Balancing Usability and Security of Graphical Passwords

Kristina Lapin(✉) and Manfredas Šiurkus

Vilnius University, Vilnius, Lithuania
kristina.lapin@mif.vu.lt, manfredas.siurkus@mif.stud.vu.lt

Abstract. Although most widely used authentication involves characters as passwords, but secure text-based passwords are complex and difficult to remember. Users want to have easy to remember passwords, but these are vulnerable to various kinds of attacks and are predictable. To address these problems, graphical passwords that involve selection of images and drawing lines have been proposed. The encoded images support creation of secure passwords and facilitate their memorability. Thus, they are considered as an alternative to strengthen password security while preserving usability because secure textual passwords become more complicated to use. The research addresses the issue of improving the user experiences during graphical authentication. This paper examines cued recall-based, pure recall-based and recognition-based approaches. The proposed scheme is based on recognition-based scheme that is selected as the least vulnerable to various attacks. The solution is currently under development, two qualitative usability testing sessions are performed and the participants' feedback is discussed.

Keywords: Graphical authentication · Recognition-based schemes · Recall-based schemes · Cued recall-based schemes

1 Introduction

A good password needs to be easy to remember and hard to guess [1]. These are contradictory requirements that encourage research on balancing security and usability of the user authentication. Textual passwords still dominate over the other methods of end-user web authentication in web applications due to their simplicity and affordability [2]. Typical authentication includes an email address and a secret alphanumeric text-based password that is cost-effective in implementation and familiar to users. However, this scheme requires significant mental effort when the user follows all security conventions for secure password creation and further usage. Saltzer and Schroeder identify the psychological acceptability as important design principle that ensures effective security [6]. There are many examples of the fact that overly complex security systems actually reduce effective security [7].

Graphical passwords are a type of knowledge-based authentication that attempt to leverage the human memory for visual information with the shared secret being related to or composed of images or sketches [3, 4]. They offer a good alternative to text-based passwords in terms of memorability and security [5]. Discussion on authentication

C. Biele et al. (Eds.): MIDI 2021, LNNS 440, pp. 153–160, 2022.
https://doi.org/10.1007/978-3-031-11432-8_15

schemes produced alternative methods, but a comparison of their security and usability attributes does not show better results comparing with widely used textual password schemes [2].

We focus on the graphical recognition-based approaches as they are aimed at strengthening security and enhancing usability. The goal of this paper is to enhance recognition-based technique that will reduce their main drawback, namely the possibility of shoulder surfing attack while preserving the high security.

This paper examines known issues of existing authentication methods and propose the preliminary solution. This paper is structured as follows. Section 2 deals with the graphical authentication schemes that are classified according to required mental efforts and actions. Section 3 describes the proposed enhancement and findings of the first qualitative studies. Finally, the conclusions are drawn.

2 Related Works

The users create textual passwords using words because want easy to rememberable secrets. Such passwords are vulnerable to dictionary attacks [9]. Exploration of a person's social information reveals their relative names that makes possible social engineering attacks [10–12].

The idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images or sketches [4]. The recognized drawback of graphical passwords is shoulder surfing when someone captures the password while watching over the user's shoulder during the entering [1, 13]. There are many attempts to overcome this challenge.

Graphical passwords are classified according the required mental efforts or metrics based on user actions. Classification based on mental efforts comprises recognition-, recall- and cued recall-based approaches [4, 13].

Cued-recall approach involves images to create an association with words that facilitate creation of a stronger textual password. An example of this approach is InkBlot authentication [14] where the user has to associate the randomly looking images with memorable textual character or pair of them. Associations support the creation of strong textual random character password. Observation of the shown images does not help the attacker because the association outcome cannot be observed. As all textual passwords, the InkBlot secret string can be cracked using keystroke logger. From the memorability perspective, the advantage is that such a scheme facilitates memorability of complex password elements. However, the users can still forget more sophisticated password creation rules because the users may not necessarily select the first letter of the associated word and link it to security word. This may result with difficulties recalling the password elements [15]. All in all, cued-recall schemes are better than textual passwords because of their resilience to brute force and dictionary attacks and partially facilitated memorability. However, the security problem remains with keystroke logging; usability drawback can occur when the user uses a sophisticated password creation rule.

