International Journal of scientific research and management
(IJSRM) ||Volume|| 1 ||Issue|| 4 ||Pages|| 168-175 ||2013||
Website: www.ijsrm.in ISSN (e): 2321-3418

Audio Signature in Graphical Password Authentication System

Deepasree P O[1], Avanish Kumar Singh[2]

[1]Nehru College of Engineering and Research Center, Department of Computer Science and Engineering, Pampadi, Thrissur, Kerala, India
[1]deepasree.po@gmail.com , [2]aavi13@gmail.com

Abstract: ***Graphical passwords, which consist of clicking or dragging activities on the pictures rather than typing textual characters, might be the option to overcome the problems that arise from the text-based passwords system. An important usability goal for knowledge-based authentication systems is to support users in selecting passwords of higher security, in the sense of being from an expanded effective security space. User is asked to select a sound signature, which helps the user in order to remember the click-points during login phase even if the user tries to login after a long time, and a tolerance dimension during password creation process. Persuasion is used to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points.***

Keywords: ***Sound signature, Authentication, Tolerance dimension, Human factors.***

1. INTRODUCTION

Human factors are often considered the weakest link in a computer security system. There are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. It is now beyond any doubt that user authentication is the most critical element in the field of Information Security. For the vast majority of computer systems, passwords are the method of choice for authenticating users. Authentication is the first step of information security. Authentication refers to the process of confirming or denying an individual's claimed identity. Authentication schemes require users to memorize the passwords and recall them during log-in time. Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords.

The primary goal of improving the current user authentication technology is to make the method secure yet easier for the user. Graphical password authentication systems (GPAS), which consist of clicking or dragging activities on the pictures rather than typing textual characters, might be the option to overcome the problems that arise from the text-based password system. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated particularly by the fact that humans can remember pictures better than text. Psychological studies have shown that people can remember

pictures better than text. Pictures are generally easier to be remembered or recognized than text, especially photos, which are even easier to be remembered than random pictures. It has also been suggested that graphical passwords may be hard to guess or broken by brute force search. If the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer better resistance to dictionary attacks. Because of these advantages, there is a growing interest in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applied to ATM machines and mobile devices.

This project tries to propose an authentication mechanism which supports both usability and security. Cued click points (CCP) is a click-based graphical password scheme, a cued-recall graphical password technique. In addition user is asked to select a sound signature during registration process. Various GPAS have been proposed as alternatives to text-based passwords. It can be used as password for folder lock, web-driven applications, desktop lock etc.

1.1 Objective

The objective of this project is to provide the security for any folders in a computer system by using graphical passwords with view port, sound signature and persuasive cued click-points. Here a graphical password system with a supportive sound signature to increase the remembrance of the password is developed. Here a click-based graphical password scheme called Cued Click Points is presented. In this system, a password consists of sequence of some images in which user can select one click-point per image. The next image is based on the previous click-point. During login phase, if the selected click-point is not the appropriate one then the system will load an image which is not a part of the password image-sequence. In addition user is asked to select a sound signature during registration phase. This sound signature will be used to help the user in recalling the click point on an image during login phase. That is, during login phase, if the user clicks the appropriate point on the image then the sound that the user selected during registration phase will be played. Persuasion is used to influence user choice in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points. It can be used as password for folder lock, hard disk locking, web-driven applications, desktop lock etc.

1.2 Problem Statement

A major goal of this research is to discover how to create knowledge-based authentication schemes that are memorable, usable, and secure. The interplay between usability and security, an issue that is not well understood in current systems, is also investigated. The research is focused on click-based graphical passwords because of their potential for increased memorability and security. The main research question is: Can click-based graphical passwords simultaneously support both memorability and security, while maintaining usability? The work began with a general investigation, with new ideas being formed and tested as progressed with the research.

In this project, a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. The main objective in graphical password authentication is to provide the sound signature in graphical system and reduce the chances to forget the password. Another problem is the presence of hotspots. Hotspots are areas of the image that have higher likelihood of being selected by users as password click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully guess PassPoints[1] passwords. In order to reduce selecting the hotspots, implementation of viewport is essential. CCP are used to develop this system, because CCP reduce the time limit & increase the system speed and accuracy. Users preferred CCP to PassPoints, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.

2. SYSTEM ANALYSIS

System analysis or study is an important phase of any system development process. The system is studied to the minute detail and analyzed. The system analyst dwelled deep into the working of the present system. The system was viewed as a whole and the input of the system are identified. During analysis phase for each problem identified many alternative solutions were evaluated and selected the most feasible one. A feasibility analysis was performed to evaluate possible solutions to recommend the most feasible one.

