Bring Your Own Picture For Securing Graphical Password

Lavanya K N[1], Hithashree N A[2], Bharath G N[3], Manjunath S[4]
[1, 2, 3] Dept of Computer Science & Engineering
[4]Assistant Professor
[1, 2, 3, 4] S.J.C Institute of Technology Chikballapur - 562101

Abstract- *It is a new graphical password scheme for public terminals that replaces the static digital images typically with personalized physical tokens, 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 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 the feasibility studies of Picture examining its reliability, usability, and security against observation. The reliability study shows that image-feature based passwords are viable 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 inorder 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 the resistance to observation attack—three attackers are unable to compromise a password using shoulder surfing, camera-based observation, or malware. These results indicate that new scheme 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 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 difficulties to implement to guess are also hard to remember. This is a major problem as an average user possesses online accounts secured with up to six different passwords and representing as ubstantial 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. In order to mitigate these problems, researchers have proposed graphical password schemes that relyonin put such as selecting portions of an image. These systems have been shown to improve memorability without sacrificing input time or error rates while also maintaining a high resistance to brute force and guessing attacks. However, graphical passwords present their own problems. One issue is their susceptibility to intelligent guessing 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 This issue is particularly problematic as the image contents for graphical password systems are typically stored on authentication servers and readily presented to attackers in response to input of easily accessible user identity information To address this issue, we present a new scheme as Bring Your Own Picture, 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 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 and a demonstration of its viability through three feasibility studies covering: 1) the reliability and robustness of feature-based input; 2) participant task performance times and error rates and 3) the security of Picture against observation attack.

II. RELATED WORK

Graphical password systems are knowledge-based authenticationtechniquesthatleveragepeoples'abilitytomemoriz eand recognize visual information more readily than alphanumeric information. Researchers have explored three

broad types of graphical pass words: recall-based draw metric schemes based on sketching shapes on screen, recognition-based sonometric schemes based on selecting known items from large sets of options and cued-recall loci metric schemes based on selecting regions of prechosen images. Loci metric schemes are discussed as is multifactor authentication, as it relates and its combination of a token, or something you have, on which a password, or something you know, is entered.

Loci metric Password Schemes Cued-recall (loci metric) password schemes involve users selecting region son one or more images. 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. 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 tapping on the face, where one of the selection points was an eye 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. Evaluation soft his technique led to authentication times in the range of 7–8 s and success rates of 90–96%. A second key problem with loci metric systems is observation, as password click-points can be acquired by atackers after viewing a single authentication process. Securing against observation attack for graphical password systems is critical. "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 click points that uses eye-tracking technology 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 [26], 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, Alou et 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 device. The data from this marker generated encrypted data that were used during login. 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. This scheme is a multifactor authentication system—both a physical token and a password are needed to authenticate. It differs from prior approaches in three ways. First, it is more flexible—instead of posing restrictions on the form of tokens, any sufficiently complex image or object can be used as a 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 picture are high-entropy, sufficiently so that they have been previously proposed as a single factor authentication scheme.

Picture seeks to make graphical passwords more secure against intelligent guessing and shoulder-surfing attacks. We argue these weaknesses stem. From the case with which both password contents and password canvases can be observed or, in the case of canvases, directly accessed from a server. It tackles this problem by introducing a physical token into the authentication process. This way, BYOP transforms a graphical password, which is traditionally a single factor authentication mechanism, to a more secure multifactor authentication method. We argue that this makes Resilient-to-Internal-Observation meaning that an attacker cannot impersonate a user simply by intercepting input on the authentication device or by eavesdropping on the communication between the authentication device and verification system. BYOP authentication takes place as follows Assuming users have previously created a password, login involves users identifying themselves at a terminal in a manner fitting the system and use context. For example, systems such as office door locks may as sum of all users are valid, while a user id might be used on a public computer, and higher security applications, such as a bank, will likely rely on a physical token such as an ATM card. It 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 adjacent 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 raise the resistance to attacks based on password observation and guessing as attackers need to possess a user's genuine token or a high fidelity copy.

