ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Secure Graphical Passwords Using Live Physical Tokens

Renuka Prasad S B

Assistant Professor, Dept. of CSE, Shri Pillappa College of Engg, Bengaluru, Karnataka, India

ABSTRACT: SGPULPT is a new graphical password scheme forpublic terminals that replaces the static digital images typically used in graphical password systems with personalized physical to-kens, here in the form of digital pictures displayed on a physical user-owned device such as a mobile phone. Users present these images to a system camera and then enter their password as a sequence of selections on live video of the token. Highly distinctive optical features are extracted from these selections and used as the password. We present three feasibility studies of SGPULPT exam-ining its reliability, usability, and security against observation. The reliability study shows that image-feature based passwords are vi-able and suggests appropriate system thresholds—password items should contain a minimum of seven features, 40% of which must geometrically match originals stored on an authentication server in order to be judged equivalent. The usability study measures task completion times and error rates, revealing these to be 7.5 s and 9%, broadly comparable with prior graphical password systems that use static digital images. Finally, the security study highlights SGPUL

PT's resistance to observation attack—three attackers are unable to compromise a password using shoulder surfing, camera-based observation, or malware. These results indicate that SGPULPT shows promise for security while maintaining the usability of current graphical password schemes.

KEYWORDS: Graphical password, input, live video, observation, user study.

I. INTRODUCTION

Secure access to information underpins modern digital systems and services. We keep our communications, financial data, work documents, and personal media safe by providing identity information and then authenticating to that identity. Text passwords and personal identification numbers (PINs) are the dominant authentication method [7] as they are simple and can be deployed on systems including public terminals, the web, and mobile devices. However, passwords suffer from limitations in terms of memorability and security—passwords that are difficult to guess are also hard to remember [19]. This is a major problem as an average user possesses 25 online accounts secured with up to six different passwords [17] and representing a substantial memory burden. To deal with this problem, individuals adopt non secure coping strategies such as reuse of passwords across systems, noting down passwords, or simply forgetting them entirely [1]. In order to mitigate these problems, researchers have proposed graphical password schemes [5], [6] that rely on input such as selecting portions of an image. These systems have been shown to improve memorability without sacrificing input time or error rates [24] while also maintaining a high resistance to brute force and guessing attacks [5].

However, graphical passwords present their own problems. One issue is their susceptibility to intelligent guessing [7], [8] and shoulder-surfing attacks. Such attacks are effective because the sections of images that users select as password items are both easy for an attacker to observe by snooping over shoulders or setting up a camera to record input and also relatively predictable—users tend to choose hotspots such as the eyes in a facial portrait [11], [12]. This issue is particularly problematic as the image contents for graphical password systems are typically stored on authentication servers [5] and readily presented to attackers in response to input of easily accessible user identity information.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

To address this issue, we present a new point-click graphical password system, SGPULPT—Bring Live Physical Tokens that increases resistance to observation attack by coupling the user's password to an image or object physically possessed. This is achieved by using live video of a physical token, such as an object, a photograph, or even an image of a body part (e.g., a palm), as the canvas for entering a graphical password. This physical object replaces easily accessible server-based images [7], and we argue that attackers will struggle to capture useful replicas of this content. We present an implementation for the scheme based on SIFT image features [20] and a demonstration of its viability through three feasibility studies covering: 1) the reliability and robustness of SGPULPT feature based input; 2) participant task performance times and error rates using SGPULPT; and 3) the security of SGPULPT against observation attack.

II. RELATED WORK

Graphical password systems are knowledge-based authentication techniques that leverage peoples' ability to memorize and recognize visual information more readily than alphanumeric information [22]. Researchers have explored three broad types of graphical passwords: recall-based draw-metric schemes based on sketching shapes on screen, recognition-based cognometric schemes based on selecting known items from large sets of options, and cued-recall loci-metric schemes based on selecting regions of pre-chosen images [5], [14]. Loci-metric schemes are discussed as is multifactor authentication, as it relates to Pass-BYOP and its combination of a token, or something you have, on which a password, or something you know, is entered.