2.1 Initial Study

The first step in the system development life cycle is the identification of a need. This is a user's request to change, improve, or enhance an existing system. Because there is likely to be stream of such requests, standard procedures must be established to deal with them. The initial investigation is one of handling this. The objective is to determine whether the request is valid and feasible before a recommendation is reached to do nothing, improve or modify the existing, or build a new one.

The user's request specifies the following:

- Nature of work requested
- Expected benefits to be derived from proposed change
- Input and output description
- Requesters signature, title and development
- Signature, title and department of person approving the request

The user's request identifies the need for change and authorizes the initial investigation. It may undergo several modifications before it becomes a written commitment. Once the request is approved, the following activities are carried out. Background investigation, fact-finding and analysis and presentation of results is called project proposal. The proposal, when approved, initiates a detailed user-oriented specification of the system performance and analysis of the feasibility of the system. A feasibility study focuses on identifying and evaluating alternative systems with a recommendation of the best system. This deals with initial investigation.

The major steps in defining user requirements are:

- Studying the present system
- Verifying the problem
- Defining the performance expected by the system

2.2 Background Investigation

Once the project is initiated, the analyst begins to learn about the setting, the existing system and the physical processes related to the revised system. The analyst should prepare an organization chart with a list of the functions and the people who perform them.

2.3 Fact-Finding

After obtaining the background knowledge, the analyst begins to collect data on the existing system's outputs, inputs and costs.

Interviews and questionnaires: In this method, questions are asked to the user to study his views and ideas. The quality of the response is judged in terms of its reliability and validity. In an interview, since the analyst and the person interviewed meet face to face, there is an opportunity for greater flexibility in eliciting information.

2.4 Detailed Study

Analysis is a detailed study of the various operations performed by the system and the relationship within and outside the system. One aspect of analysis is defining the boundaries of the system and determining whether or not a system should consider other related system. During analysis, data is collected on the available files, decision points, and transactions handled by the present system. In system design, we move from logical to the physical aspects of life cycle.

- Analyze the findings and records the results
- Define the document in outlining the proposed system
- Test the purpose to design against the known facts
- Estimate the resources needed to design and implement the system, its failure and problem

2.5 Feasibility Study

After the problem is clearly understood and solutions proposed, the next step is to conduct the feasibility study. Many feasibility studies are disillusioning for both users and analysts. Feasibility study is defined as evaluation or analysis of the potential impact of a project or program. The objective is to determine whether the system is feasible. First, the study often pre-supposes that when the feasibility document is being prepared. The analyst is in a position to evaluate solutions. Second, most studies tend to overlook the confusion inherent in system development: the constraints and the assumed attitudes. Three key considerations are involved in the feasibility analysis: economic, technical and operational.

2.5.1 Operational Feasibility

Operational feasibility determines if the human resources are available to operate the system once it has been installed. The resources that are required to implement or install are already available with the organization. The persons of the organization need no exposure to computer but have to be trained to use this particular software. A few of them will be trained. Further, training is very less. The management will also be convinced that the project is optimally feasible.

2.5.2 Economic Feasibility

Economic feasibility determines whether the time and money are available to develop the system. It also includes the purchase of new equipment, hardware, and software. A software product must be cost effective in the development, on maintenance and in the use. Since the hardware and resources are already available with the organization, the organization can afford to allocate the required resources.

2.5.3 Technical Feasibility

Technical feasibility assesses whether the current technical resources are sufficient for the new system. If they are not available, can they be upgraded to provide the level of technology necessary for the new system? It checks whether the proposed system can be implemented in the present system without supporting the existing hardware.

3. SOUND SIGNATURE IN GPAS

3.1 Existing System

In the existing system**,** Brostoff and Sasse carried out an empirical study of passfaces, which illustrates well how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation, the user chooses several predefined regions in an image as his or her password. To log in, the user has to click on the same regions in effect. PassPoints proposed passwords, which could be composed of several points anywhere on an image.

Cued click points is a proposed alternative to PassPoints. In Cued click-points, users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point. It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in effect leading users down a “path” as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. While the predictability problem can be solved by disallowing user choice and assigning

passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Number of graphical password systems has been developed. Study shows that text-based passwords suffer with both security and usability problems.

3.2 Drawbacks of Existing System

Although PassPoints is relatively usable, security weaknesses make passwords easier for attackers to predict. It seems obvious that some areas of an image are more attractive to users as click-points. Hotspots are areas of the image that have higher likelihood of being selected by users as password click-points. If this phenomenon is too strong, the likelihood that attackers can guess a password significantly increases. If attackers learn which images are being used, they can select a set of likely hotspots through image processing tools or by observing a small set of users on the target image and then building an attack dictionary based on those points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can more successfully guess PassPoints passwords. Users also tend to select their click-points in predictable patterns, which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against PassPoints based on image processing techniques and spatial patterns are a threat.