III. IMPLEMENTATION

The Pass BYOP 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 30frames/s. The web cam is connected to a PC running Pass BYOP. The interface and video feed are show non-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, as illustrated in (2) in users make selections by tapping the screen to visually highlight 70×70 pixel (approximately1.5cm2) 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

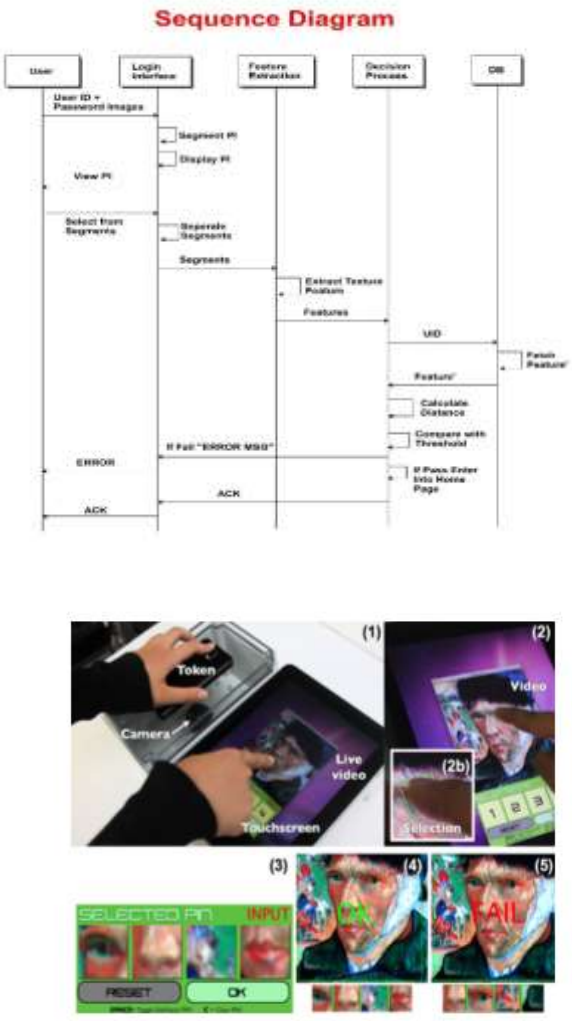
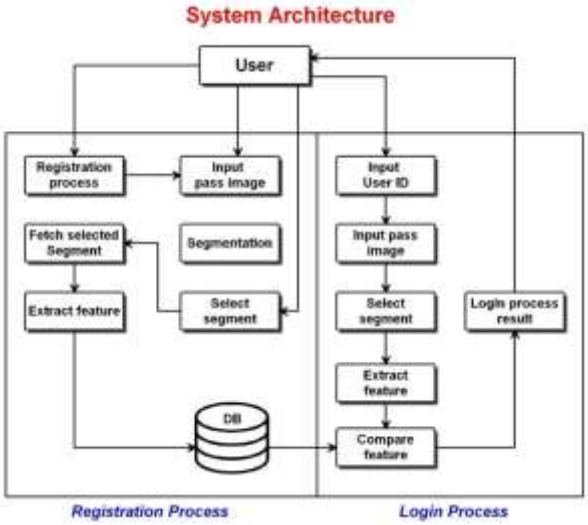


Fig. 2. (1) Overview of the PassBYOP system. (2) Input selection and closeup (2b). (3) Input selections that make up a password. (4) Successful authentication and (5) denied authentication.

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 fingers elections. This technique does not work with Pass BYOP as variations in image placement on the terminal camera will lead to substantial variations in the XY pixel positions of image content. Instead, Pass BYOP selections are stored on the authentication server as a set of optical features computed with the SIFT image processing algorithm. 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 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 central70× 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 threshold 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 100 000 images with an overall accuracy of 80%.



1. User Registration:

In this module user has to register by giving his information such as user id, user name, password, valid e-mail id etc., and after giving this information, user has to upload the

image which he has brought with him. After uploading, he has to select the five locations in that image as the password.

2. Upload Image:

In this module user has to upload image at the time of registration and same image at the time of authentication, image will be split in to the number of coordinate blocks and store in the application, if the user selects the location, that location specific block hash code will be stored in the database.

3. Hash code generation and GLCM (Grey Level Co-occurrence Matrices) process:

After successful selection of locations of the image, chunks of the selected image locations will be created, those details will be stored in the database, concatenating all the images locations, generate hash code for that and store in the database with respect to the user.

Password image chunks will be stored in the server.

In the GLCM process firstly convert the chunk images in to the grey scale, then get the Feature Vector of the chunks, Calculate the distance histogram of Feature Vectors between password chunks and selected chunks, if the distance is zero , then successful password authentication will be provided.

4. User Login Process:

Registered user will be login to the application by using his user id and password. After successful login , user has to upload the image which he has uploaded at the time of password setting , In the uploaded image he has to select the locations , concatenating all the images locations ,generate hash code for that .if the hash code is matched with the existing hash code and also the GLCM , user can successfully enter in to the home page , else, process ends and login page will display.