A. Loci-metric Password Schemes

Cued-recall (loci-metric) password schemes involve users selecting regions on one or more images. Blonder's [6] U.S. patent is the earliest example. A seminal example is Pass Points. During login, users are shown a previously selected image, and they 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. A longitudinal study resulted in login times of 8.78–24.25 s and a failed authentication rate of 7–13% .

While simple and effective, cued recall graphical passwords present new security issues. For instance, users typically select hotspots [23], locations on an image that are highly distinguishable, memorable, and also predictable to attackers. In the Microsoft Windows 8 graphical password system, the most common password involved a photo of a person and triple tap-ping on the face, where one of the selection points was an eye. Addressing this issue, the cued-click points (CCP) [9] sys-tem presented a series of images and allowed users to select only a single point per image, reducing the need to select common hotspots. Evaluations of this technique led to authentication times in the range of 7–8 s and success rates of 90–96%.

The second key problem with loci-metric systems is observation, as password click-points can be acquired by attackers after viewing a single authentication process [5]. Securing against observation attack for graphical password systems is critical. Chiassonet al. [11] remark: "User interface manipulations such as reducing the text size of the mouse cursor or dimming the image may offer some protection, but have not been tested." One exception is a variant of CCP that uses eye-tracking technology [16] for input. This system increased resistance to observation but negatively impacted performance: login times rose to 47.1– 64.3 s and only 67% of participants successful authenticated on their first attempt. Although more secure, this technique was prohibitively slow and error prone.

B. Multifactor Authentication Schemes

Multifactor authentication [20], based on the combination of two or more independent processes, can boost security. In typical multifactor authentication schemes, physical tokens are used to generate and store secrets for user authentication. For example, Aloulet al. [4] used mobile phones as the hardware token for one-time password generation. Dodson et al. [13] proposed a challenge-response authentication system involving a user snapping a picture of a QR code with a mobile de-vice. The data from this marker generated encrypted data that were used during login.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

While these tools offer increased security, they 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 [2].

SGPULPT is a multifactor authentication system—both a physical token and a password are needed to authenticate. SGPULPT differs from prior approaches in three ways. First, it is more flexible—instead of posing restrictions on the form of to-kens, any sufficiently complex image or object can be used as a SGPULPT token. Second, the two authentication factors are tightly coupled—the password factor is entered on the token factor. We suggest this close relationship will make the scheme easy to understand. Finally, the image tokens in SGPULPT are high-entropy, sufficiently so that they have been previously proposed as a single factor authentication scheme [20]. We also suggest that these physical data-rich tokens will be resistant to Man-in-the-Middle schemes as attackers will face substantial barriers in terms of capturing tokens in sufficient detail to support successful hacks.

III. SGPULPT IMPLEMENTATION

The SGPULPT prototype consists of a 13.5-cm-wide × 22.5-cm-long × 12-cm-high plastic box with a transparent cover and containing an upward-facing Logitech Quick-Cam E3500 webcam with a resolution of 640×480 pixels and a speed of 30 frames/s.

