IMPLEMENTATION OF EFFECTIVE GRAPHICAL PASSWORD AUTHENTICATION SYSTEM USING POI METHOD

Ms. Suganya. B[1], Mr. C. Stanley Gladson[2]
[1]M.E (CSE), A.S.L Pauls College of Engineering and Technology, Coimbatore, India.
[2]M.Tech (Network and Internet Engineering), Karunya University, Coimbatore, India.

***Abstract*: Graphical passwords provide a promising alternative to traditional alphanumeric passwords. Usable security has unique usability challenges because the need for security often means that standard human computer-interaction approaches cannot be directly applied. An important usability goal for authentication systems is to support users in selecting better passwords, thus increasing security by expanding the effective password space. They are attractive since people usually remember pictures better than words. In our project we are using Point of Interest method, here the user create a graphical password. Our approach here combines alphanumeric password with graphical passwords. Predictive performance evaluation is a fundamental issue in design, development and deployment of classification systems. As predictive performance evaluation is a multidimensional problem, single scalar summaries such as error rate, although quite convenient due to its simplicity, can seldom evaluate all the aspects that a complete and reliable evaluation must consider. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption.**

I. INTRODUCTION

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability. While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks. Contains username, graphical password, and related methods. In this module before must register the every user to use this method. After that Login the page get the Login information about the current user details.

Human factors are often considered the weakest link in a computer security system. Patrick, et al. point out that there are three major areas where human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords. On the other hand, passwords that are hard to guess or break are often hard to remember. Studies showed that since user can only remember a limited number of passwords, they tend to write them down or will use the same passwords for different accounts.

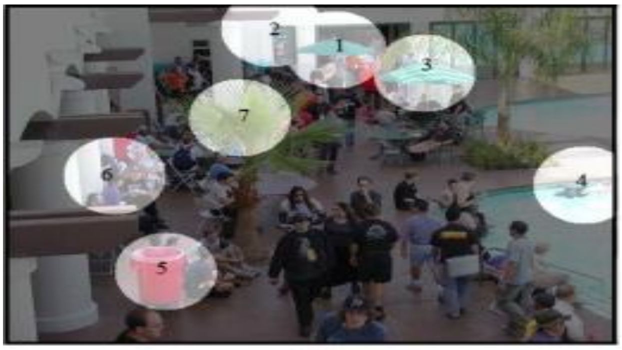
Contains graphical password information and related methods. Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words. Also, they should before resistant to brute force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

Pass faces are a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces an early recall-based graphical password approach was introduced by Greg Blonder in this approach; a user creates a password by clicking on several locations on an image. During authentication, the user must click on those locations. Pass Points builds on Blunders idea, and overcomes some of the limitations of his scheme several other approaches have been surveyed in the following paper.

Pass point graphical passwords have been shown to be susceptible to hot-spots, which can be exploited in human-seeded attacks , where by human-computed data (harvesting click-points from a small set of users) is used to facilitate efficient attacks. These attacks require that the attacker collect sufficient “human-computed” data for the target image, which is more costly for systems with multiple images. This leads us to ask whether more scalable attacks exist, and in particular, effective fully automated attacks. To address this question, in the present work, we introduce and evaluate a set of purely automated attacks against Pass-Points-style graphical passwords. Our attack method is based on the hypothesis that users are more likely to choose click-points relating to predictable preferences, e.g., logically grouping the click points through a click-order pattern (such as five points in a straight line), and/or choosing click-points in the areas of the image that their attention is naturally drawn towards

II. POINT OF INTEREST METHOD

Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. We have developed one such system, called Pass Points, and evaluated it with human users.



(a)

Fig.1. Login Page

The results of the evaluation were promising with respect to removability of the graphical password. In this study we expand our human factors testing by studying two issues: the effect of tolerance or margin of error, in clicking on the password points and the effect of the image used in the password system. In our tolerance study, results show that accurate memory for the password is strongly reduced when using a small tolerance (10 x 10 pixels) around the user’s password points. This may occur because users fail to encode the password points in memory in the precise manner that is necessary to remember the password over a lapse of time.

In our image study, we compared user performance on four everyday images. The results indicate that there were few significant differences in performance of the images. This preliminary result suggests that many images may support memo ability in graphical password systems.

Login Information: Contains username, graphical password, and related methods. In this module before must register the every user to use this method. After that Login the page get the Login information about the current user details.

Graphical Password: Contains graphical password information and related methods. Graphical passwords refer to using pictures (also drawings) as passwords. In theory,

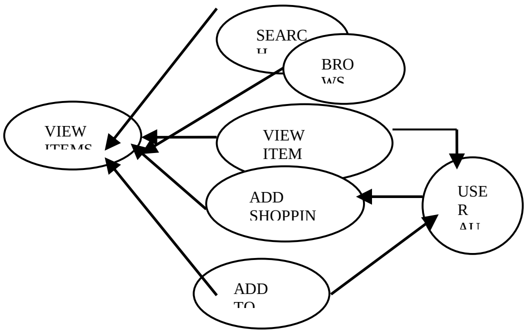


Fig.2. Use Case Diagram

graphical passwords are easier to remember, since humans remember pictures better than words. Also, they should before resistant to brute force attacks, since the search space is practically infinite. In general, graphical passwords techniques are classified into two main categories: recognition-based and recall based graphical techniques. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

Pass faces are a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces an early recall-based graphical password approach was introduced by Greg Blonder in this approach; a user creates a password by clicking on several locations on an image. During authentication, the user must click on those locations. Pass Points builds on Blunders idea, and overcomes some of the limitations of his scheme several other approaches have been surveyed in the following paper.

