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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

A Survey of Bring your Own Picture for Securing Graphical Passwords

S.V. Jinisha[1], R. Kalaiselvi[2],

P.G Student, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay, Tamilnadu, India [1]

Associate Professor, Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil, Thuckalay, Tamilnadu, India [2]

Abstract: For the vast majority of computer systems, passwords are the method of choice of authenticating users. However, passwords suffer from limitations in terms of memorability and security passwords that are difficult to guess and also hard to remember. To address this issue, proposed a new point-click graphical password system, PassBYOP that increases resistance to observation attack by coupling the user's password to an image or object physically possessed. This is achieved by using a photograph or even an image of a body part, as the canvas for entering a graphical password. In previous graphical password systems, the passwords are represented as the XY image coordinate selections, PassBYOP selections a set of optical features computes with the SIFT image processing algorithm and are stored on the authentication server. The matching process is involved in minimizing the Euclidean distance between the sets of feature points in the original and entered password items. 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.

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

I.INTRODUCTION

Secure access to information underpins modern digital systems and services. Passwords 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 [5] 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 [13]. This is a major problem as an average user possesses 25 online accounts secured with up to six different passwords [12] 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]. To mitigate these problems, researchers have proposed *graphical password* schemes [3], [4] 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 [17] while also maintaining a high resistance to brute force and guessing attacks [3]. One issue is their susceptibility to intelligent guessing [3], [6],[24] and shoulder-surfing attacks [23].

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 [16]. Researchers have explored three broad types of graphical passwords: recall-based *drawmetric* schemes based on sketching shapes on

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

screen, recognition-based *cognometric* schemes based on selecting known items from large sets of options, and cued-recall *locimetric* schemes based on selecting regions of prechosen images [3], [10]. Locimetric schemes are multifactor authentication, as it relates to PassBYOP. setting up a camera to record input and also relatively predictable—users tend to choose *hotspots* such as the eyes in a facial portrait [9], [21], [24]. This issue is particularly problematic as the image contents for graphical password systems are typically stored on authentication servers [3].To address this issue, we present a new point-click graphical password system, *PassBYOP—Bring Your Own Picture*, that increases resistance to an observation attack by coupling the user's password to an image or object physically possessed. This is achieved by using a live video of a physical token, such as an object, a photograph, or even an image of a body part as the canvas for entering a graphical password. We present an implementation for the scheme based on SIFT image features [14] 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 PassBYOP 3) the security of PassBYOP against observation attack.

A. Locimetric Password Schemes

Cued-recall (locimetric) 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 PassPoints [22]. 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, while simple and effective, cued-recall graphical passwords present new security issues. For instance, users typically select *hotspots* [21], locations on an image that is 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[24]. Addressing this issue, the cued-click points (CCP) [7] system presented a series of images and allowed users to select only a single point per image, reducing the need to select common hotspots.

B. Multifactor Authentication Schemes

Multifactor authentication [19], 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. 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 [2].PassBYOP is a multifactor authentication system—both a physical token and a password are needed to authenticate. PassBYOP 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 PassBYOP 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 easy to understand. Finally, the image tokens in PassBYOP are high-entropy, sufficiently so that they have been previously proposed as a single factor authentication scheme [14]. 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. PASSBYOP OVERVIEW

PassBYOP seeks to make graphical passwords more secure against intelligent guessing and shoulder-surfing attacks [20],[22]. This way, PassBYOP transforms a graphical password, which is traditionally a single factor authentication mechanism, to a more secure multi-factor authentication method. We argue that this makes PassBYOP *Resilient-to-Internal-Observation* [5], 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. Authentication requires both the physical token and the password simultaneously. We

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

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.

