4th National Conference On Emerging Trends In Computer Science & Engineering (NCETCSE-2018)

PassBYOP: Bring Your Own Picture for Securing Graphical Passwords

[1]Bhargava B ,[2]Chethana A H, [3]Jeevitha Gowda , [4]Pooja B S , [5]Tanuj

[1,2,3,4]UG Students,[5]Assistant Professor

Department of Computer Science and Engineering.

BGS Institute of Technology , BG Nagar,Mandya-571448

Abstract-PassBYOP is a new graphical password scheme for public terminals that replaces the static digital images typically used in graphical password systems with personalized physical to-kens, herein 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 se-quence 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 PassBYOP 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 PassBYOP'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 Pass- BYOP shows promise for security while maintaining the usability of current graphical password schemes.

Index Terms—Graphical password, input, live video, observa¬tion, user study.

I. INTRODUCTION

Secure access to information underpins modern digital systems and services. We keep our communications, finan¬cial 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 nonsecure coping strategies such as reuse of passwords across systems, noting down passwords, or simply forgetting them en¬tirely [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], [32] and shoulder-surfing attacks [31]. Such attacks are effec-tive 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 rel¬atively predictable—users tend to choose hotspots such as the eyes in a facial portrait [11], [28], [32]. This issue is particu-larly 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 ac¬cessible user identity information [27].

To address this issue, we present a new point-click graphical password system, PassBYOP—Bring Your Own Picture, that in-creases resistance to observation attack by coupling the user's password to an image or object physically possessed. This is achieved by using live video

Manuscript received May 27, 2017; revised August 17, 2017; accepted September 26, 2017. The work of A. Bianchi was supported by the Samsung Research Fund, Sungkyunkwan University, 2014. The work of I. Oakley was supported by the Basic Science Research Program through the National Re-search Foundation of Korea funded by the Ministry of Science, ICT and Future Planning (2014R1A1A1002223). This paper was recommended by Associate Editor S. Rubin.

A. Bianchi is with the Department of Industrial Design, Korea Ad-vanced Institute of Science and Technology, Daejeon 305-338, Korea (e-mail: andrea.whites@gmail.com).

I. Oakley is with the Department of Human and Systems Engineering, Ulsan National Institute of Science and Technology, Ulsan 689-798,Korea (e-mail:ian.r.oakley@gmail.com).

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 PassBYOP feature based input; 2) participant task performance times and error rates using Pass-BYOP; and 3) the security of PassBYOP against observation attack.

II. RELATED WORK

Graphical password systems are knowledge-based authenti-cation 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 drawmetric schemes based on sketching shapes on screen, recognition-based cognometric schemes based on selecting known items from large sets of op-tions, and cued-recall locimetric schemes based on selecting regions of prechosen images [5], [14]. Locimetric 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.

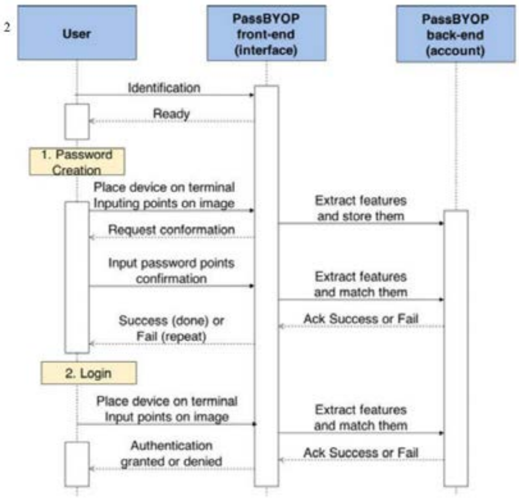
2
User
PassBYOP front-end (interface)
PassBYOP back-end (account)
Identification
Ready
1. Password Creation
Place device on terminal Inputing points on image
Request conformation
Input password points confirmation
Success (done) or Fail (repeat)
Extract features and store them
Extract features and match them
Ack Success or Fail
2. Login
Place device on terminal Input points on image
Authentication granted or denied
Extract features and match them
Ack Success or Fail

Fig. 1. Sequence diagram showing the steps involved in creating a PassBYOP password for the first time (1. Password Creation) and when attempting to login (2. Login).