5. Admin:

Admin has to login to his account by the authenticated user name and password. Admin can able to view all the user's details, who are successfully region.

IV. ALGORITHM

Haralicket all first introduced the use of co-occurrence probabilities using GLCM for extracting various texture features. GLCM is also called as Gray Level Dependency Matrix. It is defined as "A two-dimensional histogram of gray levels for a pair of pixels, which are separated by a fixed spatial relationship." GLCM of an image is computed using a displacement vector d, defined by its radius δ and orientation θ. To reduce the dimension of the GLCM feature Harralicket all proposed texture features that can be categorized into contrast, orderliness, homogeneity and statistical features. Others include sum and difference measures, maximal correlation coefficient and information measures of correlation1 and 2.

The basic GLCM algorithm is as follow:

1. An image texture is a set of standards of measurements computed in image processing intended to enumerate the apparent texture of a leaf image. Leaf image texture gives information regarding the spatial arrangement of color or intensities in a leaf image or selected region of a leaf image.
2. The co-occurrence matrix GLCM (i,j) counts the co-occurrence of pixels with gray value i and j at given distance d. The direction of neighboring pixels to represents the distance can be selected.
3. Count all pairs of pixels in which the first pixel has a value i, and its matching pair displaced from the first pixel by d has a value of j.
4. This count is entered in the Ith row and jth column of the matrix Pd[i,j]
5. The elements of Pd[i,j]can be normalized by dividing each entry by the total number of pixel pairs.
6. Normalized GLCM N[i,j], defined by:

$$N[i,j] = \frac{P[i,j]}{\sum_i \sum_j P[i,j]}$$

EVALUATION

1. Reliability Study

This study assessed the reliability of Pass BYOP 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 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.

2. Security Analysis

This section provides a security analysis of the Pass BYOP system. We developed a threat model for Pass BYOP 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 Pass BYOP camera). We analyze theft and guessing attacks conceptually and describe a study to assess resilience to the three different forms of observation.

a) Theft: While Pass BYOP 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, Pass BYOP offers advantages over purely token-based systems, including those based on secured evince pairing over visual channels. 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 Pass BYOP 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 security perspective, typical cued-recall graphical passwords have practical password spaces comparable in cardinality to four- or five-digit PINs. Data from the feasibility study suggest that Pass BYOP has a similarly sized password space—with a matching threshold of 40%, the heatmap analysis indicates that each Pass BYOP selection has a viable radius of 35 pixels (0.75 cm), leading to a valid selection area of 0.56 cm2, a figure very close to that used in benchmark systems such as the 0.53cm2 used in Pass Points. Thus, given a total selection space of 450 × 500 pixels, the total number of discriminable selection points for each user input is approximately ∼220. Over a four-item PIN, according to the calculations used by Wiedenbeck et al, this leads to a total Hartley entropy (or available password space) of ∼log2(220.44), a figure greatly exceeding that of a four-digit numerical PIN [5]. We acknowledge that these entropy figures are optimistically high and represent a theoretical maximum—in reality, only a subset of the possible hotspots are actually likely to be selected.

However, this entropy calculation appears in closely related work, and using this common formulation makes Pass BYOP comparable with prior work. We also note that in contrast with other graphical password schemes, Pass BYOPs use of a token makes guessing attacks insufficient if used alone—they must be combined with theft or observation in order to also acquire either the users token or a high fidelity copy. We argue that this increases the security of Pass BYOP relative to prior approaches.

3) Observation: Cued-recall graphical passwords are vulnerable to observation attacks. A single observation can be enough to disclose a password to a by stander. Reflecting the importance of this vector, an observation attack was staged on the Pass BYOP system to empirically assess the system's resistance to this type of threat. Three types of observation were considered: shoulder-surfing, a camera attack, and an attack based on malware that takes over the Pass BYOP terminal and records the image displayed on the screen and the coordinates of the input points selected by the user. This last attack represents a worse-case scenario—a substantial and comprehensive 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 enter icon. We conducted an empirical study to explore the resistance of Pass BYOP 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 entered two Pass BYOP passwords in two different attack scenarios. The first involved the use of a public system assigned image depicting a parking lot, as in, while the second involved the use of a private personally selected image, in to his 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 disclosed at login time. On the other hand, the private scenario explores whether there is additional security value in Pass BYOP's support for personally selected and maintained user-owned images.