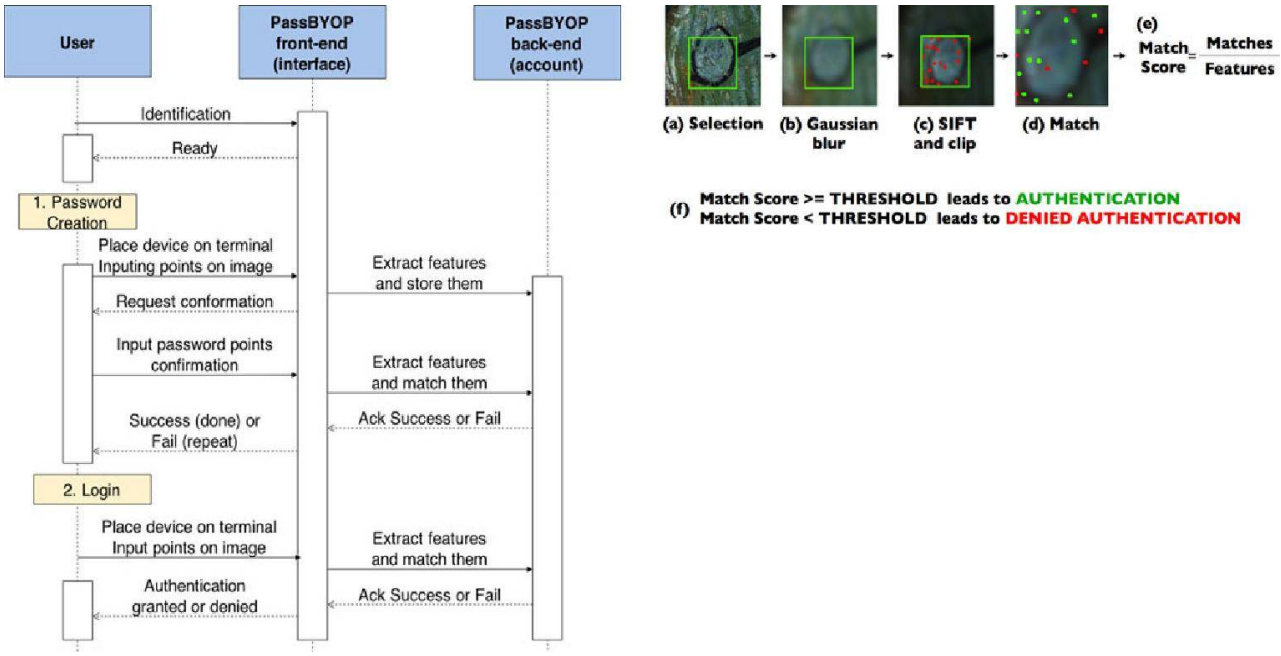

Fig.1. Sequence diagram showing the steps involved in creating a SGPULPT password

The webcam is connected to a PC running SGPULPT. The SGPULPT interface and video feed are shown on an Apple iPad that is connected wirelessly to the PC via a screen-sharing application and fixed to the surface of a desk. The video resolution on the iPad is 450×600 pixels or approximately 8.5 cm × 14 cm. All input to the system is made on the iPad touchscreen. Specifically users make selections by tapping the screen to visually highlight 70 × 70 pixel (approximately 1.5 cm^2) portions of the displayed image, drag to move this region and release to select it. Once an image portion is selected, it is stored as a password item and displayed as feedback to the user at the base of the screen. Users must input a total of four items and then press an OK button in order to enter a complete password. They can also press a reset button to clear the entered password items at any time.

In existing graphical password systems, the passwords are represented as the XY image coordinates of finger

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

selections. This technique does not work with SGPULPT as variations in image placement on the terminal camera will lead to substantial variations in the XY pixel positions of image content. Instead SGPULPT selections are stored on the authentication server as a set of optical features computed with the SIFT image processing algorithm [20]. This was achieved by capturing a 140 × 140 image subsection around the center point of each password item. A Gaussian blur was then applied and Lowe's [20] SIFT algorithm was computed with the peak threshold set to 2 and the edge threshold set to 10. This yields a list of image features and descriptors. Those that fell outside the central 70 × 70 selection box were discarded and the remainder used for password matching.

The matching process involved minimizing the Euclidean distance between the sets of feature points in the original and entered password items. Subsequently, a thresh-old on the percentage of matching features was used to determine whether the entered password matched the original. Lower threshold levels result in a lenient password system, whereas higher levels are stricter. This process hinges on the fact that SIFT features are highly distinctive, robust to noise, accurate, and rotation invariant—capable of matching the features extracted from a single image against a database containing 100000 images with an overall accuracy of 80% [20]

IV. EXPERIMENTAL RESULTS

A. Reliability Study

This study assessed the reliability of SGPULPTin order to determine suitable thresholds for the equality of two password items in terms of the minimum number of image features they should possess and the percentage of image features that should match. As variations in token placement are inevitable with SGPULPT's camera-based setup, we also explored the robustness of the system with rotated input images. Finally, we assessed the uniqueness of feature-based password items.

1) **Materials:**Five source images were selected based onthe image categories with highest success rate in prior work [8]. They depicted cars, a mural, toys, a statue, and a human face. These images were displayed on a Samsung Galaxy S-IImobile phone with a screen resolution of 480 × 800 pixels and each image was preprocessed to match this screen resolution.