III. PASSBYOP OVERVIEW

PassBYOP seeks to make graphical passwords more secure against intelligent guessing and shoulder-surfing attacks [27], [30]. We argue these weaknesses stem from the ease with which both password contents and password canvases can be observed or, in the case of canvases, directly accessed from a server [30]. PassBYOP tackles this problem by introducing a physi-cal token into the authentication process. This way, PassBYOP transforms a graphical password, which is traditionally a single¬factor authentication mechanism, to a more secure multifactor authentication method. We argue that this makes PassBYOP Resilient-to-lnternal-Observation [7], meaning that an attacker cannot impersonate a user simply by intercepting input on the authentication device or by eavesdropping on the communica¬tion between the authentication device and verification system.

PassBYOP authentication takes place as follows (see Fig. 1). Assuming users have previously created a password, login in-volves users identifying themselves at a PassBYOP terminal in a manner fitting the system and use context. For example, systems such as office door locks may assume all users are valid, while a user ID might be used on a public computer, and higher security applications, such as a bank ATM, will likely rely on a physi-cal token such as an ATM card. PassBYOP could be integrated into any of these scenarios. Second, users place a prechosen password image or object they possess on top of a camera unit in the terminal. This is captured and displayed live on an adja-cent touch screen. Third, they tap on the image locations that correspond to their password. This way, authentication requires both the physical token and the password simultaneously. We 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.

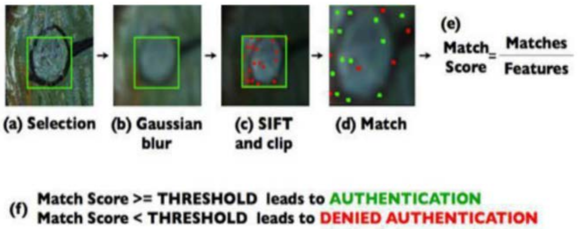
(a) Selection
(b) Gaussian blur
(c) SIFT and clip
(d) Match
(e)
Match Score = Matches / Features
(f)
Match Score >= THRESHOLD leads to AUTHENTICATION
Match Score < THRESHOLD leads to DENIED AUTHENTICATION

Fig. 2. PassBYOP process from image selection through feature extraction to image matching and production of a match score

IV. IMPLEMENTATION

The PassBYOP prototype consists of a 13.5-cm-wide x 22.5- cm-long x 12-cm-high plastic box with a transparent cover and containing an upward-facing Logitech QuickCam E3500 webcam with a resolution of 640x480 pixels and a speed of 30 frames/s. The webcam is connected to a PC running PassBYOP. The PassBYOP interface and video feed are shown on an Apple iPad that is connected wirelessly to the PC via a screen-sharing application [see (1) in Fig. 2] and fixed to the surface of a desk. The video resolution on the iPad is 450x600 pixels or approx-imately 8.5 cm x 14 cm. All input to the system is made on the iPad touchscreen. Specifically, as illustrated in (2) in Fig. 2, users make selections by tapping the screen to visually highlight 70 x 70 pixel (approximately 1.5 cm) 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 [see (3) in Fig. 2]. 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 [30], the passwords are represented as the XY image coordinates of finger selections. This technique does not work with PassBYOP as variations in image placement on the terminal camera will lead to substantial variations in the XY pixel positions of image content. Instead, PassBYOP 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 x 140 image subsection around the center point of each password item (see Fig. 3). 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 x 70 selection box were discarded and the remainder used for password matching [see Fig. 3(d)].