Popular examples of recall-based approaches are Draw-A-Secret (DAS) [16] and PassGo [17] authentication methods where the latter can be viewed as a discretized version of the DAS [16]. The user draws a continuous stroke or several strokes on chosen elements of the grid or set of points. According to involved user actions this approach is classified also as a draw-metric authentication scheme [18]. The strokes are graphical, therefore easy to memorize. However, a study on widely used variation of DAS – the Android pattern lock – revealed that users are inclined to draw simple pictures, such as “L”; as a result users get weak passwords [19]. Also, input pattern is susceptible to guessing [20], shoulder surfing [1, 13], smudge[21], thermal [22] and video-based [23] attacks. An interesting improvement to these challenges is proposed in behavioral pattern lock approach [24] in which the users do not need to create their own pattern and memorize them. Instead, during the login, the public patterns are shown along with guidance on how to draw them. This approach acquires touch dynamics from the touch screen and sensors, extracts useful features that classify users using machine learning.

Pure recognition-based approaches present set of pictures. The users are expected to recognize the secret pictures, selected during the registration. Popular examples are Passfaces [25] and Déjà vu [26]. Passfaces exploit the human brain’s ability to quickly recognize familiar faces, Déjà vu is based on the ability to remember previously seen images [13]. During login the user points the password image in several rounds, therefore, these schemes are also classified as loci-metric or click-based graphical password schemes [18].

Generally, recognition-based schemes are resilient to most of known attacks, but the shoulder surfing [2]. Passfaces can also be predictable because the attractiveness, gender and race of faces can affect the user’s choice [20]. Convex Hull Click (CHC) [1] scheme guards against shoulder-surfing attacks by human observation, video recording, or electronic capture. Similar to Passfaces, CHC requires several rounds of challenge-response authentication. In CHC the pass-icons serve as the points, and the edges are lines visualized in the user’s mind. To respond to the challenge, the user clicks anywhere within the convex hull. This is a difference with Passfaces because during CHC login the user never points directly the password icons. However, the rearrangement of the login screen, finding the pass-icons, forming the mental convex in mind requires time and mental efforts. Summarizing, advantages of recognition-based schemes are based on easier recognition of the password. However, most recognition-based schemes are vulnerable to shoulder surfing, in some cases to guessing. Although CHC scheme makes unable observation and guessing, it requires significant time and mental effort.

All graphical authentication schemes facilitate the memorability in various ways. Cued recall-based approaches involve images that help to remember the complex and unguessable textual password, but finally the user enters the textual password. Therefore, the problems with keystroke logging and memorability still remain. Recall-based schemes also support memorability but they are more vulnerable to the attacks comparing to recognition-based approaches (Table 1). Recall-based schemes require to draw the same pattern, so it can be observed, recorded and used in attacks. Recognition-based schemes involve clicking on recognized images, but each time images are presented in different positions. Therefore, the potential attack can be only shoulder surfing. Guessing occurs only for faces.

Table 1. Comparison of the graphical authentication schemes.

Scheme	User actions	Security drawbacks
Recall-based	Clicking on an image points in determined order	Shoulder surfing, guessing, smudge, thermal and video-based attacks
Cued-recall	Images associations facilitate remembering the complex textual password	Keystroke logging, memorability
Recognition-based	Selection of image or face from the provided set	Shoulder surfing, guessing (in special conditions)

In conclusion, the safest graphical passwords belong to a recognition-based group. Therefore, we further examine the way to refine their security and usability.

3 Proposed Graphical Password

Our goal is to propose improvement of the recognition-based schemes, such as Passfaces that are vulnerable to guessing and shoulder surfing attack. Our idea is to combine positive aspects of recognition-based schemes to avoid guessing and to minimize opportunities to observe it. Passfaces scheme is vulnerable to guessing because of the user's preferences to choose faces of a particular race, gender and attractiveness. Déjà vu passwords involve randomly generated images. We suggest to use gallery of photos that do not contain faces and are not randomly generated. Our assumption is that photos can be more pleasurable to use and easier to recognize comparing with randomly generated images.

Known recognition-based schemes make several image recognition rounds to strengthen security. However, this prolongs the logging and increases efforts required to authenticate. When authentication is frequently needed, it can irritate the user and discourage from using a service. To minimize the number of selection rounds we suggest to present photos on the one screen and ask the user to tap on password images. After each tap the images are reordered. This protects from shoulder surfing because while tapping the image is covered with the finger; after the operation the other image is shown on the tapped place. Because images are rearranged after each selection, the same image can be tapped several times.

To enhance security, the number of shown images can be increased. By tapping on the image, the associated complex textual string that fit security requirements is entered. The encoding of photos can be easy to figure out by trying several different passwords. Therefore, to further improve the security of this solution, the use of password hashing is proposed. This prevents the data leakage from the password database at hacking.

