Investigating the Use of Gesture-Based Passwords by the Seniors

Lakshmidevi Sreeramareddy(✉), Pewu Mulbah, and Jinjuan Heidi Feng

Department of Computer and Information Sciences, Towson University, Towson, MD 21252, USA
{lsreeramareddy,jfeng}@towson.edu,
pmulba1@students.towson.edu

Abstract. Older adults in the US are the fastest-growing demographic group, and also the fastest-growing group of internet users [1]. Many computer related tasks, such as user authentication, could be a challenge for the seniors as their cognitive and physical capabilities decline. To date, the most commonly used authentication method is alphanumeric passwords, which have substantial challenges regarding security and usability [2]. Authentication using traditional alphanumeric passwords can be particularly problematic for the seniors because secure passwords are usually hard to remember [3]. Therefore, due to memory loss, one common problem associated with aging, the traditional alphanumeric passwords could be challenging for the seniors to recall and manage. To address this challenge, we developed a gesture-based password application as an alternative to the traditional alphanumeric passwords [4]. Preliminary studies suggest that users could learn the new password method in fairly short amount of time [5]. In this paper, we report an empirical user study to investigate how the seniors interact with the gesture password application.

Keywords: Usable security and privacy · User security and privacy by design · Accessibility

1 Introduction

User authentication is a crucial area for data security. Numerous authentication techniques have been developed to fit the needs of users in different contexts. The most commonly used authentication method is the alphanumeric password. However, since strong alphanumeric passwords are hard to remember, users tend to choose easy to remember passwords that are vulnerable to dictionary attacks. We developed an alternative gesture-based password method in order to address some of the challenges of the alphanumeric passwords [4]. The motivation behind this method is that people can remember pictures better than text and for longer duration of time [6]. Therefore, gesture-based passwords may require less memory capability than the alphanumeric passwords.

Older adults in the US are the fastest-growing demographic group [1]. As people age, the cognitive capability of the human brain declines, making it harder to remember

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 107–118, 2015.
DOI: 10.1007/978-3-319-20376-8_10

and manage the traditional alphanumeric passwords. The gesture-based password may benefit seniors because of its pictorial representation of the password. However, to date, there has been limited research that investigated the usability of different types of passwords as used by the senior. In this paper, we report a user study that evaluated the use of gesture-based passwords by the seniors. In particular, we investigated how the seniors interact with the proposed gesture-based password method, the variations in the behavioral measures while drawing the password, and whether there is any difference in the interaction patterns between the seniors and young users.

2 Related Research

Alphanumeric passwords are the most commonly adopted method for authenticating users online. However, stronger alphanumeric passwords may cause usability problems. Thus, users tend to pick easy to remember passwords that are vulnerable to dictionary attacks [7, 8]. To address the limitations of the alphanumeric passwords, researchers have developed various forms of graphical passwords as alternative authentication methods [6, 9–11]. Research shows that users can remember graphical passwords better than alphanumeric passwords [12]. The limitation of some graphical passwords is that the password space is limited, making the password vulnerable to brute-force attack. Another limitation of graphical passwords is that they are more susceptible for shoulder-surfing attacks than the alphanumeric passwords [13]. More recently, shoulder-surfing defense techniques have been developed and could be adapted to prevent this attack [14].

Graphical passwords can be grouped into two types: recognition-based and recall-based. When using recognition-based passwords, user clicks on regions of a picture or select set of pictures in sequence. Then the system recognizes the selection to authenticate the user. When using recall-based passwords, user draws the password using the memory recall ability. The gesture-based password reported in this paper belongs to the recall-based password group. This method is similar to Draw-A-Secrete (DAS) [9] method developed by Jermyn et al. The DAS method requires the password to cross a sequence of grids to authenticate a user. Nail et al. [15] studied the usability of the DAS method and reported that almost 29 % of password were invalid.