The matching process involved minimizing the Euclidean distance between the sets of feature points in the original and entered password items (see Fig. 4). Subsequently, a thresh-old on the percentage of matching features was used to de-termine 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 fea-tures extracted from a single image against a database containing 100 000 images with an overall accuracy of 80% [20].

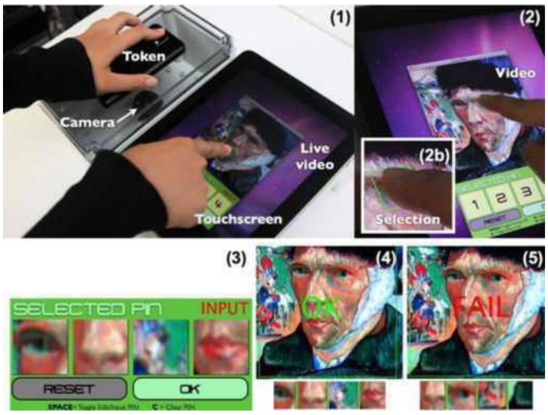

Fig. 2. (1) Overview of the PassBYOP system. (2) Input selection and closeup (2b). (3) Input selections that make up a password. (4) Successful authentication and (5) denied authentication.

V. EVALUATION

A. Reliability Study

This study assessed the reliability of PassBYOP in 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 Pass-BYOP'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 on the 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-II mobile phone with a screen resolution of 480 * 800 pixels and each image was preprocessed to match this screen resolution. We placed a 110-pixel square NyARToolkit fiducial marker [23] in the center of each image to enable accurate detection of its angle relative to the PassBYOP camera.

Four selection points were also marked on the image with a 110-pixel circle and labeled with numbers from 1 to 4. 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 PassBYOP 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 can be seen in Fig. 5. 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 experts or knowledgeable in the area of security research.

Procedure: For each of the five preselected images, each user 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). Fig. 6 shows the mean matching score for each angle studied. We exam-ined 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 mea-sures, the large number of angles considered meant that not every participant completed a trial with every possible combi-nation 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 num-ber of features and match score. In all cases, Mauchley's test assessed sphericity, and, if violated, Greenhouse-Geisser cor¬rections were employed2. Effect sizes are reported in the form of 2p = 0.009, nP = 0.305). Although there are modest variations in these latter measures, the number of features and match scores in both conditions exceed the thresholds of seven and 40% estab¬lished in the system feasibility study. Participants were capable of selecting and entering passwords with both the image selected by the experimenters and their own images.

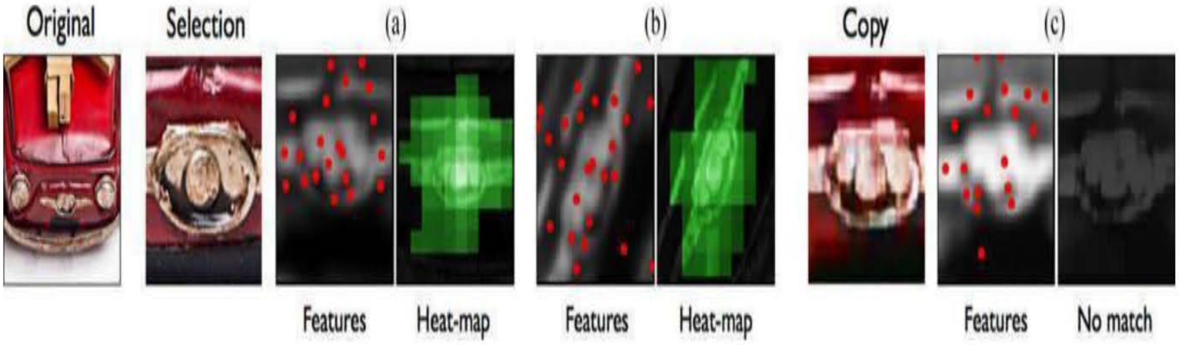

Fig. 4. Feature heatmap generated by testing the match between a selected area its transformations (rotation or translation) with the same image or a downgraded copy. Light colored zones in the heatmap indicate a match (white is 100% match). (a) Translated (b) Rotated (c) Translated.

