ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Three Step Password Scheme for Secured Data Transfer

M.S.Vinu[1], R.T.Nivetha[2], M. Mano Chitra[3], K.Priyadharsini[4]

Asst. Prof, Department of CSE, Sri Eshwar College of Engineering, Tamil Nadu, India[1]

PG, Department of CSE, Sri Eshwar College of Engineering, Tamil Nadu, India[2, 3, 4]

ABSTRACT –This paper presents the implementation of persuasive cued click points, graphical password schemes including security and authentication mechanisms using traditional password scheme along with secret key generation and biometrics. And to enhance the effective security space to support users in selecting passwords of higher security, the objective is to provide security mechanisms for the users and which makes the attackers difficult to guess the passwords. Also, rather than increasing the burden on users it is easier to follow the system suggestions for secure password features which is lagging in most of the schemes.

I. INTRODUCTION

The problems of knowledge-based authentication, typically text-based passwords, are well known. Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember [6]. A password authentication system should encourage strong passwords. We propose that authentication schemes allow user choice while influencing users toward stronger passwords. In the 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. We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP) [1], [2], and conducted user studies evaluating usability and security. The 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. In our system we use two step authentication mechanisms for secured data transfer. The two steps are textual password and graphical password. Graphical passwords are based on the idea that users can recall and recognize pictures better than words; however some of these graphical password schemes require a long time to be performed. We present and evaluate our contribution towards two step password authentication for secured data transfer. In the two steps process user navigates and interacts with various objects. The sequence of actions and interactions towards the objects construct the user's two passwords and then we go for secured data transfer for window application.

II. BACKGROUND

Text passwords are the most popular user authentication method, but have security and usability problems. Alternatives such as biometric systems and tokens have their own drawbacks [8], [9], [10].

2.1 Click-Based Graphical Passwords

Graphical password systems are a type of knowledge-based authentication that attempts to leverage the human memory for visual information [11]. A comprehensive review of graphical passwords is available elsewhere [12]. Of interest herein are cued-recall click-based graphical passwords (also known as locimetric [13]). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues [14] to aid recall. Example systems include PassPoints [15] and Cued Click- Points (CCP) [7].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

In PassPoints, passwords consist of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. Although PassPoints is relatively usable [1], [15], [16], security weaknesses make passwords easier for attackers to predict.

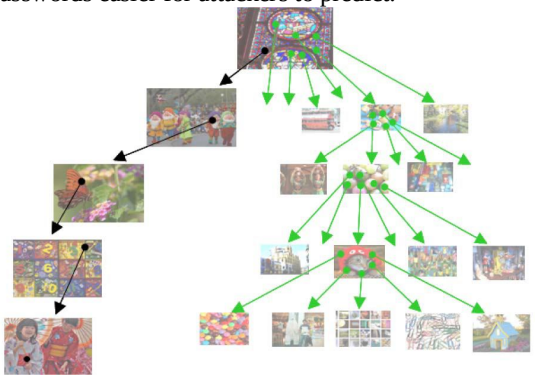

Fig. 1. A user navigates through images to form a CCP password. Each click determines the next image.

Hotspots [17], [18], [19], [20] 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 passwords [18], [19]. Users also tend to select their click-points in predictable patterns [5], [20] (e.g., straight lines), 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 [21].

A precursor to PCCP, Cued Click Points [7] was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click-points on one image, CCP uses one click-point on five different images shown in sequence. The next image displayed is based on the location of the previously entered click-point (Fig. 1), creating a path through an image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click-points results in a different image sequence.

The claimed advantages are that password entry becomes a true cued-recall scenario, wherein each image triggers the memory of a corresponding click-point. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks. User testing and analysis showed no evidence of patterns in CCP [5], so pattern-based attacks seem ineffective. Although attackers must perform proportionally more work to exploit hotspots, results showed that hotspots remained a problem [1].