The Passdoodles [16] and gesture-based touch pad system [17] are also recall-based passwords. These methods used password shape, speed of strokes and pauses between strokes in order to authenticate users. Neither method was systematically evaluated through empirical user studies. Furthermore, De Luca et al. [17] and Sae-Bae et al. [18] used specific features of passwords such as pressure, speed, and fingertip dynamics as an additional layer of authentication. Both methods require pre-defined shapes as password. Users must pick their password from system provided catalog of passwords.

Our proposed method differs from existing gesture-based methods [e.g., 6–10] in two perspectives. First, it is grid free, meaning that the drawing area has no grid. Users can freely draw on the canvas provided without any specific limitations. Second, users do not need to use predefined shapes provided by the system. The password content (drawing) is exclusively based on users' imagination.

The number of older adults using technology is growing rapidly [19]. As people age, the biological framework of health would become less efficient [20]. There are chances of declined recall ability. Since complex passwords are hard to remember, seniors tend to use weak passwords for online activities [21]. Those passwords are highly vulnerable for security attacks. Therefore, the seniors would benefit from alternative authentication solutions are easy to remember and, in the meanwhile, offer acceptable security protection.

3 Application Design

The password creation interface is demonstrated in Fig. 1. Once a password is created, we use the $N recognizer algorithm to determine how similar the newly entered password is to the original password [22]. During the authentication stage, in addition to the similarity between the password images, we also consider behavioral measures including drawing speed, pause between strokes, stroke length, password size, and movement angles, to enhance the authentication. The behavioral measures may reflect how well users remember the password and how easy it is to draw the password.

Fig. 1. Demonstration of the password creation interface

4 Participants

Twenty three senior participants took part in the study. Nine participants were females and 14 were males. The average age of the participants was 71, ranging between 65 and 81 (SD. = 4.99). Twenty two young participants took part in the study. Among the 22 participants, 12 were females and 10 were males. The average age of the young participants was 28, ranging between 21 and 38 (SD. = 4.30). All participants have previous experience using computers and the Web. All participants have Web accounts and are familiar with the traditional password authentication process.

5 Task and Procedure

A between-subject design was adopted in this study. Participants in both age groups created and re-entered passwords using a mouse. At the beginning of the study, a researcher explained and demonstrated the gesture-based passwords to the participants. The participants first tried to create one password and re-enter it multiple times. Then they started the formal session and created 6 gesture-based passwords and re-entered each password five times. The application interface used in the study for two groups of users is exactly the same. At the end of the study, participants completed a paper-based demographic questionnaire and a satisfaction survey.

6 Results

According to observation of the researchers and the satisfaction survey, all participants easily mastered the gesture-based authentication method and can comfortably draw the password.

6.1 Password Content

Participants created a total of 270 (138 from the senior group, 132 from the young group) different passwords. The researchers analyzed the password images that the participants created. The content of the passwords varies dramatically and covers a broad spectrum. The percentage of major categories of password content for two user groups are summarized in Table 1. Young users drew more (8 % more vs. seniors) accessories and electronic objects than the seniors. This may be due to the fact that young users use more electronic devices (such as smartphones, iPads or music players) on a daily basis than the seniors. Young users drew more (19 % more vs. seniors) mathematical shapes than the seniors. Interestingly, the seniors drew more human faces and emotions (9 % more vs. young) than the young users.

Among the 270 passwords, 241 (89 %) were drawings of objects or concept or sceneries. Only 29 (11 %) were based on English letters or words, which has positive security implications. Table 2 shows the sample passwords created by the seniors.

6.2 Accuracy of Password Re-Entry

The confidence score (CS) measures the accuracy of the re-entry compared to the original drawing. The CS is calculated by the $N recognizer algorithm and ranges between zero and one. The distribution of the confidence scores for the reproduced passwords entered by both groups are illustrated in Fig. 2. The confidence scores of more than 69 % of the passwords reproduced by both groups are higher than 0.8. 90 % of the passwords reproduced by both groups had confidence scores higher than 0.7. These preliminary results suggest that the participants could reproduce the password with considerable level of accuracy.