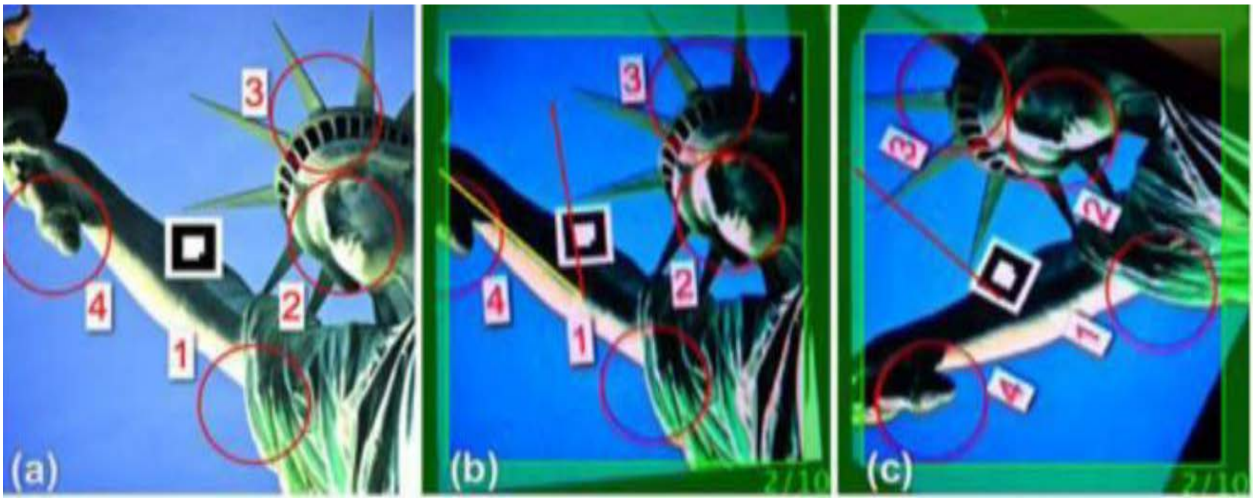

Fig. 5. (a) One of the five images used in the feasibility study. Colored lines showing the required and current angular orientation. (c) Image after the token has been rotated to match the required orientation.

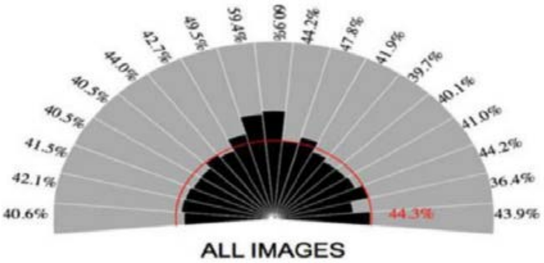

Fig . 6 . Matching score break down for angles in the feasibility study. The mean value across all angles is 44.3%

TABLE I
Results of the Usability Study

	System image	User image
Median creation time (s)	8.2 (5.7)	8.5 (2.9)
Median login time (s)	7.3 (2.8)	7.5 (2.1)
Password creation success rate	100%	100%
Successful login within 3 trials	100%	100%
Successful login at first trial	100%	85%
Successful login at second trial	–	100%
Total resets	6 / 87	7 / 90
Mean error items (in failed login)	1.7 / 4	2.1 / 4
Mean match score (successful)	72.9% (6.7)	77.1% (5.5)
Mean match score (fail)	27% (22.8)	13% (15.4)
Mean features (successful)	11 (2.2)	14.7 (4.5)

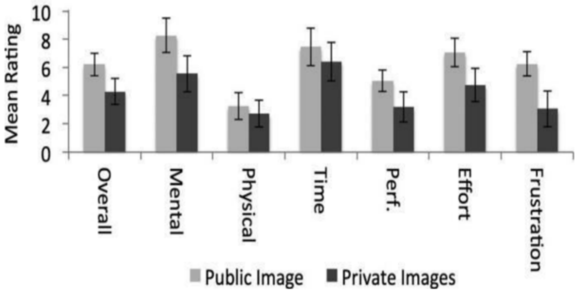

Fig. 7. TLX data showing workload in the usability study.

