the server in IPAS. Since the authentication information is conveyed implicitly, IPAS can tolerate shoulder-surfing and screen dump attack, which none of the existing schemes can tolerate. 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 this paper, IPAS may require human-interaction and careful selection of images and "click" regions. IPAS may also need user training. Once this is done, IPAS can be more robust.

A. Cloud Based Implicit Password Authentication System:

The proposed cloud based IPAS is similar to the Pass Point 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 gives this information in an implicit form that can be understood only by the server. It is explained through a Mobile Banking domain.

B. Mobile Banking domain:

In our case study, we consider mobile banking as our domain. However, our proposed (IPAS) may also be implemented in any client-server environment, where we

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

need to authenticate a human as a client (IPAS will not working machine-to-machine authentication). We also assume 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:

a. What is your favorite color?
b. What is your favorite food?
c. What is your 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 1. If my favorite food, he needs to click on the relevant image as shown in Figure2.2.

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.

Figure 2.2 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 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 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

a. ***Web Admin Module*****:** This module is developed for the administrator of the system. Who create and maintain the authentication space (the space that represents implicit 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

b. ***Customer Management Module*****:** This module is design for the user of the system. Using IPAS 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 IPAS
b) Define level of authentication
c) Redirect to the services

Lastly 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]. 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.

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

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

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

[5]. 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.

[6]. 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.

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

[8]. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon,``Pass Points: 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.

[9]. 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.

[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.