Table 1. Categories of password content from young/seniors groups

Category	Seniors (%)	Young (%)
Vegetables, fruits and other food	4.35	5.30
Trees, flowers and other plants	1.45	9.85
Animals	5.07	5.30
Human faces and emotions	19.57	10.61
Buildings	2.17	3.79
Scenery	6.52	6.06
Vehicles	2.17	6.82
Mathematical shapes	13.04	32.58
Numbers	2.90	4.55
Kitchen tools	5.80	1.52
Accessories or electronics or house tools	3.62	11.36
English words or letters	15.42	7.58
Other objects	37.68	42.42

6.3 Comparison Between Seniors and Young Users

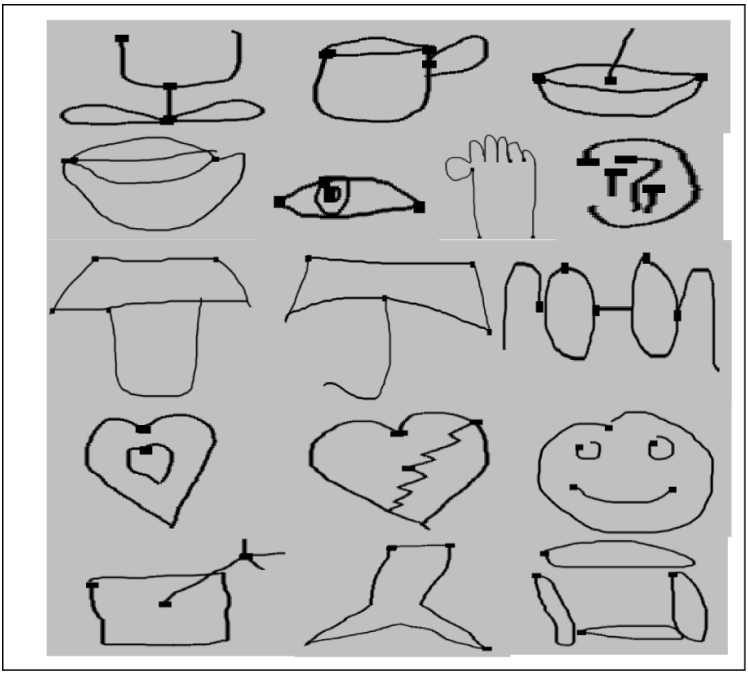
One-way Repeated Measures Analysis of Variance (ANOVA) tests were used to compare the performance measures between the two groups of users.

Confidence Score. As discussed in the previous section, the accuracy of password re-entry is obtained from confidence scores (CS). The test result suggests that there is significant difference between the confidence scores of the passwords entered by the two groups of users ($F(1, 43) = 8.16$, $p < 0.007$). The passwords re-entered by senior users have significantly higher confidence score than passwords re-entered by young users (Fig. 3). This may be due to the fact that the seniors perceive security or password more cautiously than the young group. Since they are more cautious, they might pay more attention to the task and re-enter the password more accurately than the young group.

Time to Create and Re-Enter Password. An ANOVA test was conducted using two groups of users as independent variables and the password creation time and re-entry time as the dependent variables. The test result suggests that there is significant difference between the creation time of the passwords by the two groups of users ($F(1, 43) = 13.84$, $p < 0.002$). The passwords created by senior users have significantly longer

creation time (M = 23.52 s, SD = 13.37) than passwords created by young users (M = 12.64 s, SD = 8.10) (Fig. 4). The re-entry time of passwords have no significant difference between the two groups of users (F (1, 43) = 1.61, n.s; mean 22.49 for seniors, 13.81 s for young).