Number of seven features for each password item. Participants were first given an introduction to the system and its operation. They then completed a demographics form followed by the two experimental conditions. The TLX workload data are shown in Fig. 8. These show a general trend for reduced workload in the private image con¬dition, an observation borne out by a significant difference in the summed measure of Overall Workload (t (19) = 2.835, p = 0.011, d = 0.51). To protect against alpha inflation, we do not report results for the component workload measures. Par-ticipants also rated ease of creating passwords with the private and public images at 8.3 (SD 5.8) and 6.95 (SD 2.68) and mem-orability of the private and public images at 5.8 (SD 2.19) and 4.85 (2.52), respectively. These related measures were analyzed using repeated-measure MANOVA. Pillai's trace showed a sig-nificant effect of public/private images on ease of creation and 2 memorability (V = 0.369, F(2,1 8) = 5.263, p = 0.016, nP = 0.369). However, follow-up univariate ANOVAs revealed a sig-nificant difference only in terms of ease of password creation (F(2.4 8 8,1 8.2 2 5) = 7.325, p = 0.014, nP = 0.278). In general, these subjective data favor the private image condition over the public image condition. However, we recommend caution in¬terpreting these effects, as they necessarily involve a number of independent tests. While opinions differ on how to handle such multiple comparisons [15], we note a lack of significance differences if corrective procedures, such as using a more con¬servative threshold of a = 0.01, are applied.

In the posthoc interview, participants explained these ratings by remarking that the parking lot image contains too many similar cars, making selecting password locations challenging. Several also noted that although they felt it was easier to choose memorable locations from their private images, they still some-times confused selection points with visually similar locations in their images. Finally, participants acknowledged that the choice of their private image was important and that their perceptions of the security and usability of the system partially reflected these choices.

C. Security Analysis

This section provides a security analysis of the PassBYOP system. We developed a threat model for PassBYOP that is based on vectors including token theft, guessing (both educated and brute-force), and observation (via shoulder-surfing, camera attacks, and via malware that takes over the PassBYOP cam-era). We analyze theft and guessing attacks conceptually and describe a study to assess resilience to the three different forms of observation.

1) Theft: While PassBYOP cannot prevent theft, its close coupling of a token to a password does provide benefits. Unlike many types of authentication token (e.g., door entry cards), physical possession is insufficient to crack the system— attackers must also gain access to the password. This way, PassBYOP offers advantages over purely token-based systems, including

those based on secure device pairing over visual chan-nels [21], [25]. There are also three further advantages conferred by using a token displayed on a mobile device. First, attackers must unlock the mobile device to access the token, potentially facing an additional and unrelated security scheme. Second, they must identify the precise token image, a potentially challenging process. Third, users could conceivably use software to remotely wipe a token from a stolen device. This paper argues that the relative ease with which users would be able to restrict access to obscure or remove their PassBYOP password images provides a measure of resistance to attacks based on token theft over and above that present in more traditional token-based schemes.

2) Educated Guessing or Brute Force Attacks: From a se-curity perspective, typical cued-recall graphical passwords have practical password spaces comparable in cardinality to four- or five-digit PINs [5].

