

Original Research Paper

BlindLogin: A Graphical Authentication System with Support for Blind and Visually Impaired Users on Smartphones

Yean Li Ho, Bachir Bendrissou, Afizan Azman and Siong Hoe Lau

Faculty of Information Science and Technology (FIST), Multimedia University (MMU), Melaka, Malaysia

Article history

Received: 07-12-2016

Revised: 03-05-2017

Accepted: 11-05-2017

Corresponding Author:

Yean Li Ho

Faculty of Information Science
and Technology (FIST),
Multimedia University (MMU),
Melaka, Malaysia

Email: ylho@mmu.edu.my

Abstract: Most graphical password systems on smart phones do not consider the needs of blind and visually impaired users. The main objective of this paper is to propose a new graphical authentication system which combines the usability of the graphical password with the security of the textual password and allows all types of users, including the blind and visually impaired users to use the same authentication system on a smartphone without any extra costs for special hardware. 84.6% of those surveyed would recommend BlindLogin to their friends. 46.2% of the respondents also found the BlindLogin password to be easier to remember than the regular textual password. BlindLogin is a viable alternative as a universal graphical password authentication system.

Keywords: Authentication, Blind, Graphical Passwords, Human Computer Interaction Security, Usability-Deployability-Security Model, Visually Impaired

Introduction

Authentication systems are basically categorized into three types: Knowledge-based (something you know), token-based (something you own) and biometric-based (something you are). Of the three, knowledge-based authentication systems are the most frequently used and the most common knowledge-based authentication system is the textual password. However, in 1996, a new branch of knowledge-based passwords known as graphical passwords were introduced by Blonder (1996). Thorpe and van Oorschot (2004) states that people have better recall for objects, followed by pictures and finally words.

Narender *et al.* (2010) noted that textual passwords which are long and randomly formed are hard to remember. Therefore, users go around this situation by choosing simple easy to remember and insecure words like names and dictionary words or write down their passwords on sticky notes and place them in an easily accessible location like on the computer monitor. Graphical passwords are more suitable for keyboard less systems like smartphones and can be used to overcome weaknesses of textual passwords like brute-force attacks and key-logging attacks (Kimwele *et al.*, 2009).

To date, there are more than 90 different types of graphical passwords and they can be broadly categorized as Recognition-based graphical passwords, Recall-based graphical passwords, Recognition-Recall based hybrid

passwords and Textual-Graphical hybrid passwords (Ho *et al.*, 2015). Recognition-based graphical passwords are also known as Searchmetric or Cognometric passwords. Recall-based graphical passwords can be subcategorized as Cued Recall (Iconmetric) Passwords and Pure Recall (Drawmetric) passwords, Cued Recall (Iconmetric) passwords can be subcategorized as Locimetric and Psychometric passwords. The detailed taxonomy and references for all these graphical password systems can be found in Ho *et al.* (2015).

So far, all these systems do not consider the needs of blind and visually impaired users. For a system to be truly usable, the system must be able to be used universally by all kinds of users regardless of their background and accessibility capabilities. Our proposal is to introduce a graphical password system which is almost as secure as the regular textual password system but is more usable than the existing graphical password systems in a sense that it will be usable to blind and visually impaired users as well as regular sighted users.

According to Boyd *et al.* (1990), blind activists have raised the issue that screen readers are not equipped to meet the rapid changes of modern GUI interfaces for the sighted community as most software applications have been designed for the sighted community without considering the needs of the blind and visually-impaired communities (Edwards *et al.*, 1994; Griffeth, 1996). The virtual keyboards on smartphones are not practical for blind and visually-impaired users as they require

accuracy and point relocation while entering a character (Yfantidis, 2005). Furthermore, most smartphones in the market do not support braille and special hardware is needed to support braille on a smartphone. To reduce costs, a more universal method of input is needed to allow both the sighted and visually-impaired or blind users to enter their passwords on the same interface as the rest of the world. This would contribute towards integrating the visually impaired to regular society so they will not feel so left-out and left-behind.