Table 2. Sample passwords created by seniors



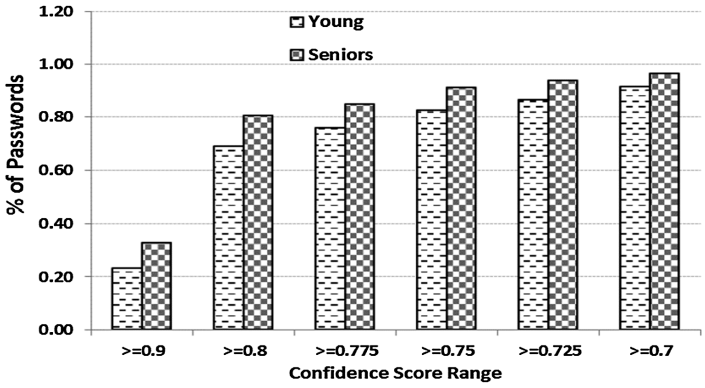


Fig. 2. Distribution of conference scores under young/seniors

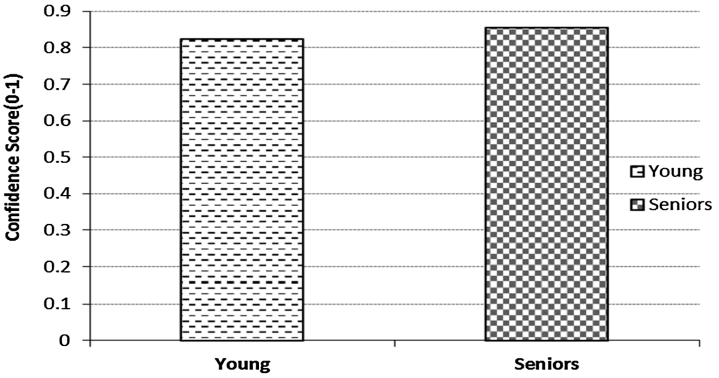


Fig. 3. Confidence score between two groups (number 0–1) young/seniors

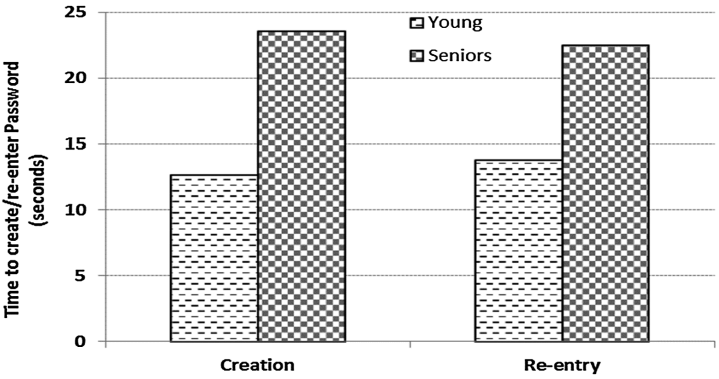


Fig. 4. Average time spent to create or re-enter passwords (seconds) young/seniors

Pauses in Creation and Re-Entry. The test result suggests that there is significant difference between the two groups of users in the pauses between strokes while creating passwords ($F(1, 43) = 24.13$, $p < 0.000$). The passwords created by senior users have significantly lower percentage of pauses ($M = 29.83$ percent, $SD = 4.47$) than passwords created by young users ($M = 40.07$ percent, $SD = 8.88$). The pauses during password re-entry also have significant difference between the two groups of users ($F(1, 43) = 46.44$, $p < 0.000$). The passwords re-entered by senior users have significantly lower percentage of pauses ($M = 25.72$ percent, $SD = 5.58$) than passwords re-entered by young users ($M = 39.08$ percent, $SD = 7.46$) (Fig. 5). Since the seniors spent a longer time during creation and similar amount of time during re-entry, the result suggests that the seniors spent most of the time drawing the strokes rather than recalling the strokes.

Length of Strokes. The test result suggests that there is significant difference in the length of the strokes between the two groups of users ($F(1, 43) = 6.39$, $p < 0.01$). The strokes drawn by seniors users have significantly short length ($M = 664.10$ pixels, $SD = 270.85$) than the strokes drawn by young users ($M = 875.74$ pixels, $SD = 290.51$).

