ISSN:2348-2079

Volume-5 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Enrichment of security using feature Set and order sequence graphical authentication

1. G.Guna Arasu, PG Scholar
2. K.Gopalakrishnan, Assistant Professor,CSE
Nandha College of Technology, Erode
gunaarasu@gmail.com, gopalakrishnanbtech@gmail.com

Abstract *- **User authentication is one of the most important procedures required to access secure and confidential data. Authentication of users is usually achieved through text-based passwords. Attackers through social engineering techniques easily obtain the text based password of a user. Apart from being vulnerable to social engineering attacks, text based passwords are either weak-and-memorable or secure-but-difficult-to-remember. Researchers of modern days have thus gone for alternative methods wherein graphical pictures are used as passwords. Image based authentication allows user to create graphical password which has advantages over text-based passwords. Graphical passwords have been designed to make passwords more memorable and easier for people to use. In this project, an Image Based Authentication system with order evaluation approach that allows users choice password and simultaneously influences users to select stronger passwords is proposed. To add a layer of security, user is asked to input own digital picture and select sequence tokens from the picture used during registration phase. The user has to reproduce the same tokens by input the same image during his login phase. Also to enhance the security, verification is done by two phases 1) Token verification and 2) Token order evaluation in the server system. This proposed system offers reasonable security and usability and appears to fit well with some practical applications for improving online security.***

I INTRODUCTION

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. People select predictable passwords. This occurs with both texts based and graphical passwords. Users tend to choose passwords that are memorable in some way, which unfortunately often means that the passwords tend to follow predictable patterns that are easier for attackers to exploit. 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.

An authentication system should encourage strong passwords while still maintaining memorability. proposed that users be persuaded to select more secure passwords.

This proposed system allows user choice while attempting to influence users to select stronger passwords. It also makes the task of selecting a weak password (easy for attackers to predict) more tedious, in order to discourage users from making such choices. In effect, this scheme 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 and create a more secure password; a feature that is lacking in other schemes. Approached to an image-feature based password system and conducted an in-lab usability study with some user participants is applied. This results show that this PassBYOP—Bring Your Own Picture scheme is effective at reducing the number of hotspots (areas of the image where users are more likely to select click points) while still maintaining usability. While not argued that graphical passwords are the best approach to authentication, find that offer an excellent environment for exploring strategies for helping users select better passwords since it is easy to compare user choices. Indeed mentioned how this approach might be adapted to text-based passwords/some graphical passwords.

II EXISTING SYSTEM

Text passwords and personal identification numbers (PINs) are the dominant authentication method are simple and can be deployed on systems including public terminals, the web, and mobile devices. Here focus on the authentication problem. The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. Graphical password systems are knowledge-based authentication techniques that leverage peoples' ability to memorize and recognize visual information more readily than alphanumeric information. Some types of graphical password are,

2.1 Locimetric Password Schemes

Cued-recall - involve users selecting regions on one or more images. During login, users are shown a previously selected image, and enter a password by clicking on a sequence of locations on the image. Authentication is successful if the XY coordinates of these clicks match a previously stored set of password points. While simple and effective, cued-recall graphical passwords present new security issues.

Cued-Click Points (CCP) - Addressing this issue, the cued-click points system presented a series of images and allowed users to select only a single point per image, reducing the need to select common hotspots.

2.1.1 Drawbacks

For instance, users typically select hotspots, locations on an image that are highly distinguishable memorable, and also predictable to attackers.

Although more secure, this technique was prohibitively slow and error prone.

A second key problem with locimetric systems is observation, as password click-points can be acquired by attackers after viewing a single authentication process.

Securing against observation attack for graphical password systems is critical.

2.2 Multifactor Authentication Schemes

Multifactor authentication, based on the combination of two or more independent processes, can boost security. In ntypical multifactor authentication schemes, physical tokens are used to generate and store secrets for user authentication. For example, One-time password generation User snapping a picture of a QR code

2.2.1Drawback

While these tools offer increased security, are susceptible to particular kinds of attack, such as Man-in-the-Middle schemes that snoop on, or alter, messages transmitted between a user and the system.

