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

Secured and Implicit Password Authentication to Avoid Attacks

Vivekanandan. S and John Deva Prasanna. D. S,
School of Computing Sciences, Hindustan University

Abstract

Authentication is the first line of defense 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 improved. Thus, a variation to the login/password scheme, viz. graphical scheme was introduced. But it also suffered due to shoulder-surfing and screen dump attacks. In this paper, we introduce a framework of our proposed IPAS, which is immune to the common attacks suffered by other authentication schemes. At the time of registration, a user should pick some questions from the database depending upon the level of security required and provide answers to the selected questions. 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. For each chosen question, the server may choose an image randomly from the authentication space and present it to the user as a challenge. The user needs to navigate the image and click the right answer. Once the key is matched, the verification is done and processes are preceded. Then, encryption and decryption processes are performed. If the key match is confirmed, further functions are done and then user login is successful. Else it is rejected and again the process initiates from the beginning leading to secure authentication. The advantage of the system is that it is immune to shoulder surfing and screen dump attack and the authentication information is presented to the user in an implicit form that can be understood and decoded only by the legitimate user.

.

Keywords: *Implicit Password Authentication System(IPAS), RSA algorithm,Authentication.*

1.Introduction

Text passwords remain ubiquitous, despite endless criticism. People consistently choose weak passwords for many reasons, including users trying to manage on average 25 password-protected accounts. Losing strategies include blaming users, and imposing complex password rules. Some claim that choosing weak password is a rational economic response. Some argue that strong passwords are nonessential for preventing automated online dictionary attacks. However implicit password authentication system may be implemented in any client-server environment, where we need to authenticate human as a client. During the time of registration, a user should pick some questions from the database depending upon the level of security required and provide answers to the selected questions. For every question the server may create an intelligent space using images, where the answer to the particular question is implicitly embedded into images. During the time of authentication, the server may pick one or more questions selected by the users at the time of registration randomly. For each question, the server may choose an image randomly from the authentication space and present it to the user. Using the stylus or the mouse, the user needs to navigate the image and click the correct image. Implicit password authentication system is immune to shoulder surfing and screen-dump attack. The authentication information is presented to the user in an implicit form that can be understood and decoded only by the legitimate user. The strength of Implicit password authentication system depends 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 difficult for a non-legitimate user. Traditional password based authentication schemes and Pass Point are special cases of implicit password authentication system.

2.Literature Survey

2.1.Universal multifactor authentication using graphical passwords

Graphical password is used to make the passwords more secure. To determine the appropriate click points and their order, the user needs some hint information transmitted only to her handheld device. We show that our method can overcome threats such as key-loggers, weak password, and shoulder surfing. With the increasing popularity of handheld devices such as cell phones, our approach can be leveraged by many organizations without forcing the user to memorize different passwords or carrying around different tokens .In most of the schemes, graphical password employs graphical presentations such as icons, human faces or custom images to create a password. [1]

2.2. Graphical password: A survey

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. 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. This survey will be useful for information security researchers and practitioners who are interested in finding an alternative to text-based authentication methods. [4]

2.3.Graphical authentication system for online banking system

The co-ordinates of each character rendered to the image is stored on the server in the form of a rectangle that defines the position on the image the character was drawn along with a unique session id to identify which image the client was sent. The image is returned to the client and rendered to the browser according to the applications requirements. The user then selects the characters from the screen with the mouse. Each mouse click co-ordinates are stored on the client in the order they were collected. When the user has completed selecting the information, the browser packages up the co-ordinates and returns them to the server. The server then processes each co-ordinate set received and attempts to map each point to a rectangle and subsequently retrieve the character that was originally drawn on the screen. The server builds a character string in the order dictated by the co-ordinates returned and then either uses the character string to check authentication data. [5]

2.4.The design and analysis of graphical passwords

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. We design and analyze graphical passwords. A graphical password serves the same purpose as a textual password, but can consist, for example, of handwritten designs, possibly in addition to text. The devices by which we are primarily motivated are PDAs such as the Palm Pilot TM, Apple Newton TM, Casio Cassiopeia E-10TM, and others, which allow users to provide graphics input to the device via a stylus. More generally, graphical passwords can be used whenever a graphical input device, such as a mouse, is available. That work proposed a password scheme in which the user is presented with a predetermined image on a visual display and required to select one or more predetermined positions on the displayed image in a particular order to indicate his or her authorization to access the resource. [2]

2.5.Modeling user choice in the pass points graphical password scheme

The main motivation for graphical passwords is the hypothesis that people are better at remembering images than artificial words. Visual objects seem to range over a much larger set of usable passwords. For example we can recognize the people we know from thousands of faces. This fact was used to implement an authentication system. As another ex-ample, a user could choose a sequence of points in an image as a password; this leads to a vast number of possibilities, if the image is large and complex, and if it has good resolution. An excellent survey of the numerous graphical password schemes that have been developed in this paper. [7]

3.Existing System

In the existing system, alphanumeric passwords are hard to remember. It is vulnerable to guessing, dictionary attack, key-logger, shoulder-surfing and social engineering. User may tend to choose a weak password or record his password. The major problem of biometric as an authentication scheme is its high cost of additional devices needed for identification process. The concept of image is secure compared to text passwords but the drawback is that images need more techniques for its accessibility. The biometric systems are vulnerable to replay attack. 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. All these issues make the password weak and also easily retrievable.