The registration scenario involves choosing the images that should be recognized during the login. The user enters a login name and chooses at least three images from the interactive photo gallery during registration (Fig. 1). The order of selections is also fixed. To confirm the registration the user repeats the choice of images with the same order. It is allowed to enter only two identical photos from the required at least three. During the login the user enters login name and selects the images in the same order.

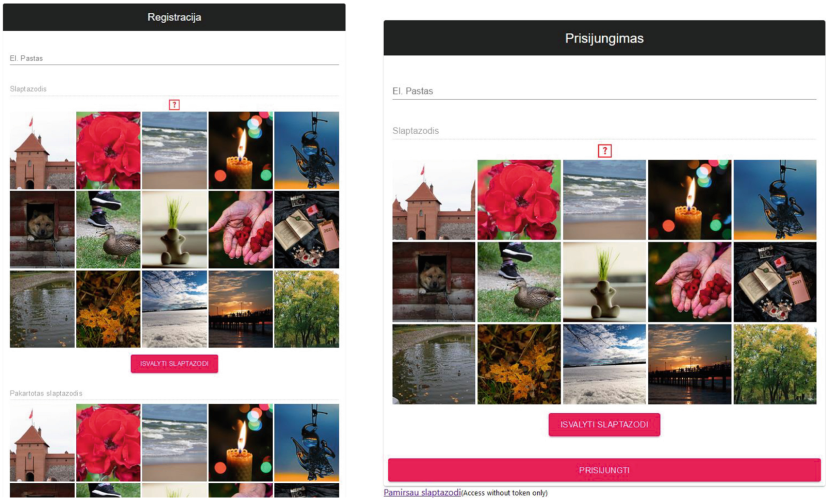

Fig. 1. The registration window asks two times to select pictures in the same order (on the left) and login interface (on the right)

At login, password photos are encrypted. Each photo corresponds to 5 characters, the password contains numbers, uppercase and lowercase letters, and characters not described in the alphabet. During the registration, the user is asked to select at least 3 photos that generate a 15-character password that is considered safe to brute force attacks [27, 28]. The implemented solution also uses cryptography, the password is encrypted using the Bcrypt library before an account is created.

If the user forgets a secret, the new password can be set using the user's e-mail. This solves the problem when a user forgot password or when the account is locked after too many incorrect attempts to log on to the system.

We conducted usability testing with 5 participants aged 20 to 58 years with various IT usage experience levels. The goal of qualitative study was to collect their opinions about how easy is to memorize the photos selected during the registration and to select them while logging. Initially, the users were exposed with a prototype that contained 30 photos. This number did not fit on the screen, so the screen had to be scrolled. Testers complained that it was difficult to find the photo after each tap. They were distracted and get confused if they didn't find the right photo on the initial screen and had to scroll.

On the second session the number of photos was reduced to fit the space above the page fold. We found that no more than 20 photos should be shown. With a larger gallery, you should consider the size of the photos to make sure they fit on the high definition screens. The photos should be reduced or enlarged according to the screen resolution. This redesign presented better results comparing to the initial version.

Testing participants requested to provide feedback while selecting an image. However, marking selected password photos is not secure because of possibility to observe.

Instead of marking the selected image, we suggest to provide the number of already selected photos. Moreover, the explanation of registration and logging procedure should be provided for the new users.

4 Conclusions

Comparison of the graphical authentication methods revealed that recognition-based approaches are the least vulnerable to attacks. This work aimed at providing a more efficient way of ensuring security while not scarifying usability. Our focus was to improve the recognition-based approach that is based on the brain's natural ability to recognize visual information. The developed scheme does not involve human faces, thus protecting against the threat of password prediction. Shoulder surfing chances are reduced due to rearrangements of the photo gallery after each selection. The user opinions during the testing revealed that this authentication is easily learned and requires an acceptable amount of efforts during registration and further authentication.

The usability and security of this scheme directly depend from the number of photos and selection rounds. The proposed scheme requires to choose at least 3 photos. This minimal case forms a 15-character length string that fits the security requirements.

The further usability studies are needed to conduct quantitative research that would allow to compare the efficiency of registration and logging with existing recognition-based methods.