3) Observation: Cued-recall graphical passwords are vul-nerable to observation attacks. A single observation can be enough to disclose a password to a bystander [11], [30]. Re-flecting the importance of this vector, an observation attack was staged on the PassBYOP system to empirically assess the sys¬tem's resistance to this type of threat. Three types of observation were considered: shoulder-surfing, a camera attack, and an at¬tack based on malware that takes over the PassBYOP terminal and records the image displayed on the screen and the coordi¬nates of the input points selected by the user. This last attack represents a worse-case scenario—a substantial and comprehen¬sive man-in-the-middle attack akin to using the system camera to skim not only the password items entered, but also a copy of the image they are entered on. We conducted an empirical study to explore the resistance of PassBYOP to these vectors using the system configuration studied in the system feasibility study: passwords composed of four items, each with a minimum of seven features and matches recorded above a threshold of 40%.

4) Security Study: A member of our research group posed as a knowledgeable security conscious victim and repeatedly en-tered two PassBYOP passwords in two different attack scenar-ios. The first involved the use of a public system assigned image depicting a parking lot, as in [8], while the second involved the use of a private personally selected image, in this case a bowl of Japanese ramen. We argue that the public scenario mimics the case of conventional cued-recall graphical passwords, where the images used for authentication are stored on a server and dis-closed at login time. On the other hand, the private scenario ex-plores whether there is additional security value in PassBYOP's support for personally selected and maintained user-owned im-ages.

a) Participants: Three participants (attackers) completed this study, a typical size of participant pool for this kind of experiment [12]. They were all graduate students from Sungkyunkwan University majoring in computer security. None was otherwise involved with this research, and each attacked PassBYOP in both public and private scenarios. Procedure: The order of the scenarios was randomly assigned to each participant, and there was a 30-min break be-tween attempts to crack each scenario. While attempting to crack each scenario, participants performed a series of three increasingly sophisticated attacks: 1) shoulder-surfing followed by 2) camera attack followed by 3) malware combined with camera attack. For each attack type, participants were requested to spend at least 10 min attempting to authenticate and were allowed three attempts to enter the correct password. If at any point the password was cracked, the attacker was not required to continue cracking the same scenario. If all three attempts failed, they moved on to the next attack. As an incentive, attackers who succeeded to crack the password with shoulder-surfing were compensated with US$10, those who succeeded with camera attack received US$8, and US$5 was provided for success with the malware attack. Lunch was offered to all the attackers.

During the shoulder-surfing stage, attackers stood near the victim (within 1.5 m) during three successful logins. Note taking was encouraged. In this camera stage, attackers were provided with an HD video recording showing a closeup of the entire login process, including password item entry and a clear capture of the mobile device showing the image token. The video was shot without visual obstructions from less than 1 m away from the user with an HDR-HC3 HDV 1080i Sony camcorder. In the malware stage, attackers were provided with an additional video recording of the login phase from the point of view of the PassBYOP system camera. Attackers were able to use any tools or resources they wished during the attacks. In the public image condition, they were automatically presented with the authentication image, while in the private condition, they were able to use Internet searches and any image processing tools they wished to find, treat, create, or modify the source image and selection points observed and captured during the attack. In total, each participant spent approximately 3 h to complete the experiment.

c) Measures: We recorded the number of passwords cracked, the relative percentage matching scores, and the mean number of matching features: These last two measures indicate how well the attackers were able to reproduce the user's input images and selections—the higher the numbers, the stronger the attacks. We also distributed a questionnaire for the attackers to indicate on a ten-item Likert scale how difficult they felt the attack was and how well they self- evaluated their performance. Finally, in a poststudy interview, we asked them to describe their process.

d) Results: A single observation was enough for all three attackers to crack the public image password [11]. In fact, they were able to do so quickly and confidently—in less than 10 s and with a matching score of 65%, substantially over the system threshold of 40%. In the self-reported questionnaire, the attack was declared to be easy (2.3 SD:2.3) and the attackers' performance to be good (8.3 SD:2.8). They reported that they entered the password after the shoulder surfing observation. One attacker indicated he or she had taken notes. With private images, the shoulder-surfing attack was com-pletely unsuccessful.