4. Proposed System

We consider mobile banking as our domain. However, our proposed IPAS may also be implemented in any client-server environment, where we need to authenticate a human as a client. 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. The bank may have a database of standard questions. During the time of registration, a user should pick some questions from the database depending upon the level of security required and provide answers to the selected questions. 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 correct answer.

5.IPAS System

5.1. System Architecture

Figure 1: Represents the architecture of an extended Implicit-Password Authentication system. It consists of Seven Modules. They are,

- Client
- Server
- Encryption and Decryption
- Image Generation
- Key generation using sms
- Authentication
- Transaction

The proposed algorithm efficiently handles the security issues. The entire processing of the system is depicted through the architecture phase.

The flow for the entire process is manipulated. The literature reviews are made after which the modules are identified, apart from which the functions of the modules are stated.

The proposed algorithm fits itself perfectly by improving the efficiency of the password and also makes the authentication more safe and secure.

The extended IPAS makes the transactions more convenient by presenting the password more securely.

This depicts itself a perfect authentication scheme and the chances of fraudulent and hacking are much reduced.

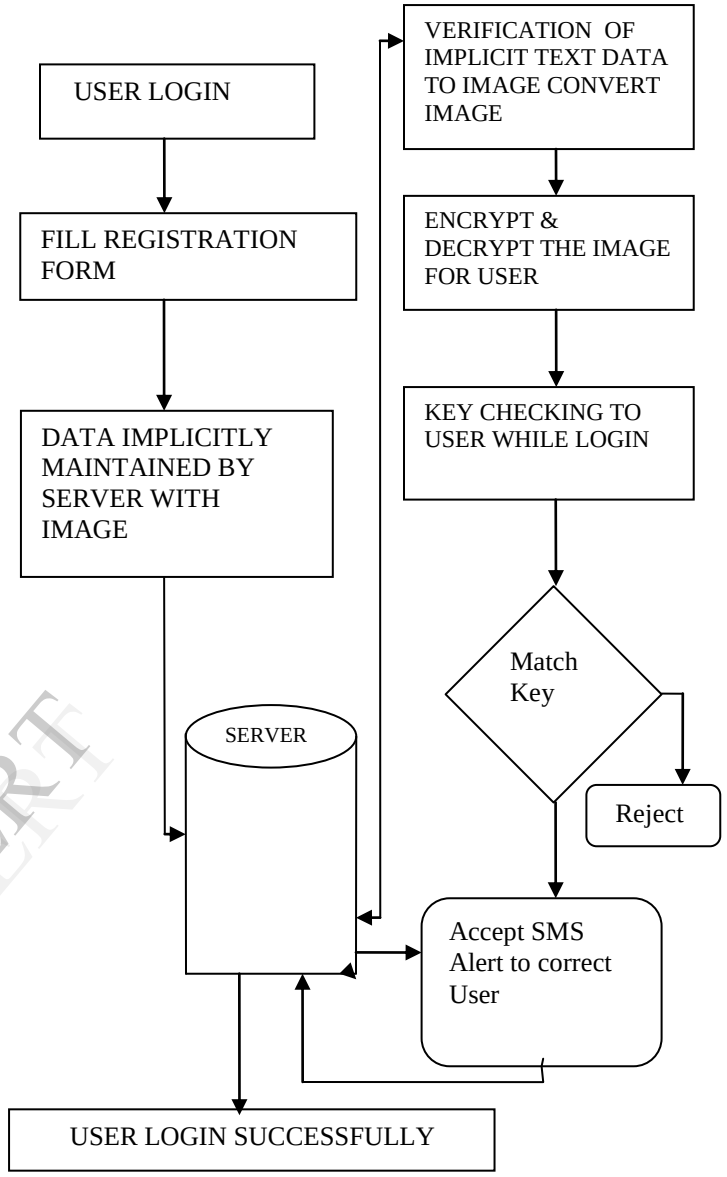


Figure 1: IPAS architecture

5.2. Module Description

5.2.1. Client

This module plays a vital role in this project because this is deviated from normal registration process. Because in this module, the client will register all his authentication information along with his user name, ID, age, sex, mobile number, address along with security questions. All the information is stored in the main server for authentication.

5.2.2. Server

Server acts as the main resource for the client. Server is responsible for maintaining all the client information. Server will generate a random number which is encrypted using RSA algorithm and the image is generated according to the answers made by the user during the registration process. Server will finally authenticate the user.

5.2.3. Encryption and Decryption

Encryption is the most effective way to achieve data security. To read encrypted information, you must have access to a secret key or password that enables you to decrypt it. A random number is taken by the server which is encrypted and is provided to the user along with the set of images which represents the answers made by the user during the registration period. The encryption is made using RSA algorithm.