3.3 Proposed System

A password authentication system should encourage strong passwords while maintaining memorability. It is proposed that authentication schemes allow user choice while influencing users toward stronger passwords. In this system, the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes choosing a more secure password the path of least resistance. Rather than increasing the burden on users, it is easier to follow the system's suggestions for a secure password – a feature lacking in most schemes. This approach is applied to create the first persuasive click-based graphical password system; Persuasive cued click-points (PCCP).

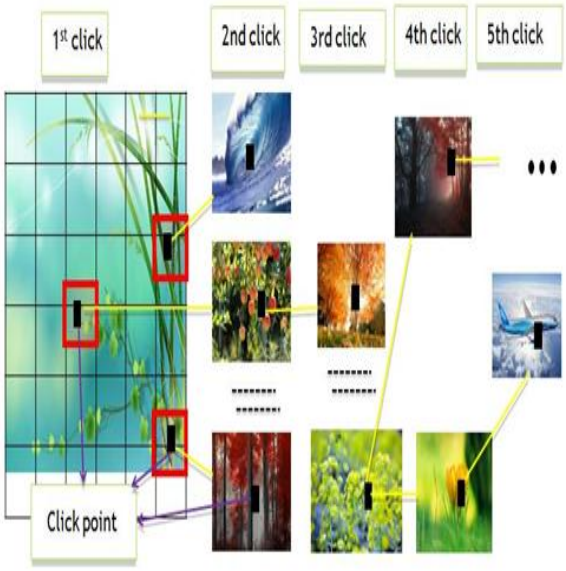

Figure 3.1 PCCP click-points Scenario

In addition a sound signature is integrated to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text. In daily life, we can see various examples of recalling an object by the sound related to that object. User enters username and selects a music which he wants to be played at login time. A tolerance value is also selected which will decide that the user is legitimate or an imposter. CCP is the best graphical password authentication technique. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point at which point they can cancel their attempt and retry from the beginning. Also number of login attempts is limited to three.

3.4 Advantages of Proposed System

This systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues, to advance understanding as is prudent before practical deployment of new security mechanisms. Here login attempt is restricted among users. Results show that PCCP is effective at reducing hotspots and avoiding patterns formed by click-points within a password, while

still maintaining usability. Users preferred CCP to PassPoints, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points. System shows very good performance in terms of speed, accuracy, and ease of use.

3.5 System Implementation

The implementation has mainly three modules:

1) Create Password Module
2) Login Module
3) Verification Module
4) Folder Lock/Unlock Module

Create Password Module: PCCP encourages users to select less predictable passwords, and makes it more difficult to select passwords where all five click-points are hotspots. Specifically, when user creates a password, user selects a click-point within each selected image. User is also asked to select the tolerance dimension during password creation. In addition user is asked to select a sound signature or music which helps the user in order to remember the click-points during login phase even if the user tries to login after a long time.

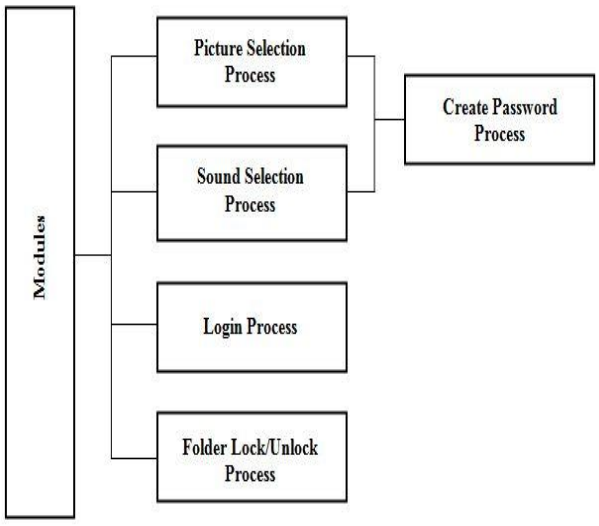

Figure 3.2 Module Description

Login Module: In login module, the user can give their username and password. In addition, a sound signature is integrated to help in recalling the password. Hacking of username and password can be done. But if the pixels are pointed out correctly, then only one can login in to user page. During login phase, username is taken from the user and is stored in corresponding variable. If the entered value matches the data in the database which is stored earlier, it will display corresponding user's first image which is selected previously during registration session. And the user can select their previously chosen images by clicking on the specific region or point chosen earlier. After repeating the same steps for all the images, comparisons are made. Even if the point chosen in the image was wrong, the user will not be informed about the wrong path which reduces the ability of hacker to guess the password. Else the user is directed to the home page where they can lock or unlock the folders and can also able to change their password as well as the music. During login, if the pixels are clicked correctly, then the selected sound is started to play. Else any other sound will be played. Here number of login attempts is limited to three since an extra protection is essential to our password-protected system. Security is the main reason to restrict access. Login attempt-limit blocks a user from making further attempts after a specified limit on retries is reached.