The objectives of this project is to propose a new graphical authentication system which is more usable to include blind and visually-impaired users and secure compared to existing ones and to implement and evaluate the proposed system using the UDS model. This paper is the initial pilot study.

Related Work

Grussenmeyer and Folmer (2017) did a comprehensive survey on touchscreen technologies for the visually impaired. Several virtual keyboard interfaces have been proposed to support both the blind or visually-impaired users as well as sighted users.

Venolia and Neiberg (1994) introduced the T-Cube, a virtual keyboard which contains pie menus in eight directions. This was followed by Cirrin which was introduced by Mankoff and Abowd (1998). Cirrin consists of a circular keyboard with alphabets arranged by simulated annealing and is controlled by a unigesture selection. Unigesture was introduced by Sazawal *et al.* (2002). This method requires the user to tilt the screen in any of the seven directions and return the screen to the center in order to select an alphabet in that area. There are two types of layouts: Clustered layout and spread-out layout. Nesbat (2003) introduced MessageEase. This method requires a user to tap the button which contains the group of characters with the required character followed by the neighbouring button in the direction of the required character. Both Jhaveri (2003) and Isokoski (2004) introduced a similar type of virtual keyboard. The 2CPS-TWO characters Per Stroke (Jhaveri, 2003) or also known as the Menu Augmented Soft Keyboard (Isokoski, 2004), is a Qwerty keyboard with a submenu with the most frequently used characters.

Perlin (2005) proposed Quickwriting where the user selects a character by using a stylus to drag towards the zone contain a group of characters with the desired character. There are four menus: lowercase, capital, punctuation and numeric. Sánchez and Aguayo (2006) proposed a virtual keyboard for mobile messenger with support for the blind and Yfantidis and Evreinov (2006) proposed an adaptive blind interaction technique for touchscreens. In Virtual Keyboard for Mobile Messenger for the Blind (Sánchez and Aguayo, 2006), a character is selected by pressing a button several times until the

desired character is selected. In Adaptive blind interaction technique touchscreens (Yfantidis and Evreinov, 2006), the three menus are displayed in sequence after an interval and a character is selected by touching the screen in a circular motion and lifting the finger at the desired character. Guerreiro *et al.* (2008) introduced NavTap and NavTouch (Guerreiro *et al.*, 2009) while Lucas *et al.* (2010) introduced another variation of the method called NavTilt.

Bonner *et al.* (2010) proposed No-Look Notes (Fig. 1) which contains a pie menu with groups of alphabets and a submenu with three characters. Li *et al.* (2011) proposed a 1 Line keyboard which contains the sequence of a Qwerty keyboard in a single line of keys. Azenkot *et al.* (2012a) introduced PassChords, a multi-touch authentication system for the blind. It is based on finger taps. Oulasvirta *et al.* (2013) proposed a two thumb mobile touchscreen layout which splits the keyboard into two parts, called KALQ. MTITK (Buzzi *et al.*, 2014) uses the normal layout of a numeric keypad with multitouch, speech, vibrations and audio to represent and select characters.

Alnfai and Sampalli (2016) tabled a summary of Braille keyboard features. Jayant *et al.*, 2010; Mascetti *et al.*, 2011; Azenkot *et al.*, 2012b; Southern *et al.*, 2012; Xiong and Sanford, 2013; Façanha *et al.*, 2014; Šepić *et al.*, 2015; Alnfai and Sampalli, 2016) proposed virtual keyboards based on the six dot Braille layout. Mattheiss *et al.* (2015) introduced an 8 dot Braille layout which includes special characters. Jayant *et al.* (2010) divides the screen into 6 areas to represent the 6 dots of the Braille alphabet and uses different haptic vibrations to differentiate between the areas tapped. Mascetti *et al.* (2011) introduced TypeInBraille which detects braille characters by touching the correct dot sequence in a series of six dots (2 columns by 3 rows). Azenkot *et al.* (2012a) proposed Perkinput which is a Braille based virtual keyboard which uses the Input Finger Detection (IFD) technology to detect the position of fingers touching the screen following the sequence found in a Perkins Braille machine. Southern *et al.* (2012) introduced Braille Touch, Xiong and Sanford (2013) introduced SlideType and Façanha *et al.* (2014) proposed LeBraille (which contains raised buttons), which support the Braille six dots layout. Šepić *et al.* (2015) proposed BrailleEasy, a one-handed Braille keyboard. Alnfai and Sampalli (2016) proposed the SingleTapBraille keyboard. It accepts single-handed taps according to the sequence of Braille dots anywhere on the screen. The system will evaluate the relationship between the dots and read out the character using Text-To-Speech software.

