Proactive Cued Click Points:A Sound Signature Integrated Graphical Password Authentication Mechanism

Sarisha Satheesan, A. Ilayarajaa

Abstract—This system presents an innovative idea that integrates graphical passwords with sound signature. The system encourages the user to select click points from images as their passwords rather than textual words. According to human psychology, one can memorize the click points easily when compared to the textual passwords. The number of click points and the number of images included in the password creation depend upon the user's choice. Apart from the click points, the system provides sound files that can be integrated to the user's password. While logging in, the system verifies the click points as well as the sound file. Hence the system provides an efficient method to create more secured passwords which are easier to manage.

Keywrods— Authentication, Graphical Password, Sound Signaure, Secure Password Creation.

I. INTRODUCTION

Commonly followed user authentication schemes, like user accounts and text based passwords have different sort of unsolved complications. Users need to handle different passwords at a time for different purposes such as email accounts, internet banking, other user accounts etc. The users often build passwords that are easy to remember, but they are more vulnerable for the hackers to guess.

An efficient authentication mechanism should encourage the users to select passwords that are strong as well as easy to remember. In our system, it is difficult to select weak passwords that are easy to guess by the hackers. This system gives appropriate suggestion for the users to select strong passwords by using different techniques. On seeing the image the user can easily memorize his password rather than textual passwords. Certain websites like banking websites etc. demands the users to change their passwords frequently. In that case also our system will be very efficient and effective in creating new passwords as it reduces the user's burden in creating strong passwords.

This system presents an innovative idea that integrates sound signature technology into graphical password scheme. The system allows the user to select click points from images as their password. The number of click points and the number of images to be included depend upon the user's choice.

Along with the click points user can also select an audio file by the time of password creation such that one audio file for one click point. While logging in, the user's click points as well as audio files are verified. If both are correct, the selected audio file will be played as indication for secure logging in. Otherwise the sound will not be played.

The next image loaded in our scheme is done using LSB algorithm, which selects the new image randomly. In effect the next image loaded depends only on the recent click point rather the order in which they are stored in the database.

The new system will not show any message saying the incorrect password. The user can log in only when the click points are correct. Otherwise the next image will be loaded based on the recent click point and this will continue indefinitely. Hence the attackers can't even understand whether they are proceeding in the correct way of guess or not.

II. LITERATURE SURVEY

The following are some of the papers reviewed to get an idea of the different systems existing in the relevant area. Text passwords are the most popular user authentication method, but have security and other related problems. Alternatives such as biometric systems and electronic cards or chips have their own drawbacks. An alternative method for this is Graphical Password System.

In the paper, performance of haze-base quantum key two server user password authentication for internet services, the authentication system uses passwords to authenticate user login and stores the password in a central server. The central server is easily prone to attack and if they are being compromised by the intruder, it is possible for the intruder to obtain the password and gain access to the contents of the user. To overcome this problem, the multi-server systems were being proposed in which the user has to communicate in parallel with several or all of the servers for the purpose of authentication. Multi-server system requires a large communication bandwidth and needs for synchronization at the user. To overcome these problems the two server authentication system proposed here uses only passwords and the session keys rather than performing any cryptographic techniques. The two server system is particularly suitable for resource-constrained users due to its efficiency in terms of both computation and communication.

Revised Manuscript Received on March, 2013.

Ms. Sarisha Satheesan, Department Of Computer Science and Engg, Annai Mathammal Sheela Engineering College, Namakkal Dist., Tamil Nadu, India.

Asst. Prof. A Ilayarajaa, Department Of Computer Science and Engg, Annai Mathammal Sheela Engineering College, Namakkal dist., Tamil Nadu, India,.

The proposed work presented a user friendly secured password authentication system with two servers by utilizing quantum channel. To start with, built user friendly browser extension password hash transparently produces a different password for each site, improving web password security. To improve the single server security problems, they created an efficient two server password authentication system.

In the paper, Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords; Cued Gaze-Points (CGP) is a shoulder-surfing resistant cued-recall graphical password scheme. This system has several advantages over similar eye-gaze systems, say a larger password space and its cued-recall nature that can help users remember multiple distinct passwords. CGP's usability is almost acceptable

In the paper, User interface design affects security - Patterns in click-based graphical passwords; design of the user interface for authentication systems influences users and may encourage either secure or insecure behavior. In this system, post-hoc analysis looks at click-point patterns within passwords and shows that Pass Points passwords follow distinct patterns. Cued Click-Points (CCP) and Persuasive Cued Click-Points (PCCP) passwords are nearly indistinguishable from those of a randomly generated dataset. These results provide insight on generating effective password spaces

In the paper, Exploiting Predictability in Click-based Graphical Passwords; they provide an in-depth study of the security of click-based graphical password schemes like Pass Points, by exploring popular points (hot-spots), and examining strategies to predict and exploit them in guessing attacks. This provides empirical evidence that hotspots do exist for many images, some more so than others. Here they explore the use of "human-computation" to predict these hotspots. They also begin to explore some click-order pattern attacks. Their results suggest that these graphical password schemes are vulnerable to offline and online attacks.