Verification Module: During verification phase, the details that the user enters during registration phase and login phase are verified.

Folder Lock/Unlock Module: Protecting your data and information from certain unwanted and prying eyes may become a dilemma if you end up with enough personal and private data on your computer or on your external storage devices. With information changing hands and data transfer figures at record numbers, critical files and folders like these need robust protection so that intruders or unauthorized users are stopped right in their tracks – whether to read, view, copy, move or delete them. If it is personal or confidential, it needs protection! Folder lock uses GPAS for protecting your files.

3.6 System Environment

This is a desktop application developed using JAVA as front end and MySql as the back end. Eclipse IDE is used, which is a multi-language software development environment.

3.6.1 Software Requirements

OS	: Windows/Linux
Language	: Core java, Jsp servlet
IDE	: NetBeans
Database	: MySQL

3.6.2 Hardware Requirements

Processor	: Pentium based systems
RAM	: 512MB (minimum)
Hard Disk	: 80 GB
Monitor	: 15 VGA Color

3.7 Methodology

An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. The proposed system accomplishes this by making the task of selecting a weak password more tedious and time-consuming. The goal is to encourage compliance by making the less secure task more time consuming and awkward. A sound signature is added to this system in order to help the user in recalling the click point on an image during login phase. During registration phase, user is asked to select a sound signature or music. That is, during login phase, if the user clicks the appropriate point on the image then the sound that the user selected during registration phase will be played.

CONCLUSION

The general goal is to make the password easy to remember and to increase the security of knowledge-based authentication schemes. Here the focus is on click based graphical passwords. The existing schemes are investigated for designing a new graphical password authentication scheme. It is possible to increase both simultaneously through careful design that considers usability and security in combination. The need for thorough usability and security evaluations is emphasized, because system design can significantly impact user behavior, sometimes in unanticipated ways, which in turn can significantly impact the security of a system.

This system shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over PassPoints in terms of usability. Being cued as each images shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. Also the sound signature helps the user to remember the click-points even if the user tries to login after a long time.

CCP offers a more secure alternative to PassPoints. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images. In future development we can also add challenge response interaction. In challenge response interactions, server will present a challenge to the client and the client need to give response according to the condition given. If the response is correct then access is granted.

REFERENCE

[1] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. "PassPoints: Design and evaluation of a graphical password system", *International Journal of Human Computer Studies*, 2011.

[2] K. Renaud. “On user involvement in production of images used in visual authentication”, *Journal of Visual Language and Computing*, 2008.

[3] P. Golle and D. Wagner. “Cryptanalysis of a cognitive authentication scheme”, *IEEE Symposium on Security and Privacy*, May 2007.

[4] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud. “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems”, *International Journal of Human-Computer Studies*, 63(1-2):128-152, 2005.

[5] D. Davis, F. Monrose, and M. Reiter. “On user choice in graphical password schemes”, *13th USENIX Security Symposium*, August 2004.

[6] D. Weinshall and S. Kirkpatrick. "Passwords You’ll Never Forget, but Can’t Recall”, *Proceedings of Conference on Human Factors in Computing Systems (CHI) ACM*, Vienna, Austria, pp. 1399-1402., 2004.

[7] J. Thorpe and P. C. v. Oorschot. "Towards Secure Design Choices for Implementing Graphical Passwords”, *20th Annual Computer Security Applications Conference (ACSAC) IEEE*, Tucson, USA, 2004.

[8] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom. "Picture Password: A Visual Login Technique for Mobile Devices," *National Institute of Standards and Technology Interagency Report NISTIR 7030*, 2003.

[9] L. Sobrado and J.-C. Birget. "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.

[10] R. Dhamija and A. Perrig. "Deja Vu: A User Study Using Images for Authentication," *Proceedings of 9th USENIX Security Symposium*, 2000.

[11] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. "The Design and Analysis of Graphical Passwords," *Proceedings of the 8th USENIX Security Symposium*, 1999.

[12] A. F. Syukri, E. Okamoto, and M. Mambo. "A User Identification System Using Signature Written with Mouse," *Third Australasian Conference on Information Security and Privacy (ACISP)*, Springer-Verlag, 403-441, 1998.

[13] J. Anderson and G. Bower. “Recognition and retrieval processes in free recall”, *Psychological Review*, March 1972.

[14] L. Standing, J. Conezio, and R. Haber. “Perception and memory for pictures: Single-trial learning of 2500 visual stimuli”, *Psychonomic Science*, 19(2):7374,1970.