Selected Regions: Contains fields about selected regions (POIs). In the proposed system, a user freely chooses a picture, POIs and corresponding words. The order and number of POIs can be enforced for stronger authentication. Together, these parameters allow for a very large password space. We believe that proposed approach is promising and unique for at least two reasons:

1) It combines graphical and text-based passwords trying to achieve the best of both worlds.
2) It provides multi-factor authentication (graphical, text, POI-order, POI-number) in a friendly intuitive system.

Communication Alternatives: In the public terminal, the user receives and the screen displays a random password image with multiple clickable areas on terminal screen. At the same time, the key image with information about click points appear on the screen of user’s handheld which is linked to the identity of the user. Therefore the user learns about the click points and their order if and only if she has access to her handheld. There are several ways to transfer the encrypted password image to the users handheld which are explained in the followings:

1) Direct Communication

The challenger sends a password image to the terminal. At the same time, the challenger prepares the key image, encrypts it, digitally signs the encrypted image and emails it to the users handheld. The users handheld verify the signature and decrypt the image. For every authentication, the key image changes but the password image may or may not change.

2) Photographic Communication

The challenger prepares a key image, encrypts it and sends it to the user’s terminal. Using the handheld’s camera, the user takes a photo of the encrypted key image which the handheld can decrypt it. At this point the user is able to click on the appropriate spots on the password image. The image on the screen remains unencrypted and doesn’t match what the user sees on the handheld. However what is important here is the click points and not the actual image.

3) Indirect Communication

Similar to method the challenger prepares a key image, encrypts it and sends it to the user’s terminal the user’s handheld and terminal are able to communicate via Bluetooth or USB and transfer a copy of the password image to the handheld and decrypt it. At this point, the user is able to click on the appropriate spots on the password image. The image on the screen remains unencrypted and doesn't match what the user sees on the handheld. Again, what is important here is the click points and not the actual image.

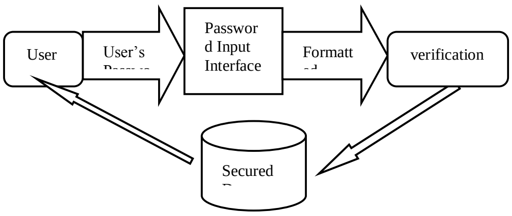


Fig.3. Architecture Diagram

III. PROBLEM DEFINITION

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Pass face technique have shown that people often choose weak and predictable graphical passwords. More research efforts are needed to understand the nature of graphical passwords created by real world users.

Comparing to text based password, it is less convenient for a user to give away graphical Passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

IV. CONCLUSION

User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. It also provides multi-factor authentication in a friendly intuitive system. We described the system operation with some examples, and highlighted important aspects of the system.

REFERENCES

[1] Paul C. van Oorschot, Amirali Salehi-Abari, and Julie Thorpe "Purely Automated Attacks on PassPoints-Style Graphical Passwords"

[2] William Stallings and Lawrie Brown. Computer Security: Principle and Practices. Pearson Education 978-0-9564263-7/6/$25.00©2011 IEEE 224.

[3] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Pass points: design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63:102–127.

[4] Robert Morris and Ken Thompson. Password security: a case history. Communications of the ACM, 22:594-597.

[5] Daniel V. Klein. Foiling the Cracker: A Survey of and Improvements to, Password Security. In Proceedings of the 2nd USENIX UNIX Security Workshop, 1990.

[6] G. Blonder, "Graphical Passwords," U.S. Patent 5559961.

[7] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in Proc. HCI, British Computer Society, Liverpool, U.K.

[8] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," Int. J. Inf. Security, vol. 8, no. 6, pp. 387–398.

[9] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords," in 16th ACM Conf. Computer and Communications Security (CCS), Chicago, IL.

[10] I. Cohen and M. Goldszmidt, "Properties and benefits of calibrated classifiers," in 8th European Conference on Principles and Practice of Knowledge Discovery in Databases, 2004, pp. 125–136.

BIOGRAPHY

Ms. Suganya. B, born in Coimbatore on 07-Nov-1990. Completed B. Tech (Information Technology) in Angel College of Engineering & Technology, Afflicted to Anna University, Chennai India. Doing M.E in Computer Science and Engineering (2012-2014) in Anna University Afflicted College, Coimbatore, Tamil Nadu, India. Have Presented 4 National Conferences and

2 International Conferences and Published 3 International Journal. Area of Specialization includes Network Security, Data Structures, and Software Testing.

Mr. C. Stanley Gladson, born in Coimbatore on 27-Aug-1990. Completed B.E (Electronics and Communication Engineering) in Angel College of Engineering & Technology, Afflicted to Anna University Chennai India. Doing M.TECH (Network & Internet Engineering) in Karunya University, Coimbatore, TamilNadu, India. Have presented 3 papers in International Conference. Area of Specialization includes Networking.