Proposed Solution

Among all the graphical password systems surveyed, there is almost no support at all for blind and visually impaired users. In fact, most software are designed for sighted users and require visually impaired users to

adjust to the interface which is not friendly to blind users (Edwards *et al.*, 1994; Griffeth, 1996). According to Yfantidis (2005), most virtual keyboards are not useful to the blind and visually impaired because they require accuracy and point relocation to enter each character.

We propose BlindLogin (Fig. 2), a reasonably secure graphical password system which is universally more usable because it supports the blind and visually impaired users as it works well with TalkBack, an Accessibility software option in the Android smartphone. As touchscreens in mobile phones lack the tactile feedback most blind users are used to (Oliveira *et al.*, 2011), BlindLogin supports both haptic and sound tactons as secondary feedback cues for the blind and visually impaired when logging into the system. These tactons aid new users to reduce errors and help the new users to memorize the layout and features of the new system (Yfantidis and Evreinov, 2006). The visually impaired user can then use the features of a black screen and maneuver according to the location. Pie menus are better than linear menus (Callahan *et al.*, 1988) because users have a tendency to remember angle directions easier than serial positions found in normal pull down menus (Yfantidis, 2005). This system is an improved version of No-Look-Notes (Bonner *et al.*, 2010). Blind users are used to the clock interface because learning is frequently done based on the clock face like the order of food located on a plate. Therefore, the clock face is a common way for blind users to understand space and to locate objects (Kamel and Landay, 2002). The RBS (2005) also advises people to use the clock face in order to communicate directions to blind people. Kane *et al.* (2011) also discovered that the visually impaired preferred using corners and edges of the touch screen as a guideline in navigating to specific locations.

The graphics are categorized in the first screen according to groups like fruits, toys, sports, clothes, masonry, military, gardening tools and plumbing tools to aid the sighted and visually impaired to remember their chosen password. The graphics are chosen according to categories in order to aid memorization of the graphical password. Each category is different from the other so that the user can remember his or her graphical password by creating a story to remember the sequence of pictures. When a visually impaired user using TalkBack and headphones selects a category, the system vibrates and reads out the group of alphabets, number and symbol related to it as well as the category label when the blind user slides his finger over each button. Once the user enters the category by double tapping the chosen category, another menu appears with five characters or objects to choose from.

The user can navigate around the screen and each button will vibrate and with Talkback enabled, the system will also pronounce that character and the type of object. Then, the user can select the desired character or object by double tapping the character. The user can repeat this as many times as he or she desires to form a more secure password.

There is also a navigation menu which contains four options: “delete the last character”, “submit”, “delete all” and “type again and exit”. This system however, can also be silent when Talkback is disabled to facilitate its use by sighted users. So, the system is supported by Talkback only for the visually-impaired and blind users. The colorful objects can help the partially blind in selecting and recognizing objects better. This system is very versatile because it gives the user the option of remembering their password based on based on graphical objects, alphanumeric characters, clockface location (Kamel and Landay, 2002; RBS, 2005) or corners and edges (Kane *et al.*, 2011) so it is more user-friendly and usable by all types of users regardless of their visual capabilities.

The password which is keyed in, is hashed with MD5 hash algorithm. The stored password would produce a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. The character set consists of 40 characters in total (26 lowercase letters +10 digits +4 special characters).

