Can I Guess Your Password? Examining Security Aspects of Graphical Passwords

Tahani Alsubait, Raghad Alabdullatif
tmsubait@uqu.edu.sa, s43780117@st.uqu.edu.sa
College of Computer and Information Systems, Umm Al-Qura University, P.O.Box: 715, Makkah, Saudi Arabia

Abstract
Whenever there is a password required to access a system, the security of this system is measured in part by the strength of the used password. Guessability is a serious security attack that has been widely used to crack passwords in relatively short times. It can take many forms such as brute force (exhaustive search) and dictionary attacks. Generally speaking, the concept has been extensively studied in the context of traditional text-based or alphanumeric passwords. However, as different graphical password schemes start to evolve, there is an urgent need to explore and analyze geussability and other security aspects of this scheme, especially, given that it is regarded a usable solution preferred to users due to their memorability feature. In this paper, we present our empirical findings on the topic after conducting a user study and a post-experiment questionnaire. We also survey the related literature and conclude with some recommendations for further research in the area.

Key words:
Authentication, Security, image-based authentication, graphical passwords, user study

1. Introduction

Security measures taken by various information systems include requesting users to provide passwords that confirm their identity. These passwords can take different forms. A traditional example of passwords is the personal identification number (PIN) used in automatic teller machines (ATMs) and mobile phones. In addition to the alphanumeric passwords, text-based passwords are also common in login screens, e.g., email login. Moreover, a password can be biometric such as eyeprints, fingerprints and faceprints which are widely used in modern smart phones. Despite their widespread, these biometric passwords raise concerns regarding privacy as people are reluctant to providing their personal biometric data that may be misused or hacked and prefer to use them in limited applications such applications that provide governmental services. Similarly, traditional text-based passwords suffer from many security issues [1]. A study back in 1990 showed that 25% of passwords could be cracked using simple dictionary attacks [2]. More recently, with advancements in algorithms and processing powers, an article reported that 80% of passwords were cracked in just 30 seconds [3].

As methods of compromising traditional passwords get improved, researches thrive to find alternative solutions [4]. One promising alternative is the more recent graphical password, also referred to as image-based password, with real world deployments. Image-based passwords have been mainly suggested by HCI researchers to improve usability of login procedures as it is widely believed that human memories are better in remembering images, compared to text [5, 6, 7, 8]. In addition to studying the memorability effect of whole images, some studies showed an interest in studying the memorability of certain areas of images [9], a concept related to the state-of-the-art Persuasive Cued Click Points (PCCP) in the graphical passwords area of research. Nonetheless, security aspects of graphical passwords still need further consideration by researchers in the “usable security” community.

Different schemes of graphical passwords have been proposed, the above-mentioned cue-recall scheme being one of them [1]. Other schemes include recall-based systems, where users are asked to recall the whole graphical password by drawing it, and recognition-based schemes, where users are asked to identify images that they have previously selected during registration.

On a series of studies on different authentication mechanisms, we noticed an interesting phenomenon when asking participants to setup cue-recall passwords; people tend to choose similar cue click points. This has brought up some questions regarding how effective graphical passwords are, and more precisely, how vulnerable they are to guessability attacks. Along similar lines, there is a need to develop measures of the strength of a given image-based password, just as we do with text-based passwords. Given such measurement, helpful suggestions can be offered to users to help them choose stronger passwords, and hence, enhance the security, and possibly usability, of image-based passwords. General rules or recommendations are usually given to users when choosing their text-passwords, such as avoiding the use of very common passwords, e.g., the word “love”, or widely accessible personal information, e.g., user’s birthdate or children’s names and so on. Moreover, calculating password space for text-based passwords is a well-known process, however, this is not the case for image-based passwords. Note that studying password spaces is

Manuscript received April 5, 2020
Manuscript revised April 20, 2020

something that can be done and understood theoretically, but understanding common user behavior when choosing passwords is something that must be done empirically through user studies. In this research, we present our findings on the topic after conducting a user study composed of two phases: a simulation phase and a post-questionnaire phase. We discuss these findings and conclude with some thoughts for advancing research in this demanding area.

2. Background and terminology

Many concepts that apply to text-based passwords also apply to graphical passwords. In this section, we shed light on some of these concepts and provide some examples to understand how they are applied in the graphical password's context.