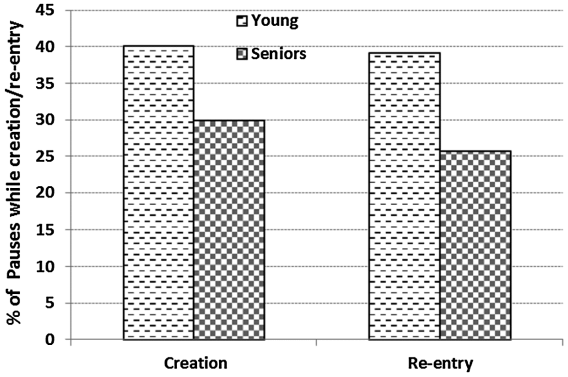


Fig. 5. Percentage of pauses during creation and re-entry for young/seniors

The length of strokes drawn during re-entry also have significant differences between the two groups of users ($F(1, 43) = 8.86$, $p < 0.005$). The passwords re-entered by seniors users have significantly short strokes ($M = 641.20$ pixels, $SD = 260.36$) than passwords re-entered by young users ($M = 894.72$ pixels, $SD = 309.58$) (Fig. 6).

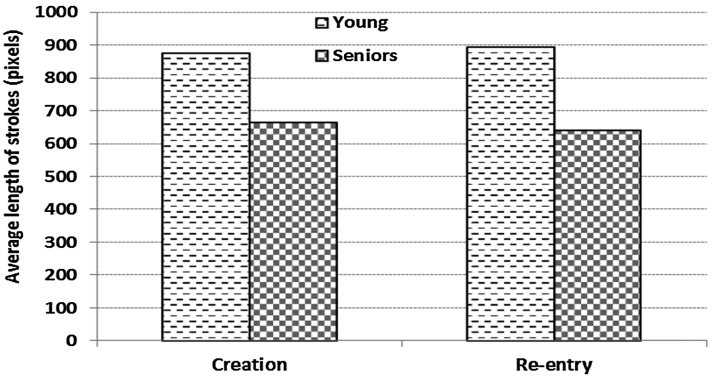


Fig. 6. Average length of strokes during creation and re-entry (pixels) for young/seniors

Password Size. The test result suggests that there is significant difference between the two user groups in the size of the passwords created ($F(1, 43) = 7.05$, $p < 0.01$). The passwords created by seniors users have significantly smaller size ($M = 2084.1.10$ pixels, $SD = 14879.76$) than passwords created by young users ($M = 35811.14$ pixels, $SD = 22353.22$). The size of password during re-entry also has significant differences between the two groups of users ($F(1, 43) = 8.24$, $p < 0.006$). The passwords re-entered by senior users have significantly smaller size ($M = 19979.84$ pixels, $SD = 14012.17$) than passwords re-entered by young users ($M = 38168.45$ pixels, $SD = 26803.85$) (Fig. 7).

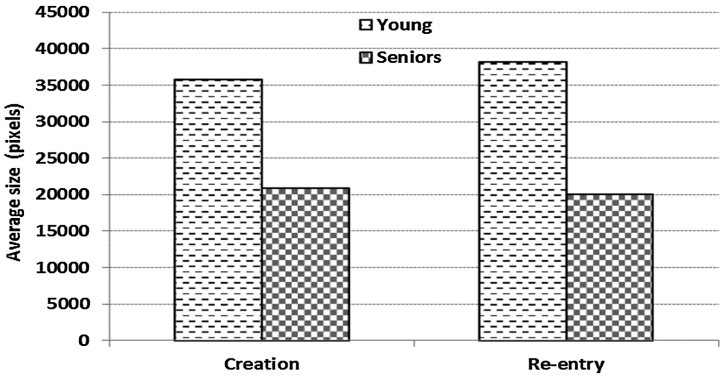


Fig. 7. Average size during creation and re-entry (bounding box pixels) for young/seniors

Drawing Speed. The test result suggests that, there is significant difference in the drawing speed between the two groups of users ($F(1, 43) = 21.69$, $p < 0.000$). The passwords created by seniors users have significantly lower speed ($M = 0.42$ number of pixels per milliseconds, $SD = 0.27$) than passwords created by young users ($M = 1.02$ number of pixels per milliseconds, $SD = 0.55$). The speed of password during re-entry also have significant difference between the two groups of users ($F(1, 43) = 29.76$, $p < 0.000$). The passwords re-entered by seniors users have significantly lower speed ($M = 0.50$ number of pixels per milliseconds, $SD = 0.28$) than passwords re-entered by young users ($M = 1.20$ number of pixels per milliseconds, $SD = 0.54$) (Fig. 8). This result is consistent with the fact that the seniors spent a longer time drawing the strokes.