IV. IMPLEMENTATION

The PassBYOP 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 QuickCam E3500 webcam with a resolution of 640×480 pixels and a speed of 30 frames 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 450×600 pixels or approximately 8.5 cm × 14 cm. All input to the system is made on the iPad touch screen. Specifically, as illustrated in (2) in Fig. 2, users make selections by tapping the screen to visually highlight70×70 pixel (approximately 1.5 cm2) 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. (3) in Fig. 2]. Users must input a total of four items and then press an OK button 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 [22], the passwords are represented as the *XY* image coordinates of finger selections. Instead, PassBYOP selections are stored on the authentication server as a set of optical features computed with the SIFT

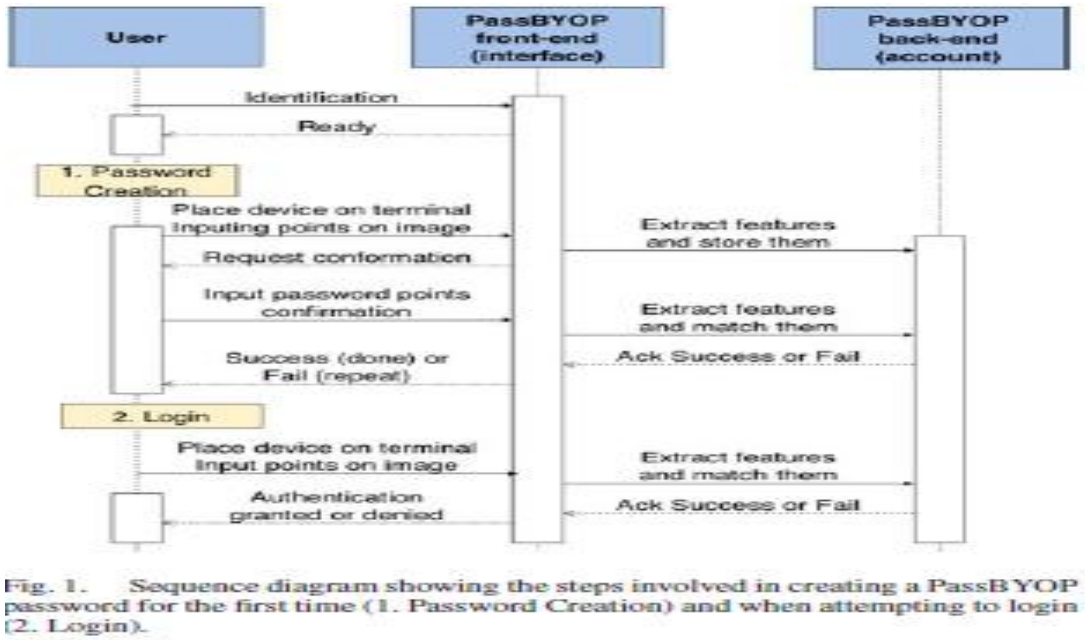

Fig. 1. Sequence diagram showing the steps involved in creating a PassBYOP password for the first time (1. Password Creation) and when attempting to login (2. Login).

Figure 1: Password creation.

image processing algorithm. [14].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 [14]SIFT algorithm was computed with the peak threshold set to 2 and the edge threshold set to 10. 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