2.1 Password space

Password space refers to the number of unique password options available. For example, if the user is allowed to choose a 4-digit numerical PIN, the password space would be (104). Similarly, for recognition-based graphical passwords, we consider the number of images available in the panel and the number of rounds. For example, the password space of a panel of 7 images and 4 rounds is (74). For cue-recall graphical passwords, we consider PassPoints [10, 11, 12], where a password is a sequence of n=5 click points in a given image, as an example to determine the password space. Given that the password recall is acceptable within a system-specified tolerance, the theoretical password space is reported to be 243 conceivable passwords. We argue that increasing the number of click-points and decreasing the tolerance space improve security.

Passwords' spaces are considered a measure of the strength of the password mechanism. Obviously, the higher the password space is the higher its resistance to guessability attacks, as we will see below.

2.3 Guessing entropy

The password entropy indicates how random users create passwords out of a given password space [13]. It relates to the ability of the attackers to guess the password and how difficult it is for them to do so.

2.4 Guessability attacks

Guessing attacks are among the most common types of attacks. We reported some statistics on such attacks for the traditional text-based passwords in the introduction section. However, statistics on similar attacks for image-based passwords are scarce. Dictionary attacks and Exhaustive-search (brute-force) attacks are common example of guessing attacks [14]. The former refers to predicting a list of commonly used passwords with high probability in order to reach an acceptable success rate [15]. The latter refers to the exhaustive search of all possible passwords within the theoretical password space.

On the other hand, there many defensive methods that have been proposed against guessing attacks [1]. These include the use of CAPTCHA [16], limiting the number of login attempts, two factor authentications, to name a few.

2.5 Capture attacks

Another kind of security attacks on different password schemes is the so-called capture attacks [17]. Shoulder surfing attacks and social engineering attacks are some common examples of capture attacks. Shoulder surfing attack refers to the usage of observation techniques in order to capture the login credentials, whether by observing the login process directly or recording it via external recording devices. As the screen space required for displaying image-based passwords are bigger compared to the space required to enter traditional text-based passwords, shoulder surfing attacks must be taken more seriously in graphical passwords. Despite that, some early graphical password schemes argued that they are resistant to shoulder-surfing attacks [1].

Social engineering is considered a hot issue in the security domain. Attackers can gain access to secure systems by convincing users to divulge their login credentials by manipulating them in a social engineering manner. A common type of social engineering is phishing attack, which is tricking the user to enter his/her login credentials into a fraudulent website that disguised as a legitimate source with the aim to steal the login credentials.

3. Related work

Previous studies in the area of graphical passwords present a wide range of solutions and lay down a theoretical backing for future researchers. For example, Biddle et al. [1] surveyed published literature in the area of graphical passwords in a twelve-year period, focusing on security and usability features of the proposed methods. They identified usability requirements and highlighted major security threats that need to be addressed by image-based password schemes. Other papers that survey the area of graphical passwords include [18, 19].

Along similar lines, Zhu et al. [20] lay down a theoretical foundation for understanding memorability in click-based images. They developed a model of image point memorability (IPM) and discuss both the defensive and offensive applications of the proposed model. For example, they show how to utilize the model to generate graphical honey passwords. Their empirical findings show that effective password space is as small as 30.58 bits, despite that the theoretical and commonly believed strength is 43 bits.

Davis et al. [21] conducted a user study over 16 weeks where students were asked to use graphical password schemes to access class material. The results of the user study show that users tend to select passwords that can be predictable and successfully guessed by attackers, which is similar to the findings of our study detailed below. Similarly, Dirik et al. [22] reported that users concentrate at certain areas when choosing click-points for PassPoints passwords.

Additionally, Golofit [23] highlights the importance of investigating the human factors of graphical passwords. In particular, he investigated users' selected click-based passwords in terms of the features of images used. The study reports on the features of areas that would be avoided by users such as flat areas and objects with irregular-structures.

Along offensive paths in studying graphical passwords, some researchers have reported success in exploiting hotspots using image processing tools [22, 24, 25]. For example, Thorpe and Oorschot [25] proposed a method to build "human-seeded" dictionary attacks.

4. Experimental Design

The motivation behind this work, is the urgent need to examine the effectiveness of graphical passwords. Effectiveness can refer to different aspects, here we focus on the effectiveness of the password in accomplishing the main goal of authentication which is allowing access to legitimate users only, hence increasing the guessability entropy. In order to examine the security aspects of graphical passwords in general, and guessability in particular, we designed a user study where we recruited 50 participants, we chose a homogenate group of all female university students. Participants we are asked to setup their passwords once at the beginning of the experiment by choosing one click point in 3 images. The images used in the experiment were carefully selected so that they adhere to the recommendations suggested in the literature for click-based passwords. In particular, they have many objects, no much empty spaces and no centric objects or objects with particular importance in the image. The images are shown in Figures 1,2 and 3 below.