The camera attack was also unsuccessful, but two attackers were able to compromise a single password item. This attack took longer (15-45 minutes) because attackers extracted frames from the HD footage when the phone was facing the camera and used image editing tools such as Adobe Photoshop to recompose the source image used in the authentication. The attack was reported to be moderately difficult (7, SD:1) and performance to be relatively low (4, SD:2.6). One attacker explained that the difficulty was to create an image to match the original observed image. Although the footage was clear, it was challenging to reproduce an identical replica, as even small variations of size, viewing angle, or illumination led to substantially different image features.

Finally, the malware and camera attack was the most effective—it represents a worst-case scenario. Two attackers were able to compromise two of the password items—half the full password. This attack took approximately the same time as the camera attack and was not reported to be easier (7.6 SD:0.5) although it resulted in modest improvements to self-reports of performance (5.3 SD:0.5). Attackers indicated they followed an image recomposition process broadly similar to that used with the camera attack, but they encountered two unexpected difficulties. First, the low resolution of the system camera (640 * 480) led to downsampled image captures that could not be directly used to authenticate—features derived from low-resolution copies differ from those extracted from high-resolution originals displayed on the phone. Second, mi-nor movements of the phone to bring the selection points into the field of view of the camera meant that attackers were not able to rely on a single frame showing the entire image and were forced to edit together multiple frames to produce their final image—a laborious task.

These results compare well with prior cued-recall password systems [8], [30], [31] that exhibit little to no resistance against shoulder-surfing. Attacks on PassBYOP took substantial time and effort and yielded a low success rate—although several items were successfully entered, no attacker managed to crack a full PassBYOP password. This result demonstrates the increased security of the PassBYOP approach against observation. It is particularly compelling as, although the attackers were partially able to crack the password, the threat model used in the malware attack was extremely generous in the type and nature of the infor¬mation provided. This suggests PassBYOP would exhibit a very high resistance to observation if deployed in a real-world setting.

VI. DISCUSSION

We presented three empirical examinations of the PassBYOP system. In the first, we established the feasibility of using image features as password items in terms of their uniqueness and the reliability with which they can be entered. In the second, we established basic user performance data while operating PassBYOP: Login took a median of 7.5 s, and although error data was unevenly distributed, mean rates were 9%. Finally, in the third study, we examined security and established that the use of an external token image increases the resistance to observation attack without compromising security against other vectors such as intelligent guessing or brute force. These results compare well with seminal prior work such as Passpoints [30], which yielded mean login times of 8.78-24.25 s and 1.55-2.75 failed authentication attempts prior to successfully entering a password. Similarly, Chiasson et al. [8] present a lab study of click-point- based graphical passwords using multiple images and report a median login time of 7 s and an error rate of 6%. Although we have informally tested the system with a range of mobile devices and token types and in different lighting conditions, formal study of these variables is an important next step toward demonstrating the robustness and viability of the approach. PassBYOP also used a low-resolution camera, which increased robustness against tamper-based ob-servation attacks, but may have made it harder to recognize genuinely correct tokens and features. In the future, PassBYOP performance should be tested with a variety of cameras. Finally, the current

PassBYOP system achieved multitouch input capa-bility by wirelessly streaming video from the PassBYOP host computer to an iPad tablet. While this approach was simple and effective, greater speed and efficiency would be attained with a native application.

In summary, this paper proposed improving the security of graphical password systems by integrating live video of a phys¬ical 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 sys¬tems 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 [5], [16], [30]. Ultimately, we argue this paper demonstrates that PassBYOP conserves the beneficial properties of graphical passwords while increasing their security.

ACKNOWLEDGMENT

We would like to thank our HOD and Guide.

REFERENCES

[1] 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. Financial Cryptography, 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,p. 19, 2012.

[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 Privacy Security, 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, 200