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

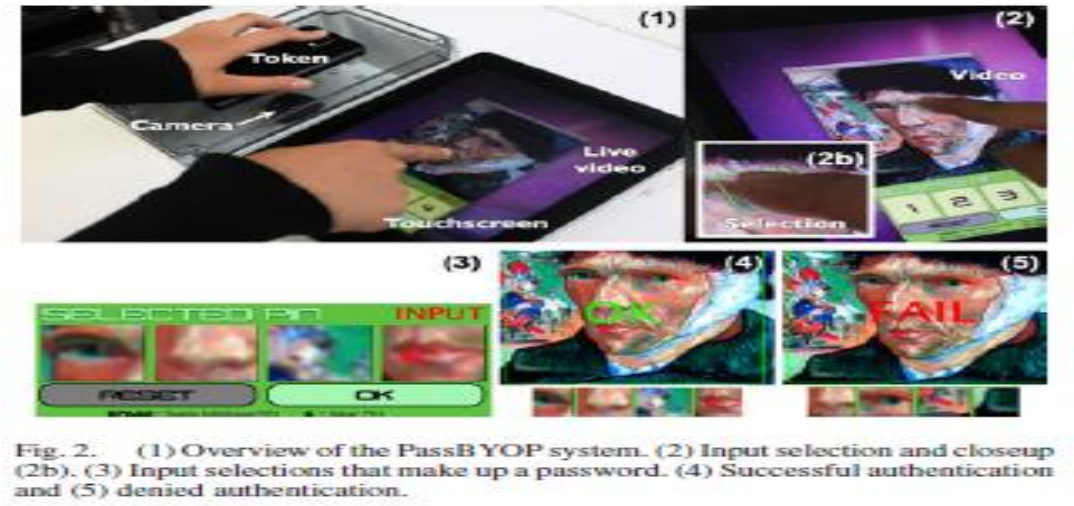

Fig. 2. (1) Overview of the PassBYOP system. (2) Input selection and closeup (2b). (3) Input selections that make up a password. (4) Successful authentication and (5) denied authentication.

Figure2: Overview of the PassByop System.

between the sets of feature points in the original and entered password items. A threshold on the percentage of matching features was used to determine whether the entered password matched the original. This process hinges on the fact that SIFT features are highly distinctive, robust to noise, accurate, and rotation invariant.

Fig. 3. PassBYOP process from image selection through feature extraction to image matching and production of a match score.

Figure 3: PassByop Process from image selection through feature extractionto image matching and production of a match score.

V. COMPARISON OF PASSMATRIX WITH SIFT

Method/Time(ms)	Create Time	Login Time	Confirm Time
PassMatrix	8.6	7.8	9
PassMatrix+SIFT	6	4.8	4.6

Figure 4: Create, login, and Confirm time of PassMatrix with SIFT features.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

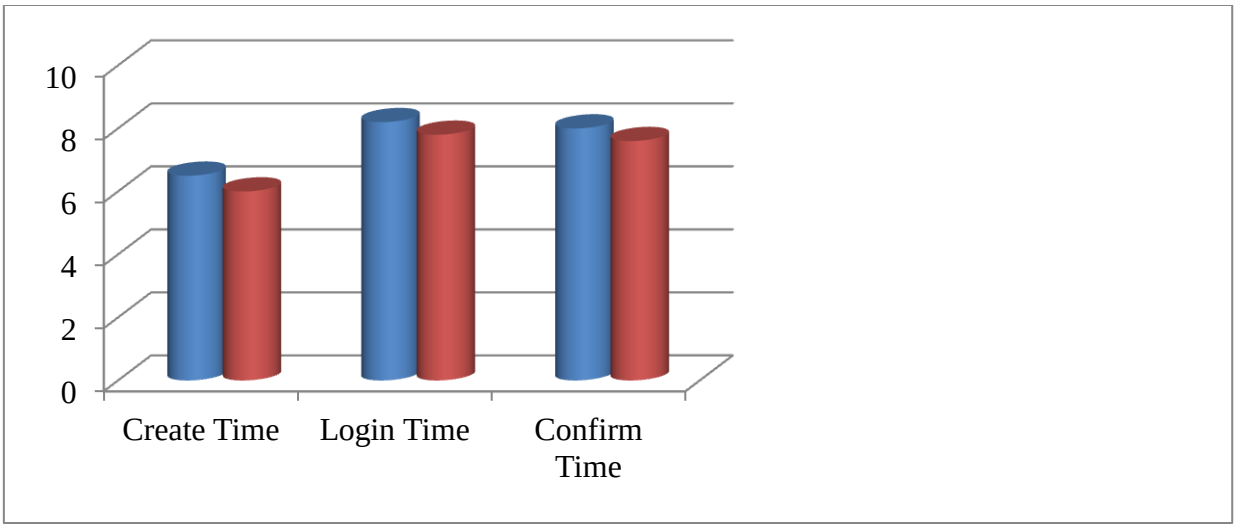

Figure 5: performance analysis of Create Time, Login Time and Confirm Time.