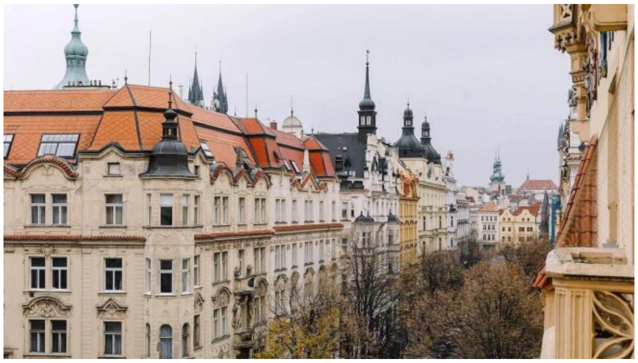

Fig. 1 Image of round (1).

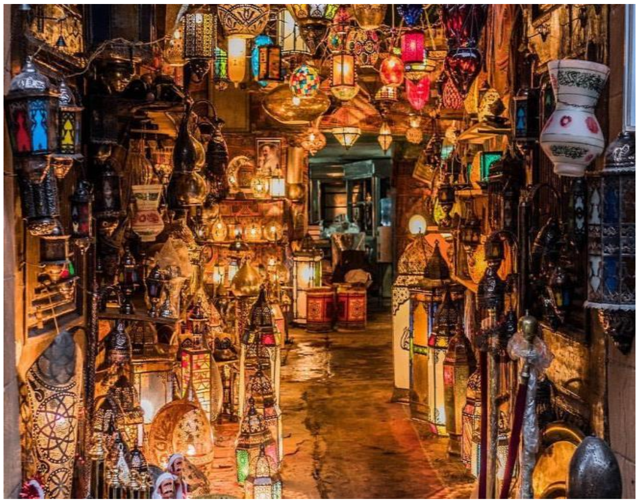

Fig. 2 Image of round (2).

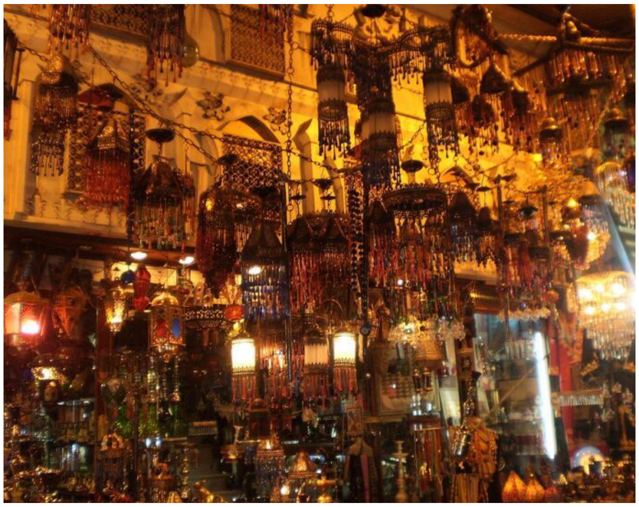

Fig. 3 Image of round (3).

Then, students were asked to participate in two experiments. First, they were asked to recall their own click-points. Secondly, they were asked to try to guess other participants' click-points. Additionally, we utilized a questionnaire to get deeper insights on the reasons behind the observed behaviors.

5. Findings and discussion

The first kind of analysis we did, was regarding the patterns in which the participants chose their click-points. Noticeably, as shown in Figures 4,5 and 6, there was a few hotspots that were selected by many students, the darker or larger the red area is, the higher number of students who chose a click point in the area. An example is the top of the first building in the first images. This leads us to argue that the practical password space of click-based passwords is not as high as its theoretical space. making the need to use persuasive methods urgent. A human analysis of these hotspots show that participants tend to chose objects with clear edges, bright spots in dark areas or dark spots in bright areas, fancy color areas, and central objects.