In the paper, Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords; the usability effects of modifying system parameters to increase the security of a click-based graphical password system. Usability tests for graphical passwords have used in password spaces smaller than that of common text passwords. The lab study compares the effects of varying the number of click-points and the image size. There is no usability advantage was evident between more click-points. This is a contradiction to our expectation that larger image size (with fewer click-points) might over usability advantages over more click-points (with correspondingly smaller images). The results suggest opportunities for better matching graphical password system. We can use more click-points on smart phone displays where larger image sizes are not possible.

III. EXISTING SYSTEM

Different authentication schemes like user accounts with text-based passwords, biometric authentication schemes, electronic cards or chips etc. have their own problems in authorization. Our focus of study deals with graphical password authentication scheme and their issues.

- Click- Based Graphical Password System

The systems that use graphical passwords may use some images as their passwords. In click based graphical passwords system, the click points in an image is selected as the password. These click points or pixels are also known as pass points

In Pass Point System, the user can select click points from a sequence of images as their password. To log in, the user must repeat the same sequence of pass points. Otherwise the images will load indefinitely disabling the user from logging in to the system. It is quite difficult to point to the exact click point again and again; therefore the user is allowed to click over small range surrounding the original point. This square is known *tolerance square*. In an image, there are attractive regions known as *hot spots.* There is chance for the user to select hot spots as their password click points. In that case, the hackers may guess the click points from the hot spots.

- Persuasive Cued Click Points

In persuasive cued click points, the persuasive technology is incorporated. The persuasive technology makes the task of creating weak passwords very tedious and time consuming. Thereby it encourages the user to select highly secure passwords very easily. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not depends on system-generated passwords. To be effective, the users must use the persuasive elements and the resulting passwords must be memorable.

Visual attention research shows that different people are attracted to the same predictable regions in an image. If users select their own click-based graphical passwords without guidance, hotspots will remain an issue. The older versions suggest that user choice in all types of graphical passwords is inadvisable due to predictability. The system may influence users to select more random click-points while maintaining usability. The goal was to encourage more secure behaviour by making less secure choices (i.e., choosing poor or weak passwords) more time consuming In effect, behaving securely became the safe path of least resistance

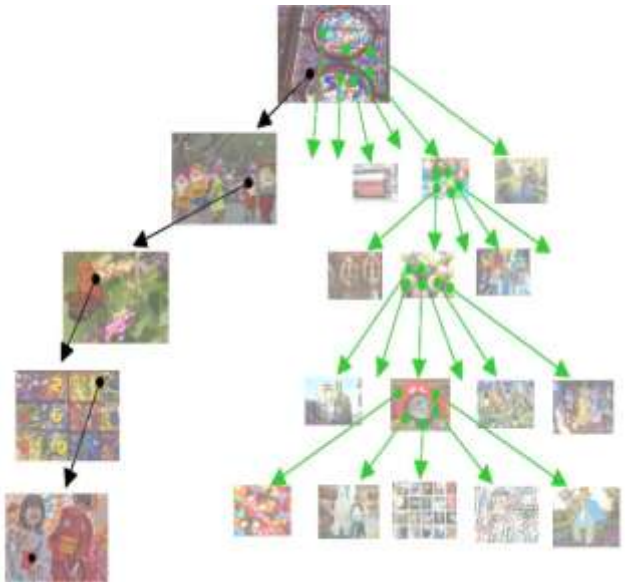

Fig. 1 Each click point in the same image leads to different next image

In this system the next image to be loaded depends upon the previous click point. It means that from a single image, different click points may lead to different images. (Fig. 1) This is implemented by the usage of LSB algorithm. For each click point or pixels in an image may lead to different sequence of images for password creation. This is the main advantage of persuasive technology in graphical password authentication scheme. The path of images for correct selection will differ from that of wrong selection. (Fig. 2)

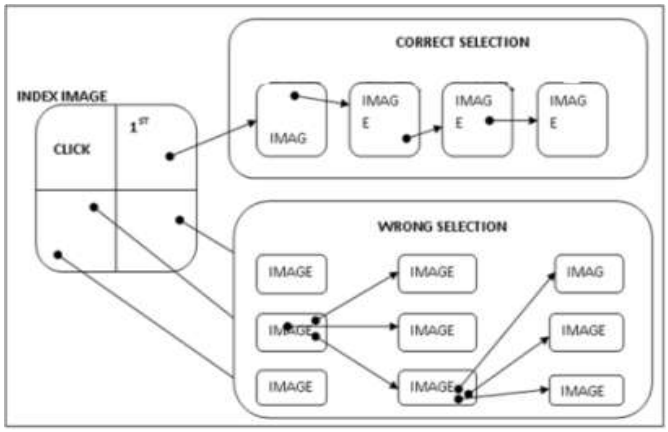

Fig. 2 The image sequence for correct as well as wrong passwords.