III PROPOSED STSTEM

Various password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. To address this issue, present a new point-click graphical password system, PassBYOP—Bring Your Own Picture that increases resistance to observation attack by coupling the user's password to an image.

3.2.1 PASSBYOP Scheme

PassBYOP seeks to make graphical passwords more secure against intelligent guessing and shoulder-surfing attacks. PassBYOP tackles this problem by introducing a physical token into the authentication process. PassBYOP is a multifactor authentication system—both a physical token and a password are needed to authenticate. This way, PassBYOP transforms a graphical password, which is traditionally a single factor authentication mechanism, to a more secure multifactor authentication method. Assuming users have previously created a password, login involves users identifying themselves at aPassBYOP terminal in a manner fitting the system and use context. argue this raises the resistance of PassBYOP to attacks based on password observation and guessing as attackers need to possess a user's genuine token or a high fidelity copy.

Present an implementation for the scheme based on SIFT image features. PassBYOP selections are stored on the authentication server as a set of optical features computed with the SIFT image processing algorithm. After login attempt the matching process involved which minimizing the Euclidean distance between the sets of feature points in the original and entered password items. Subsequently, a threshold on the percentage of matching features was used to determine whether the entered password matched the original.

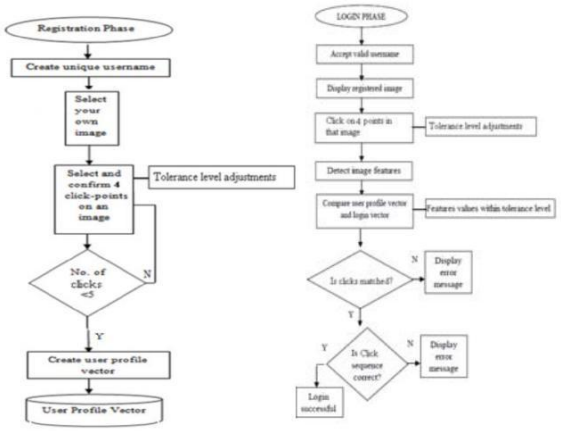
3.2.2 Advantages

PassBYOP substantially increases resistance to shoulder-surfing attacks compared with existing graphical password schemes**.**

- PassBYOP conserves the beneficial properties of graphical passwords while increasing their security.
- The proposed scheme shows promise as a usable and memorable authentication mechanism.
- PassBYOP approach is flexible and user friendly.
- Avoided guessing attacks and several possible attacks

- Provide high level user security with minimal cost
- Supports more number of user authentication applications

IV. SYSTEM ARCHITECTURE



4.1 USER INTERFACE DESIGN

User interface design or user interface engineering is the design of computers, appliances, machines, mobile communication devices, software applications, and websites with the focus on the user's experience and interaction. The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals—what is often called user-centered design. To run this project develops a GUI application in C#.net.

4.2 NEW USER REGISTRATION

User registration module describes the new user account creation. Initially user need to create personal details, username, password and retype password and then user answer the questions displayed which are used to retrieve forget text password and finally completing these steps user account created successfully in the server database. Then server is in waiting status to receive the registration or verification request from clients.

4.3 USER TEXT BASED AUTHENTICATION

Each registered client must clear the text based authentication by providing username and password in client side page. For verification user must fill the username and password, it should be validated with the usernames and passwords stored in the server database if verification success next authentication will be shown else verification failed not proceed further. After successful authentication user needs to complete the further image registration by setting up own picture with object based features clicks which are store in the server database and user it for next verification.

4.4 USER OWN PICTURE PASS BY OP REGISTRATION

Once client clear the text based authentication, need to complete registration process for account creation by setup own picture and feature based clicks for passbyop authentication. A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). Like that in passbyop scheme passwords consist of a sequence of user four click points on an input own picture. Users may select any pixels in the image as click-points for their password. Then the picture and features values are stored in the server database thus user account will be created successfully.