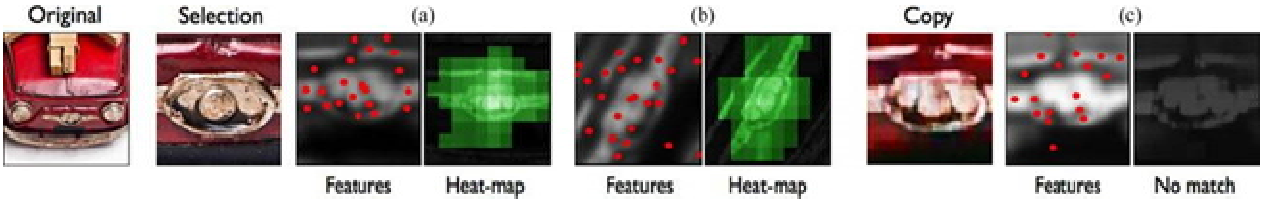

Fig. 2. Feature heat map generated by testing the match between a selected area its transformations (rotation or translation) with the same image or a downgraded copy. Light colored zones in the heat map indicate a match (white is 100% match). (a) Translated (b) Rotated (c) Translated.

We placed a 110-pixel square NyARToolkit fiducial marker in the center of each image to enable accurate detection of its angle relative to the SGPULPT camera.

Four selection points were also marked on the image with a 110-pixel circle. The selection points were chosen in a pilot study where eight users (two females, aged between 20 and 25 years) choose four pass-words items on the selected images and entered them into the SGPULPT system five times. We chose prominent distinctive points from among the selections in these sessions—either those that were frequently chosen or, if there was substantial variation in the points selected by users, one of the items at random. An example of one of final images used in the study. The experimental task involved users selecting these marked points in order. The use of predetermined and clearly marked selection points ensured the results were not influenced by issues such as memorability.

2) **Participants:**We recruited 15 volunteers (four females,two left-handed) from Sungkyunkwan University. They were a mix of students and staff, aged between 20 and 29 years (Mean: 24, SD: 2.83). None were security

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

experts or knowledgeable in the area of security research.

3) **Procedure:**For each of the five preselected images, eachuser completed a block of 11 input trials composed of selecting the four marked points in ascending numerical order. Each user experienced the five images in a random order, and the first trial with each image was used as a reference for matching input in the subsequent ten trials. During each trial, the user also had to rotate the image to a specific angle prior to making input. For the first trial, this rotation angle always corresponded to aligning the long axis of the phone with the camera, but for all other trials, the required angle randomly varied from this vector by up to 90°, in 10° increments, in both rotational directions. The required angle was shown on screen by a short yellow line, and the angular position of the image was tracked using the AR marker and displayed as a red line. Before they were able to make selections, participants needed align these two lines. Selections made on nonaligned images were discarded and participants presented with a mild warning—an error beep. In case of inadvertent errors, participants were also able to press an on-screen reset button and start a new trial at any time. In total, this study captured 3000 valid selection events—15 participants × 5 images × 10 trials × 4 selection items. For each selection, we logged time, the number of features extracted, and the matching score.

4) **Results:**The mean completion time was 15.5 s (SD: 1.2),the average number of features extracted was 7.6 (SD: 2.7), and the average matching score was 44.3% (SD: 11.4). We examined the independent variables of image (five levels) and angle (nineteen levels) separately using one-way repeated measures ANOVA and MANOVA tests. This is because of the sparsity of the data collected—although the design was repeated measures, the large number of angles considered meant that not every participant completed a trial with every possible combination of image and angle, thus precluding the use of two-way tests. For each variable, we conducted an ANOVA on the time data and a MANOVA on the closely related measures of number of features and match score. In all cases, Mauchley's test assessed sphericity, and, if violated, Greenhouse-Guesser corrections were employed. Effect sizes are reported in the form of partial eta squared (η_p^2).