V. RESULTS

Table shows the results of the attacks for authentications with both public and private images. A single observation was enough for all three attackers to crack the public image password. 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 completely unsuccessful. Although attackers spent between 10 and 30 min trying to find a similar image using the Internet (one attacker searched on the victim's personal homepage), they were unable to authenticate within the given trials, and none of the features could be matched. Attackers reported the task to be difficult (10, SD:0) and their performance to be low (3.6, SD: 4.6). We attribute this low performance to the fact that the SIFT algorithm is capable of detecting and recognizing the features of a single image from a dataset of 100 000 key points with an accuracy of 80% .As such, even If an attacker synthetically constructs an image where each pixel is computationally generated with a random color ,the chance that any of the features required per selection will match the features of the stored password image will be 20% or lower. Based on this

TABLE II

RESULTS FOR THE OBSERVATION ATTACK USING PUBLIC AND PRIVATE IMAGES SHOWING 1) NUMBER OF ITEMS CRACKED, 2) THE PERCENTAGE MEAN MATCH SCORE ATTAINED, AND 3) THE MEAN NUMBER OF MATCHING FEATURES

	Shoulder surfing			Camera			Malware & Camera		
	Items cracked	Mean score	Features	Items cracked	Mean score	Features	Items cracked	Mean score	Features
Attacker1	4/4	62.75%	6.25	–	–	–	–	–	–
Attacker2	4/4	65%	6.25	–	–	–	–	–	–
Attacker3	4/4	63.25%	6.75	–	–	–	–	–	–
Average	4/4	63% (0.2)	6.4(0.3)	–	–	–	–	–	–

	Shoulder surfing			Camera			Malware & Camera		
	Items cracked	Mean score	Mean Features	Items cracked	Mean score	Mean Features	Items cracked	Mean score	Mean Features
Attacker1	0/4	0%	0	1/4	12.5%	1.12	0/4	0%	0.5
Attacker2	0/4	0%	0	1/4	26.58%	3.41	2/4	22.12%	2.25
Attacker3	0/4	0%	0	0/4	17.07%	1.62	2/4	41.5%	4.12
Average	0/4	0%	0	0.7(0.6)	19.19(8.3)	2.1(1.2)	1.3(1.1)	21.99(16.8)	2.29(1.8)

evidence, we argue that even with the more liberal matching threshold of 40% used in Pass BYOP, the chances of a randomly generated image leading to a matching feature set is very low—certainly much lower than the one intent chance of guessing a single numeric PIN item. The camera attack was also unsuccessful, but two attackers were able to compromise a single password item. This attack took longer(15–45minutes) 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 were 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 recompositing 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 down sampled 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, minor 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 Pass BYOP took substantial time and effort and yielded a low success rate—although several items were successful entered, no attacker managed to crack full Pass BYOP password. This result demonstrates the increased security of the Pass BYOP approach against observation. It is particularly compelling as, although the attackers were partially able to crack the password, the threat model used in them alware attack was extremely generous in the type and nature of the information provided. This suggests Pass BYOP would exhibit a very high resistance to observation if deployed in areal-world setting.

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. 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,andP.vanOorschot,"Graphicalpasswords:Learning 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,andP.vanOorschot,"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, 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. Dependable Secure Comput., vol. 9, no. 2, pp. 222–235, Mar./Apr. 2012.

[12] A.DeLuca,E.vonZezschwitz,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,consumerfriendlywebauthenticationandpayments withaphone,"inProc.2ndInt. 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," inProc.SIGCHIConf.HumanFactorsComput.Syst.,2009,pp .889–898.

[15] A.Gelman,J.Hill,andM.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-gazeentry incued-recall graphical passwords," in Proc.SIGCHIConf. 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.Hartand L.Staveland, "Development of a multi dimensional work load 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,"Distinctiveimagefeaturesfromscaleinvariantkeyp oints,"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 cameraphonesforhumanverifiableauthentication,"Int.J.Sec urityNetw., 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.

[23] NyARToolkit. 2015. [Online]. Available: http://nyatla.jp/nyartoolkit
K.Renaud and A.DeAngeli, "My password is here! An investigation in to visuo-spatial authentication mechanisms," Interacting Comput., vol. 16, pp. 1017–1041, 2004.

[24] N. Saxena, J. E. Ekberg, K. Kostiainen, and N. Asokan, "Secure device pairing based on a visual channel (short paper)," in Proc. IEEE Symp. Security Privacy, 2006, pp. 306–313.