4.5 USER AUTHENTICATION BY TEXT/ PASS BY OP REQUEST/RESPONSE

Once users complete the registration process, need to clear the verification process for to access their account. For verification/authentication user input and send the username and password for text based verification to the server once server clears the text based authentication then send the user picture (given own picture by user during registration) to the user then user select the four clicks and send back the values to the server for matching result.

VI CONCLUSION

In summary, this project proposed for improving the security of graphical password systems by integrating live video of a physical token that a user carries with them. It first demonstrates the feasibility of the concept by building and testing a fully functional prototype. It then illustrates that user performance is equivalent to that attained in standard graphical password systems through a usability study assessing task time, error rate, and subjective workload. Finally, a security study shows that PassBYOP substantially increases resistance to shoulder-surfing attacks compared with existing graphical password schemes. Ultimately this project demonstrates that PassBYOP conserves the beneficial properties of graphical passwords while increasing their security. While this approach was simple and effective, greater
speed and efficiency would be attained with a native application.

By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, PassBYOP has advantages over other systems in terms of usability. But in proposed system user verification process is not achieves high level security so focused on verification process and propose Feature points with order evaluation approach i.e not only verify feature points but also verify the order of feature points. During registration the feature points are stored in the server with its order sequence and match the feature points and its sequence thus achieve high level security and also provide better usability.

REFERENCES

[1]. Adams. A. and Sasse. M., "Users are not the enemy," Commun. ACM, vol. 42, pp.40–46, 1999.

[2]. Adham. M., Azodi.A., Desmedt.Y., and Karaolis.I., "How to attack twofactor authentication internet banking," in Proc. 17th Int. Conf. Financial Cryptography, 2013, pp. 322–328.

[3]. Aloul.F., Zahidi.S., and El-Hajj.W., "Two factor authentication using mobile phones," Proc. Comput. Syst. Appl., 2009, pp. 641–644.

[4]. Biddle. R., Chiasson.S., and van Oorschot.P., "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys vol. 44, no. 4, p. 19, 2012.

[5]. Blonder. G. E., "Graphical passwords," U.S. Patent 5 559 961, 1996.

[6]. Bonneau. J., Herley. C., van Oorschot. P. C., and Stajano. F., "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE Symp. Security Privacy, 2012, pp. 553– 567.

[7]. Chiasson. S., Biddle. R., and van Oorschot. P., "Asecond look at the usability of click-based graphical passwords," in Proc. 3rd Symp. Usable Privacy Security, 2007, pp. 1–12.

[8]. Chiasson.S., van Oorschot. P.C., and Biddle.R., "Graphical password authentication using cued click points," in Proc. 12th Eur. Symp. Res. Comput. Security, 2007, pp. 359–374.

[9]. Chiasson.S., Forget.A., Biddle.R., and Oorschot.P.C., "User interface design affects security: Patterns in click-based graphical passwords, Int. J. Inf. Security, vol. 8, no. 6, pp. 387–398, 2009.

[10]. Chiasson.S., Stobert.E., Forget.A., Biddle.R., and Van Oorschot. P.C., "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," IEEE Trans. Dependable Secure Comput., vol. 9, no. 2, pp. 222–235, Mar./Apr. 2012.

[11]. De Luca. A., von Zezschwitz.E., Nguyen.N.D.H., Maurer.M., Rubegni.E., Scipioni.M.P., and Langheinrich.M., "Back-of-device authentication on smartphones," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2013, pp. 2389– 2398.

[12]. Dodson.B., Sengupta.D., Boneh.D., and Lam.M.S., "Secure, consumerfriendly web authentication and payments with a phone," in Proc. 2nd Int. ICST Conf. Mobile Comput., Appl., Serv., 2010, pp. 17–38.

[13]. Everitt.K.M., Bragin.T., Fogarty.J., and Kohno.T., "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2009, pp. 889–898.

[14]. Gelman.A., Hill.J., and Yajima.M., "Why (usually) don't have to worry about multiple comparisons," J. Res. Educ. Effectiveness, vol. 5, no. 2, pp. 189–211, 2012.