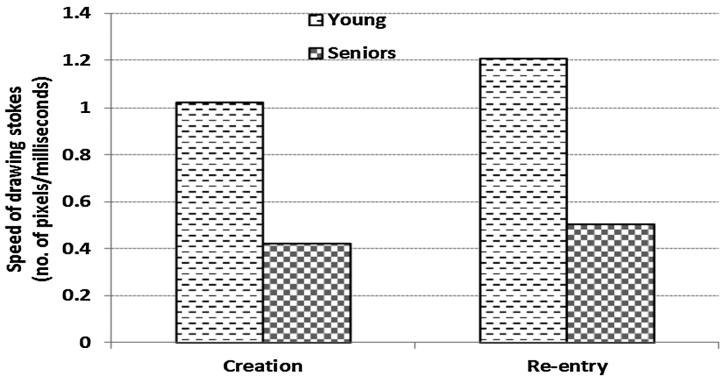


Fig. 8. Average drawing speed of creation and re-entry (number of pixels per milliseconds) for young/seniors.

Number of Strokes in Password. An ANOVA test result suggests that there is no significant difference in the password stroke count between the two groups of users ($F(1, 43) = 0.93$, $p < 0.33$, n.s.; 4.34 stokes for seniors, mean 4.4 strokes for young). The stroke count of password during re-entry also has no significant difference between

the two groups of users ($F(1, 43) = 0.36$, $p < 0.54$, n.s.; 4.32 strokes for seniors, mean 4.37 stokes for young).

7 Discussions and Future Work

This study is a preliminary investigation on how gesture-based passwords are used by the seniors. The study provides initial insight about how the senior users construct the passwords and what types of concepts or objects they might use in their passwords. The collection of passwords that participants created helps us understand the actual password space. Encouragingly, the content of the passwords seems to be quite diversified. Seniors drew a higher percentage (19.57 %) of human faces and emotions than young users (10.61 %). Seniors drew a lower percentage (13.04 %) of mathematical shapes than young users (32.58 %). Seniors also drew a lower percentage (3.62 %) of electronics or house tools compared to young users (11.36 %). The influence of the traditional alpha-numeric passwords seems to be limited as suggested by the low percentage of passwords based on letters and numbers (18 % for the seniors, 12 % for the young users).

The results demonstrate that there are differences in a number of performance measures between young and senior participants when creating and entering gesture-based passwords. Interestingly, senior users re-entered gesture-based passwords with higher accuracy than young users. The senior participants who spent longer time while creating the gesture-based passwords had significantly lower percentage of pauses when re-enter passwords. It seems that the seniors had easier and smoother transition between strokes, as indicated by the dramatically lower percentage of time pausing between strokes during the re-entries. The senior participants also drew shorter strokes at lower speed than young users. These results suggest that the proposed gesture-based password method has the potential to be adopted by seniors. The difference in behavior measures provides insights to modify the current design to accommodate to the special needs of senior users.

Longitudinal studies are planned to investigate the memorability of the gesture passwords over a long period of time. Studies are needed to investigate how to modify the design of gesture-based password application to better fit the interaction style of senior users. It will also be interesting to examine how the proposed method works with real-life applications such as Email, Facebook, or E-commerce sites.

8 Conclusion

As the confidence scores demonstrate, senior participants were able to reproduce the passwords with accuracy. The content of the passwords drawn is diversified, which has positive implications for security. The seniors and young users also demonstrated different interaction patterns when using the gesture-based passwords. The differences in the performance data between the young and the seniors are very interesting. The seniors preferred passwords with shorter length, the re-entries resulted in higher accuracy, and the passwords have lower percentage of pauses compared to the young users. This research suggests that the gesture-based password method might serve as an alternative authentication solution for seniors.