2.2 Persuasive Technology

Persuasive Technology was first articulated by Fogg [22] as using technology to motivate and influence people to behave in a desired manner. 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. As detailed below, PCCP accomplishes this by making the task of selecting a weak password more tedious and time consuming. The path of least resistance for users is to select a stronger password (not comprised entirely of known hotspots or following a predictable pattern). The formation of hotspots across users is minimized since click-points are more randomly distributed. PCCP's design follows Fogg's Principle of Reduction by making the desired task of choosing a strong

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

password easiest and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

2.3 Persuasive Cued Click Points

Visual attention research [23] shows that different people are attracted to the same predictable areas on an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will remain an issue. We investigated whether the system could influence users to select more random click-points while maintaining usability [1], [2], [3], [4]. The goal was to encourage more secure behavior by making less secure choices (i.e., choosing poor or weak passwords) more time consuming and awkward. In effect, behaving securely became the safe path of least resistance [1]. By adding a persuasive feature to CCP [7], PCCP [1] encourages users to select less predictable passwords, and makes it more difficult to select passwords where all five click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a viewport (see Fig. 2). The viewport is positioned randomly, rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots. 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 must select a click-point within this highlighted viewport and cannot click outside of the viewport, unless they press the shuffle button to randomly reposition the viewport. While users may shuffle as often as desired, this significantly slows password creation. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images. Like PassPoints and CCP, login click-points must be within the defined tolerance squares of the original points. The theoretical password space for a password system is the total number of unique passwords that could be generated according to the system specifications. Ideally, a larger theoretical password space lowers the likelihood that any particular guess is correct for a given password.

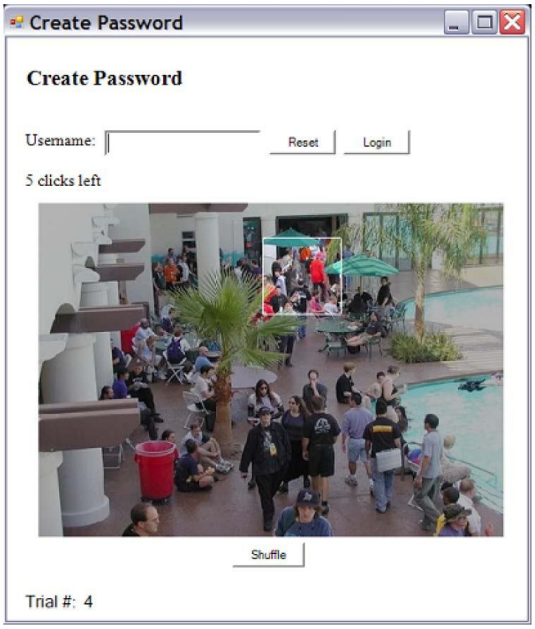

Fig. 2. PCCP Create Password interface. The viewport highlights part of the image.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

III. PROPOSED AUTHENTICATION SCHEME FOR SECURED DATA TRANSFER

In our system we use three step authentications; one is textual password, second is graphical password and third is biometric. Only if the sender and receiver pass through these three steps they can transfer their confidential data in a secured way. For both sender and receiver registration is done.

In the first step (i.e.) the textual password they are asked to enter user name and password, then their finger print sample is saved and a generate button that is present there will generate a secret key based on random key generation algorithm. The secret key will be generated for both sender and receiver separately. Once the registration is over we will encrypt the password and secret key in the database using secured SHA-1 algorithm. In the login process, the sender and receiver should enter their user name, password and secret key which is generated in the registration process. Then decryption is done for the password and secret key and if it matches the user can successfully login.

In the second step (i.e.) the graphical password once the login by both sender and receiver is done in parallel, based on the sender's and receiver's information a session key will be generated by the key generator. The session key will be randomly generated for each login process. Based on session key, sender's secret key and receiver's secret key, a graphical key will be generated by the key generator. The graphical key will be sent to both sender and receiver ad it's an eight digit key. In the graphical password step, images will be in the screen where only one image is dynamic. We have to double click on the dynamic image to move it to a particular position so that the image will be hidden. There is no control like button to move to next step. Using the graphical key X and Y coordinates are formed. The user should double click on that coordinate so that a runtime control (text box) will be generated. There both the sender and receiver should enter the graphical key. If wrong clicks are made the processing will be immediately stopped.