References

1. Wiedenbeck, S., Waters, J., Sobrado, L., Birget, J.-C.: Design and evaluation of a shoulder-surfing resistant graphical password scheme. In: Proceedings of the working conference on Advanced visual interfaces, pp. 177–184. Association for Computing Machinery, New York (2006). https://doi.org/10.1145/1133265.1133303
2. Bonneau, J., Herley, C., van Oorschot, P.C., Stajano, F.: The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, pp. 553–567. IEEE (2012). https://doi.org/10.1109/SP.2012.44
3. Nelson, D.L., Reed, V.S., Walling, J.R.: Pictorial superiority effect. J. Exp. Psychol. Hum. Learn. Mem. **2**, 523–528 (1976). https://doi.org/10.1037/0278-7393.2.5.523
4. Biddle, R., Chiasson, S., Van Oorschot, P.C.: Graphical passwords: learning from the first twelve years. ACM Comput. Surv. (CSUR). **44**, 1–41 (2012)
5. Kayem, A.V.D.M.: Graphical passwords – a discussion. In: 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 596–600 (2016). https://doi.org/10.1109/WAINA.2016.31
6. Saltzer, J.H., Schroeder, M.D.: The protection of information in computer systems. Proc. IEEE **63**, 1278–1308 (1975). https://doi.org/10.1109/PROC.1975.9939
7. Dourish, P., Redmiles, D.: An approach to usable security based on event monitoring and visualization. In: Proceedings of the 2002 Workshop on New Security Paradigms, pp. 75–81. Association for Computing Machinery, New York (2002). https://doi.org/10.1145/844102.844116
8. Platt, D.: The Joy of UX: User Experience and Interactive Design for Developers. Addison-Wesley Professional, Boston (2016)

9. Morris, R., Thompson, K.: Password security: a case history. Commun. ACM. **22**, 594–597 (1979). https://doi.org/10.1145/359168.359172
10. Ramanan, S., Bindhu, J.S.: A survey on different graphical password authentication techniques. Int. J. Innov. Res. Comput. Commun. Eng. **2**(12), 7594–7602 (2014)
11. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. J. Inf. Secur. Appl. **22**, 113–122 (2015). https://doi.org/10.1016/j.jisa.2014.09.005
12. Yıldırım, M., Mackie, I.: Encouraging users to improve password security and memorability. Int. J. Inf. Secur. **18**(6), 741–759 (2019). https://doi.org/10.1007/s10207-019-00429-y
13. Sarohi, H.K., Khan, F.U.: Graphical password authentication schemes: current status and key issues. IJCSI **10**, 437 (2013)
14. Stubblefield, A., Simon, D.: Inkblot authentication (2004)
15. Shnain, A.H., Shaheed, S.H.: The use of graphical password to improve authentication problems in e-commerce. In: AIP Conference Proceedings, vol. 2016, p. 020133 (2018). https://doi.org/10.1063/1.5055535
16. Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The design and analysis of graphical passwords. In: Proceedings of the 8th USENIX Security Symposium, Washington, D.C., p. 15 (1999)
17. Tao, H.: Pass-Go, a new graphical password scheme (2006)
18. Sharma, A., Dembla, D., Shekhar: Implementation of advanced authentication system using opencv by capturing motion images. In: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 759–765 (2017). https://doi.org/10.1109/ICACCI.2017.8125933
19. Andriotis, P., Tryfonas, T., Oikonomou, G.: Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 115–126. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07620-1_11
20. Davis, D., Monrose, F., Reiter, M.K.: On user choice in graphical password schemes. In: Proceedings of the 13th USENIX Security Symposium, San Diego, CA (2004)
21. Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M.: Smudge attacks on smartphone touch screens. In: Proceedings of USENIX Conference on Offensive Technology (WOOT), pp. 1–7 (2010)
22. Abdelrahman, Y., Khamis, M., Schneegass, S., Alt, F.: Stay cool! Understanding thermal attacks on mobile-based user authentication. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pp. 3751–3763. Association for Computing Machinery, New York (2017)
23. Ye, G., et al.: Cracking android pattern lock in five attempts. In: Proceedings of the 2017 Network and Distributed System Security Symposium 2017 (NDSS 2017). Internet Society, San Diego, California, USA (2017)
24. Ku, Y., Park, L.H., Shin, S., Kwon, T.: Draw it as shown: behavioral pattern lock for mobile user authentication. IEEE Access **7**, 69363–69378 (2019). https://doi.org/10.1109/ACCESS.2019.2918647
25. Two Factor Authentication, Graphical Passwords - Passfaces
26. Dhamija, R., Perrig, A.: Déjà Vu: A User Study Using Images for Authentication. Presented at the (2000)
27. Komanduri, S., et al.: Of passwords and people: measuring the effect of password-composition policies. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2595–2604. Association for Computing Machinery, New York (2011)
28. Kelley, P.G., et al.: Guess again (and again and again): measuring password strength by simulating password-cracking algorithms. In: 2012 IEEE Symposium on Security and Privacy, pp. 523–537 (2012). https://doi.org/10.1109/SP.2012.38