VI. EVALUATION

A. Reliability Study

This study assessed the reliability of PassBYOP 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. 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.

B. Usability Evaluation

The second study in this paper explores user performance with PassBYOP in terms of entry times and error rates for comparison with prior graphical password system schemes.

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 and observation 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 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 channels [15], [18]. 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

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

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 security perspective, typical cued-recall graphical passwords have practical password spaces comparable in cardinality to four- or five-digit PINs [3].

3) Observation:

Cued-recall graphical passwords are vulnerable to observation attacks. A single observation can be enough to disclose a password to a bystander [9],[22]. Reflecting on the importance of this vector, an observation attack was staged on the PassBYOP 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 PassBYOP 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 worst-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 entered on.

VII. 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 were unevenly distributed, the 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. This is a highly positive conclusion as the underlying complexity of the recognition and comparison system in PassBYOP is substantial—to achieve equivalent results to prior graphical password systems is a strong endorsement of the technical viability of the approach.

This result also shows that the increased resistance to observation achieved by PassBYOP does not place additional burdens on users—speed and accuracy are broadly comparable with prior systems. Worth contextualizing is the conclusion in the light of prior work that aims to compare graphical passwords against observation attacks. It allows users to enter information comfortably and traditionally, while still introducing a hard-to-observe component—the PassBYOP tokens. Furthermore, the fact that these tokens are self-selected, rather than issued by a central certified authority, such as a bank, may also confer additional advantages. Specifically, in the usability study, participants experienced lower levels of self-reported workload and stated they preferred their own images to a standard system provided alternative. In terms of the system, we used SIFT, a single feature extraction technique, and a more extensive investigation of alternative techniques may reveal a more efficient or otherwise optimal candidate. Similarly, the feature matching algorithm we used was based on the comparison of Euclidean distance between features, as in [14]. Exploring more advanced similarity metrics could improve system performance. Furthermore, we did not perform any formal evaluation to determine the feasibility of PassBYOP across different devices and in different environmental conditions. Although we have informally tested the system with a range of mobile devices and token types and in different lighting conditions, the 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 observation attacks but may have made it harder to recognize genuinely correct tokens and features.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

VIII. CONCLUSION

In the future, PassBYOP performance should be tested with a variety of cameras. Finally, the current PassBYOP system achieved multitouch input capability 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. This paper 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 PassBYOP substantially increases resistance to shoulder-surfing attacks compared with existing graphical password schemes[3], [11], [22]. Ultimately, we argue this paper demonstrates that PassBYOP conserves the beneficial properties of graphical passwords while increasing their security.

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] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys* vol. 44, no. 4,p. 19, 2012
[4] G. E. Blonder, "Graphical passwords," U.S. Patent 5 559 961, 1996.
[5] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of webauthentication schemes," in *Proc. IEEE Symp. Security Privacy*, 2012, pp. 553–567.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] H. Kim and J. Huh, "Pin selection policies: Are they really effective?"*Comput. Security*, vol. 31, no. 4, pp. 484–496, 2012.
[13] G. Lowe, "Distinctive image features from scale-invariant keypoints, " *Int. J. Comput. Vision*, vol. 60, no. 2, 91–110, 2004.
[14] 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.
[15] D. Nelson, V. Reed, and J. Walling, "Pictorial superiority effect," *J. Exp. Psychol.: Human Learning Memory*, vol. 2, no. 5, pp. 523–528, 1976.
[16] K. Renaud and A. De Angeli, "My password is here! An investigation into visuo spatial authentication mechanisms," *Interacting Comput.*, vol. 16,
pp. 1017–1041, 2004.
[17] 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.
[18] B. Schneier, "Two-factor authentication: Too little, too late," *Commun. ACM*, vol. 48, no. 4, p. 136, 2005.
[19] F. Tari, A. Ozok, and S. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords,"in *Proc. 2nd Symp. Usable Privacy Security*, 2006, pp. 56–66.