In the third step (i.e.) the finger print of the user is used. If the sample matches with the stored or registered sample then the user can send and receive data.

We have also proposed the secured data transfer using Triple DES algorithm where the sender will encrypt data using that algorithm and will send to receiver. The receiver in turn will decrypt the data which is shown in Fig. 3

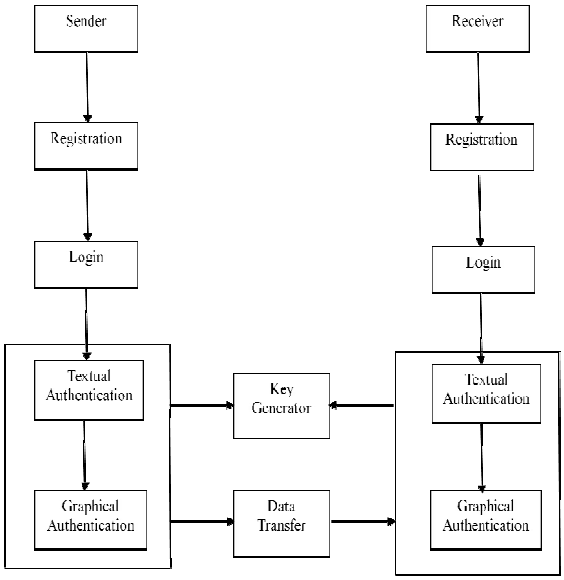

Fig. 3 Authentication Scheme for Secured Data Transfer

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. CONCLUDING REMARKS

A Common Security goal of authentication in systems is to maximize the effective password space is achieved. It is difficult to implement automated attacks against graphical passwords. This system provides secrets that are easy to remember and very difficult for intruders to guess which provides a safe and secure transaction. Better user interface design can influence users to select stronger passwords in our system. Our approach is efficient at reducing the formation of hotspots and pattern thus increasing the effective password space.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.
[6] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.
[7] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.
[8] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.
[9] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.
[10] D. Nelson, V. Reed, and J. Walling, "Pictorial Superiority Effect," J. Experimental Psychology: Human Learning and Memory, vol. 2, no. 5, pp. 523-528, 1976.
[11] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," to be published in ACM Computing Surveys, vol. 44, no. 4, 2012.
[12] 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," Int'l J. Human- Computer Studies, vol. 63, nos. 1/2, pp. 128-152, 2005.
[13] E. Tulving and Z. Pearlstone, "Availability versus Accessibility of Information in Memory for Words," J. Verbal Learning and Verbal Behavior, vol. 5, pp. 381-391, 1966.
[14] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.
[15] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005.
[16] K. Golofit, "Click Passwords under Investigation," Proc. 12th European Symp. Research in Computer Security (ESORICS), Sept. 2007.
[17] A. Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme," Proc. Third ACM Symp. Usable Privacy and Security (SOUPS), July 2007.
[18] J. Thorpe and P.C. van Oorschot, "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords," Proc. 16th USENIX Security Symp., Aug. 2007.
[19] A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "On Purely Automated Attacks and Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2008.
[20] P.C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely Automated Attacks on PassPoints-Style Graphical Passwords," IEEE Trans. Information Forensics and Security, vol. 5, no. 3, pp. 393- 405, Sept. 2010.
[21] B. Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, 2003.
[22] J. Wolf, "Visual Attention," Seeing, K. De Valois, ed., pp. 335-386, Academic Press, 2000.
[23] D. Davis, F. Monrose, and M. Reiter, "On User Choice in Graphical Password Schemes," Proc. 13th USENIX Security Symp., 2004.
[24] PD Photo, PD Photo Website, http://pdphoto.org, Feb. 2007.