5.2.4. Image Generation

A set of images are generated by the server based on the answers made by the user during the registration period. One relevant image is displayed in a random pattern and other set of irrelevant images along with the encrypted data. User will select the correct image by proper judgment of correct answer with respect to the answers made during the registration period.

5.2.5. Key Generation Using Sms

This module is used to generate session for the login client. If the user is an authenticated person, he gets his session via mobile using which the client can perform further transaction. Thus a hacker cannot know or access transaction since he doesnt know the session. This generation of the password is achieved by real-time mobile connected. The mobile number of the user is obtained from the server. A random value is send as SMS to the mobile number of the user for further authentication to avoid any further attacks.

5.2.6. Authentication

The User ID is verified in the registration process and the image verification is done by the server, based on the answers

made by the user during the registration period. One relevant image is displayed in a random pattern and other set of irrelevant images along with the encrypted data. After random number or session key verification, the user is allowed for further process.

5.2.7. Transaction

If the client completes all of the authentication process then the system allows the user to continue his transaction like

deposit, withdraw, mini statement and so on. At the time of each and every transaction, server must authenticate the user.

5.3. Impact of IPAS

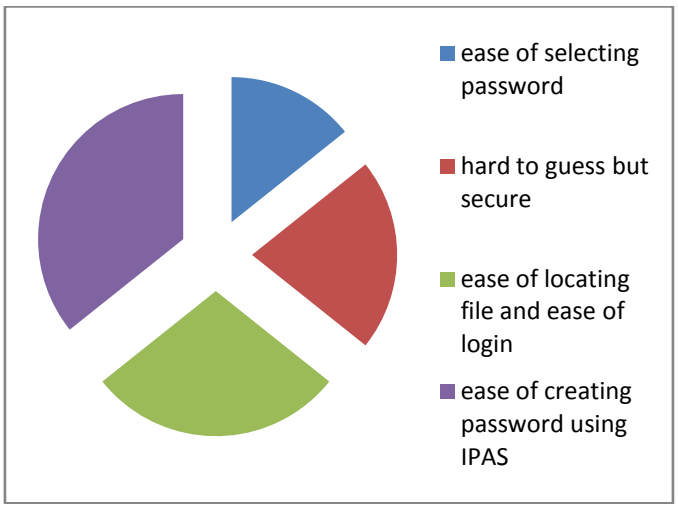
- Currently used security systems are not efficient as the proposed system.
- IPAS is immune to shoulder surfing and screen-dump attack IPAS is immune to shoulder surfing and screen-dump attack.
- The authentication information is presented to the user in an implicit form that can be understood and decoded only by the legitimate end user.
- 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.
- Traditional password based authentication schemes and Pass Point are special cases of IPAS.

6.Analysis Report

The level of usability is based on four factors. They are,

- ease of thinking of a file to select for the password;
- ease of locating the file chosen;
- ease of creating the password using IPAS;
- ease of logging into the website with the chosen password.

The user's suggestions of using IPAS are,
About 20% of users – easy of selecting the password.
About 30% of users – thought hard to guess and thought more secure.
About 40% of users – finds ease of locating the file.
About 20 to 50% of users – easy of creating password using IPAS.
About 20 to 40% - ease of logging into the website with the chosen password.



7.Conclusion and Future Enhancement

7.1. Conclusion

Implicit password is a more secure compared with the existing system. This system can be implemented in places where security is poor or additional security is needed. This concept can be used extensively in the field of banking since transactions are prone to more fraudulent. Hacking of password is impossible because password can be hacked but the implicit password cannot be hacked , only the legitimate user identify the implicit password. Also, text passwords can be retrieved through techniques like key logger , shoulder surfing and screen dump so on. But, implicit password cannot be retrieved since no trial and error methods can be applied on it. The reference observations clearly state that passwords face a number of issues regarding their security and those issues can be resolved in this project.

7.2. Future Enhancement

Images are currently implemented in this system. . In future, all types of digital objects can be implemented depending upon the usability This system is currently tested in banking applications. We intend to extend the application to other types of fields too.

REFERENCES

[1] Sabzevar, A.P. & Stavrou, 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] 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.

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

[5] Wells, Jason; Hutchinson, Damien; and Pierce, Justin, "Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication, formation Security Management *Conference. Paper* 58.

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

[8] Wei-Chi, K. and T. Maw-Jinn (2005). "A Remote User Authentication Scheme Using Strong Graphical Passwords", *Local Computer Networks, 2005*. 30th Anniversary.

[9] Lashkari, A. H., F. Towhidi, et al. (2009). "A Complete Comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms", *Computer and Electrical Engineering, 2009.* ICCEE '09. Second International Conference.

[10] Renaud, K. (2009)."On user involvement in production of images used in visual authentication." *J. Vis. Lang. Comput*. 20(1): 1-15.

[11] 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.

[12] 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.

[13] 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.

[14] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, ``Authentication using graphical passwords: Effects of tolerance and image choice", *Symposium on Usable Privacy*

and Security (SOUPS), 6-8 July 2005, at Carnegie-Mellon Univ.,Pittsburgh.