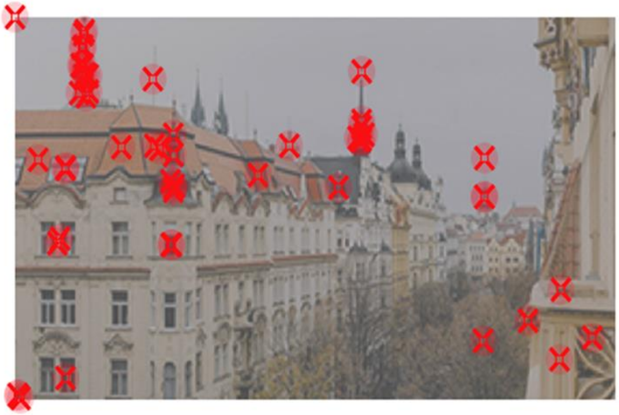

Fig. 4 Hotspot analysis for image (1)

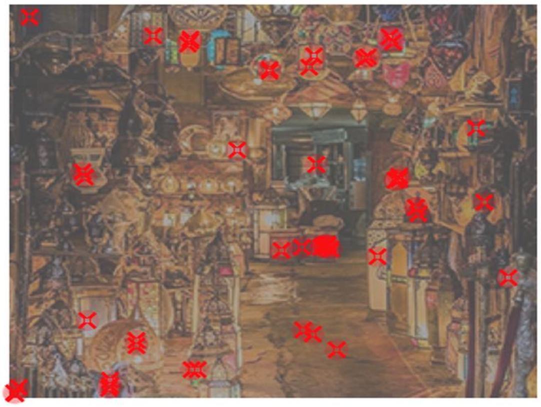

Fig. 5 Hotspot analysis for image (2)

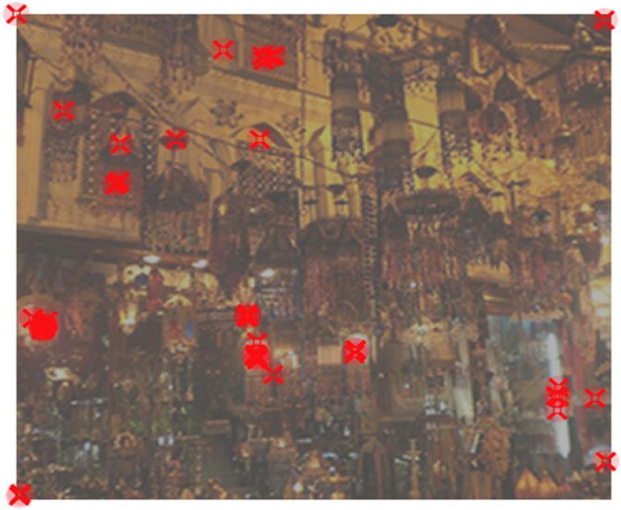

Fig. 6 Hotspot analysis for image (3)

During the questionnaire, participants reported that the main reasons for their choices were: easy recall on their side (70%) and hard guessability on attackers' side (30%). Moreover, some of them reported that some click points were more attractive and eyecatchers compared to other parts of the image while some participants reported that they have no particular reasons for their choice. This leads us to argue that psychological examination of users' behaviors is needed, preferably in multidisciplinary studies.

Additionally, we analyzed how often participants could guess the click-points of other participants and found out that 27%. Of guessing attempts were successful. However, no successful guessing attempts were made through the three images in sequence. Hence, we argue that increasing the number of rounds in click-based passwords is recommend for higher security.

Along similar lines, we observed how often users can guess their peers' passwords after allowing them to observe each other's passwords. Without doubt, the percentage increased to 82% successful guesses. We argue that decreasing the tolerance space of the click-points increase the security of click-based passwords.

6. Conclusion and future work

Graphical passwords date back to 1996 [1]. Nowadays, they exist in various deployment schemes in real world applications. They have been categorized into: recall-based, recognition-based and cue-recall passwords. Despite the difficulty of conducting user studies, there is a great need to use this type of examination to improve our understanding of both the theoretical and practical aspects of graphical passwords In this paper, we presented our findings are related insights of conducting a user study to examine different security aspects of graphical passwords, in particular the guessability issue.

Further research present here can go in two directions: defensive or offensive research paths. The former improves procedures for securing users using graphical passwords along with service providers relying on this technology. This may go in different directions such as providing better theoretical backing, improving measurement procedures for security metrics and suggesting stronger graphical passwords for more usable and secure authentication solutions. These can be oriented either manually or automatically. Automatic-oriented methods include the use of the-state-of-the-art machine learning algorithms for predicting hotspots, recurring sufficient training data. In addition, random suggestions of click-points can be compared to user-selected points in terms of effectiveness. The offensive path can suggest methods for cracking passwords with no much human effort.