- Limitations of Existing System

In click based graphical password system, instead of selecting an image, we can select several click points as the password. It may be difficult to hack these click points and the order. However in an image there may be hot spots i.e. most attractive regions. There is chance for using these regions as the click points. The presence of hot spots may cause guessing of the click points. Click cued points is a click-based graphical password scheme. Various graphical password schemes have been proposed as alternatives to text-based passwords. It can be used as password for folder lock, web-driven applications, desktop lock etc. Various graphical password schemes have been proposed as alternatives to text-based passwords. Research shows that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Human psychology studies have shown that the human brain is better at recognizing and recalling images than text.

IV. PROPOSED SYSTEM

The proposed system is the integration sound signature into graphical password scheme. The Graphical password scheme is very secure and difficult to hack and it is quite easy to remember. In our new system, an extra feature is added to this technology, i.e. Sound Signature.

The user is given the privilege to select a sound file as well as tolerance level while he is creating the new login account. (Fig. 3) When then user logs in, if the click points are correct, the selected sound file will be played. Otherwise the sound file will not be played.

Fig. 3 The login page with sound signature and tolerance level selection

The user can also select sound signature files for each click point.(Fig 4) This helps the user in making sure that he is correctly entering the password click points. In this system, when users build a password, the images are slightly shaded except for a viewport. The viewport is positioned randomly on the image, rather than placing to a specific place to avoid hotspot regions, because such information might allow attackers to improve guesses and could lead to the formation of new hotspots. (Fig 5)The viewport's size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users are requested to select a click-point within this highlighted viewport and cannot click outside of the viewport. The viewport appear only during password creation. When the user enter the password later, the images are displayed without shaded region or the viewport, and users can click anywhere on the images. Like Pass Points and CCP, login click-points must be within the defined tolerance squares of the original points

Fig. 4 Loading image and getting click points along with sound signature.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

- Advantages of the Proposed System

Various graphical password schemes have been proposed as alternatives to textual passwords. Researches shows that textual passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text. Another advantage of the proposed system is the security provided by it. The proposed system will help in guessing attacks. The new system can block pattern based attacks and hotspot attacks. The new system will provide view ports to the user while selecting the password. This will help to avoid hotspot attack. The new system is a click point based password system. Therefore capturing passwords by shoulder surfing and malware like key loggers will not work.

V. IMPLEMENTATION ISSUES

The following sections depict several practical design and implementation issues in building the new system.

- Discretization

Discretization of click-points allows for approximately correct click-points to be accepted by the system without storing exact click-point coordinates exactly. Our system implemented Centered Discretization, dividing the image into square tolerance areas, to determine whether a login pass point falls within the same tolerance area.

- Deterministic Image Sequencing

The deterministic image sequencing approach allows a different sequence of images per each user while still guaranteeing a consistent mapping of click-points to images for each user. Using this implementation, there is a possibility that images are reused for a given user. A user clicking on an incorrect location during login might, by chance, see an image belonging within their password space. There is no evidence this occurred in any of our studies. The image selection algorithm could be modified to disallow all image reuse for a given user, providing enough verifiable information to determine the entire password to an attacker who learns only the last image.

- Viewport Details

The viewport visible during password creation must be large enough to extend some degree of user choice, but it must be small enough to have its intended effect of distributing click points across the image.(Fig 5) Physiologically, the human eye can observe only a small part of an image at a time.

VI. CONCLUSION

A common security goal in password-based authentication systems is to maximize the effective password space. This affects usability when user choice is included. It is possible to allow user choice while still increasing the effective password space. Furthermore, methods such as viewport (used during password creation) cannot be exploited during an attack.

Fig 5 Hotspot elimination by using viewport

Users could be further altered (at some cost in usability) from selecting obvious click points by limiting the number of shuffles allowed during password creation or by progressively slowing system response in repositioning the viewport. The approaches discussed in this paper present a middle ground between insecure but memorable user-chosen passwords and secure system generated random passwords that are difficult to remember.

REFERENCES

1. S. Chiasson, R. Biddle, and P. van Oorschot, “A Second Look at the Usability of Click-Based Graphical Passwords,” Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.
2. S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, “Influencing Users towards Better Passwords: Persuasive Cued Click- Points,” Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.
3. S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, “Multiple Password Interference in Text and Click-Based Graphical Passwords,” Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.
4. E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, “Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords,” Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.
5. S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, “User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords,” Int’l J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009.