References

1. Hart, T.A., Chaparro, B.S., Halcomb, C.G.: Evaluating websites for older adults: adherence to 'senior-friendly' guidelines and end-user performance. Behav. Inf. Technol. **27**, 191–199 (2008)
2. Biddle, R., Chiasson, S., Van Oorschot, P.C.: Graphical passwords: learning from the first twelve years. ACM Comput. Surv. **44**(4), 1–41 (2012)
3. Renaud, K., Ramsay, J.: Now what was that password again? a more flexible way of identifying and authenticating our seniors. Behav. Inf. Technol. **26**(4), 309–322 (2007)
4. Sreeramareddy, L., Feng, J., Sears, A.: Poster: preliminary investigation of gesture-based password: integrating additional user behavioral features. In: Symposium on Usable Privacy and Security (SOUPS), pp. 4–5 (2012)
5. Sreeramareddy, L., Janprasert, A., Heidifeng, J.: Evaluating gesture-based password and impact of input devices. In: The International Conference on Security and Management (2014)
6. Gao, H., Guo, X., Chen, X., Wang, L., Liu, X.: YAGP: yet another graphical password strategy. In: 2008 Annual Computer Security. Applications Conference, pp. 121–129 (2008)
7. Adams, A.: Users are not the enemy. Commun. ACM **42**(12), 40–46 (1999)
8. Abdullah, M.D.H., Abdullah, A.H., Ithnin, N., Mammi, H.K.: Towards identifying usability and security features of graphical password in knowledge based authentication technique. In: 2008 Second Asia International Conference Modeling and Simulation, pp. 396–403 (2008)
9. Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The design and analysis of graphical passwords. In: Proceedings of 8th USENIX Security Symposium, pp. 1–4 (1999)
10. Weiss, R., De Luca, A.: PassShapes - Utilizing Stroke Based Authentication to Increase Password Memorability, pp. 18–22 (2008)
11. Owen, G.S.: Graphical passwords: a survey. In: 21st Annu. Computer Security Applications Conference, (ACSAC), pp. 463–472 (2005)
12. Brostoff, S., Sasse, M.A.: Are passfaces more usable than passwords? a field trial investigation. In: McDonald, S., Waern, Y., Cockton, G. (eds.) People and Computers XIV — Usability or Else!: Proceedings of HCI 2000, pp. 405–424. Springer, Heidelberg (2000)
13. Lashkari, A.H., Farmand, S., Zakaria, O.B., Saleh, R.: Shoulder surfing attack in graphical password authentication. Int. J. Comput. Sci. Inf. Secur. IJCSIS **6**(2), 145–154 (2009)
14. Zakaria, N.H., Griffiths, D., Brostoff, S., Yan, J.: Shoulder surfing defence for recall-based graphical passwords. In: Proceedings of Seventh Symposium Usable Privacy and Security - SOUPS 2011, p. 1 (2011)
15. Nali, D., Thorpe, J.: Analyzing user choice in graphical passwords. School of Computer Science, Carleton University Technical report TR-04-01, pp. 1–6 (2004)
16. Varenhorst, C.: Passdoodles: a lightweight authentication method. MIT Res. Sci. Inst. (2004)
17. DeLuca, A., Hang, A., Brudy, F., Lindner, C., Hussmann, H.: Touch me once and i know it' s you! implicit authentication based on touch screen patterns. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 987–996 (2012)
18. Sae-Bae, N., Ahmed, K., Isbister, K., Memon, N.: Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 977–986 (2012)
19. Czaja, S.J., Lee, C.C.: The impact of aging on access to technology. Univers. Access Inf. Soc. **5**(4), 341–349 (2007)
20. Age Related Cognitive Decline. Life Extension Foundation for Long lIfe. http://www.lef.org/Protocols/Neurological/Age-Related-Cognitive-Decline/Page-01

21. CareMonitor, L.: Online Password Security Tips for Seniors, Senior Tech Daily. http://seniortechdaily.com/online-password-security-tips-for-seniors/
22. Anthony, L., Wobbrock, J.O.: A lightweight multistroke recognizer for user interface prototypes. In: Human- Computer Interaction Institute, Carnegie Mellon University (2012)