References

[1] R. Biddle, S. Chiasson, and P. van Oorschot, 2012. “Graphical passwords: Learning from the first twelve years,” ACM Computing Surveys, 44(4), 41 pages.

[2] D. Klein, “Foiling the cracker: A survey of, and improvements to, password security,” in Proceedings of the 2nd USENIX Security Workshop, Portland, Oregon, August 27, 1990, pp. 5-14.

[3] K. Gilhooly, “Biometrics: Getting Back to Business”, in Computerworld, May 2005.

[4] V. Zimmermann and N. Gerber, "The password is dead, long live the password – A laboratory study on user perceptions of authentication schemes," International Journal of Human-Computer Studies, vol. 133, 2020, pp. 26-44.

[5] Bower, G. H., Karlin, M. B., & Dueck, A. (1975). Comprehension and Memory for Pictures. Memory and Cognition, 2, 216-220.

[6] Calkins, M. W. (1898) Short studies in Memory and Association from the Wellesley College Laboratory. Psychological Review, 5, 451-462.

[7] Paivio, A., Rogers, T. B., & Smythe, P. C. (1968) Why Are Pictures Easier to Recall Than Words? Psychonomic Science, 11, 137-138.

[8] Shepard, R. N. (1967). Recognition Memory for Words, Sentences, and Pictures. Journal of Verbal Learnings and Verbal Behavior, 6, 156-163.

[9] Khosla, A., Xiao, J., Torralba, A., and Oliva, A. 2012. Memorability of image regions. In Advances in Neural Information Processing Systems, 305-313.

[10] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Basic results. In 11th International Conference on Human-Computer Interaction (HCI International), July 2005.

[11] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies, 63(1-2):102–127, 2005.

[12] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In 1st Symposium on Usable Privacy and Security (SOUPS), July 2005.

[13] Burr, W. E., Dodson, D. F., & Polk, W. T. 2004. Electronic authentication guideline, 800-63. US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

[14] Gong, L., Lomas, M. A., Needham, R. M., & Saltzer, J. H. 1993. Protecting poorly chosen secrets from guessing attacks. IEEE journal on Selected Areas in Communications, 11(5), 648-656.

[15] Adams, C. 2011. Dictionary Attack. In Encyclopedia of Cryptography and Security, H. C. A. van Tilborg and S. Jajodia, Eds. Springer, New York, Dordrecht, Heidelberg, London, 332-332.

[16] Pinkas, P., and Sander, T. 2002. Securing passwords against dictionary attacks. In Proceedings of the 9th ACM conference on Computer and communications security (CCS '02), Vijay Atluri (Ed.). ACM, NY, USA, 161-170.

[17] C. Katsini, M. Belk, C. Fidas, N. Avouris, and G. Samaras, “Security and usability in knowledge-based user authentication: A review,” in Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI ’16), ACM, New York, NY, USA, 2016, pages 63:1–63:6.

[18] M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi. Towards identifying usability and security features of graphical password in knowledge based authentication technique. In Second Asia International Conf. on Modelling & Simulation, pages 396–403. IEEE, 2008.

[19] K. Renaud. Evaluating authentication mechanisms. In L. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pages 103–128. O’Reilly Media, 2005.

[20] B. Zhu, J. Yan, D. Wei and M. Yang “Security Analyses of Click-based Graphical Passwords via Image Point Memorability”, in CCS '14: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security November 2014 Pages 1217–1231.

[21] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, 2004.

[22] Dirik, A., Memon, N., and Birget, J. 2007. Modeling user choice in the PassPoints graphical password scheme. In Proc. Symp. on Usable Privacy and Security (SOUPS’07).

[23] Golofit, K. 2007. Click passwords under investigation. In 12th European Symposium on Research in Computer Security (ESORICS’07). LNCS vol. 4734 (Sept. 2007).

[24] A. Salehi-Abari, J. Thorpe, and P. van Oorschot. On purely automated attacks and click-based graphical passwords. In Annual Computer Security Applications Conf. (ACSAC), 2008.

[25] J. Thorpe and P. C. van Oorschot. Human-seeded attacks and exploiting hot-spots in graphical passwords. In 16th USENIX Security Symposium, August 2007.