We note that times were high because participants had to perform two substantial tasks—align the image on the Pass-BYOP camera system and, then, select four targets. As the alignment angle and selection targets were marked in the same way throughout the study, it is not surprising that task time re-mains relatively stable—a significant effect was observed, but the effect size is very small. The substantial variations in the number of features and match score according to the image variable highlight the importance of the choice of source image in the PassBYOP system—some of the images used in the study were more feature rich, resulting in a more distinctive canvas on which to enter a password.

V. CONCLUSION

In summary, SGPULPT proposed 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 SGPULPT substantially increases resistance to shoulder-surfing attacks compared with existing graphical password schemes. Ultimately, we argue and demonstrate that SGPULPT conserves the beneficial properties of graphical passwords while increasing their security.

Future Enhancement :Our future work will be based on Click-based graphical password schemes require a user to click on a set of points on one or more presented background images. With Pass Points, users create a password by clicking five ordered points anywhere on the given image. To log in, users must correctly repeat the sequence of clicks, with each click falling within an acceptable tolerance of the original point. To implement this aspect, along with a scheme converting the user-entered graphical password into a cryptographic verification key, a "robust discretization" scheme. It consisted of three overlapping grids (invisible to the user) used to determine whether the click-points of a login attempt were close enough to the original points to be accepted.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

REFERENCES

[1] A. Adams and M. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, pp. 40–46, 1999.
[2] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, "How to attack two-factor authentication internet banking," in *Proc. 17th Int. Conf. FinancialCryptography*, 2013, pp. 322–328.
[3] ARTigo, http://www.artigo.org/.
[4] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," *Proc. Comput. Syst. Appl.*, 2009, pp. 641–644.
[5] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learn-ing from the first twelve years," *ACM Comput. Surveys* vol. 44, no. 4
[6] G. E. Blonder, "Graphical passwords," U.S. Patent 5 559 961, 1996.
[7] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proc. IEEE Symp. Security Privacy*, 2012, pp. 553–567.
[8] S. Chiasson, R. Biddle, and P. van Oorschot, "A second look at the usability of click-based graphical passwords," in *Proc. 3rd Symp. Usable PrivacySecurity*, 2007, pp. 1–12.
[9] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proc. 12th Eur. Symp. Res.Comput. Security*, 2007, pp. 359–374.
[10] S. Chiasson, A. Forget, R. Biddle, and P. C. Oorschot, "User interface design affects security: Patterns in click-based graphical passwords, *Int.J. Inf. Security*, vol. 8, no. 6, pp. 387–398, 2009.
[11] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. Van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," *IEEE Trans. DependableSecure Comput.*, vol. 9, no. 2, pp. 222–235, Mar./Apr. 2012.
[12] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2013, pp. 2389–2398.
[13] B. Dodson, D. Sengupta, D. Boneh, and M. S. Lam, "Secure, consumer-friendly web authentication and payments with a phone," in *Proc. 2nd Int.ICST Conf. Mobile Comput., Appl., Serv.*, 2010, pp. 17–38.
[14] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2009, pp. 889–898.
[15] A. Gelman, J. Hill, and M. Yajima, "Why we (usually) don't have to worry about multiple comparisons," *J. Res. Educ. Effectiveness*, vol. 5, no. 2, pp 189–211, 2012.
[16] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," in *Proc. SIGCHI Conf.Human Factors Comput. Syst.*, 2010 pp. 1107–1110.
[17] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proc. 16th Int. Conf. World Wide Web*, 2007, pp. 657–666.
[18] S. Hart and L. Staveland, "Development of a multi-dimensional workload rating scale," *Human Mental Workload*. New York, NY, USA: Elsevier, 1988, pp. 139–183.
[19] H. Kim and J. Huh, "Pin selection policies: Are they really effective?" *Comput. Security*, vol. 31, no. 4, pp. 484–496, 2012.
[20] G. Lowe, "Distinctive image features from scale-invariant keypoints," *Int.J. Comput. Vision*, vol. 60, no. 2, 91–110, 2004.
[21] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human verifiable authentication," *Int. J. Security Netw.*, vol. 4, no. 1/2, pp. 43–56, Feb. 2009.
[22] D. Nelson, V. Reed, and J. Walling, "Pictorial superiority effect," *J. Exp.Psychol.: Human Learning Memory*, vol. 2, no. 5, pp. 523–528, 1976.