The recommended minimum password length in the app is 10 characters or 10 objects. The password space is $40^{10} = 10485760000000000$ combinations. The probability of guessing the password correctly is:

$$\left(\frac{1}{40}\right)^{10} = 9.537 \times 10^{-17}$$

A dictionary attack and a brute force attack were done on the system to test the security of a 10 character or 10 object password using this system. The dictionary attack was attempted with a weak password using the UNIQPASS wordlist of 2,151,220 unique ASCII passwords. This method works only with relatively weak passwords, passwords that consist of common, meaningful words or names or letters or a combination of them. It takes about 5 min and 11 sec to test a password against all entries of the wordlist. However, we also use the mangling rules where for every word in the dictionary, 50 other words are derived. In this case, the time necessary to exhaust all possible words is roughly 51 times, which is about 4 h 24 min and 21 sec. The benchmarking test using John the Ripper for the brute force attack yielded the system cracking capacity, which is 6900 combinations per second. Given the password complexity, we can calculate how many combinations are needed to be tried in order to crack a password. The minimum password length is 10 and the charset is 40 characters. Therefore, $40^{10} = 10485760000000000$ combinations. Therefore, the amount of time needed to brute-force a password using this system is:

$$\frac{10485760000000000 \text{ combinations}}{6900 \frac{\text{combinations}}{\text{second}}} = 1519675362318.84 \text{ seconds} \\ = 48188.59 \text{ years}$$

Table 1. Summary of results according to the UDS model

	UDS criteria	Better than textual password	Neutral	Worse than textual password
Usability	Memorywise-effortless	46.20%	30.80%	23.10%
	Scalable-for-users	30.80%	38.50%	30.50%
	Nothing-to-carry	Nothing to carry -84.6%		
Deployability		Need to carry many things-15.4%		
	Physically-effortless	46.20%	23.10%	30.80%
	Easy-to-learn	30.80%	30.80%	38.50%
	Efficient-to-use	46.20%	38.50%	15.40%
	Infrequent-errors	15.40%	30.80%	53.90%
	Easy-recovery-from-loss	15.40%	38.50%	46.20%
	Accessible	15.40%	53.80%	30.80%
	Negligible-cost-per-user	30.80%	53.80%	15.40%
	Server-compatible	38.50%	46.20%	15.40%
	Browser-compatible	38.50%	46.20%	15.40%
Security	Mature	15.40%	0%	84.60%
	Non-proprietary	84.60%	0%	15.40%
	Resilient-to physical-observation	53.90%	15.40%	30.80%
	Resilient-to-targeted-impersonation	53.90%	23.10%	23.10%
	Resilient-to-throttled-guessing	46.20%	46.2	7.70%
	Resilient-to-unthrottled-guessing	38.50%	7.70%	53.90%
	Resilient-to-internal-observation	38.50%	46.20%	15.40%
	Resilient-to-leaks-from-other-verifiers	30.80%	61.50%	7.70%
	Resilient-to-phishing	61.60%	23.10%	15.40%
	Resilient-to-theft	53.90%	23.10%	23.10%
	No-trusted-third-party	No trusted third party -69.2%		
		trusted third party required -30.8%		
		Yes	Don't know	No
	Requiring-explicit-consent	76.90%	7.70%	15.40%
	Unlinkable	53.80%	15.40%	30.80%

Evaluation

A pilot test user study of 25 questions was conducted on 13 blind and visually impaired users with various levels of visual impairment (61.5% totally blind and 38.5% partially blind) between the ages of 29-68 (84.6% male and 15.4% female) based on the Usability-Deployability-Security (UDS) Model proposed by Bonneau *et al.* (2012). Table 1 above shows a summary of results obtained according to the UDS Model.

Discussion

About 38.5% felt that the system was not so easy to learn and 53.9% made quite a number of errors because the system was new to them and they were unfamiliar with it. Each participant took about an average of half an hour to undergo training and was allowed to only try the system once during the training. In addition, 46.20% felt that their graphical password was not easy to recover in the case of a loss because the system did not have any provision for lost passwords as yet. The majority (53.8%) felt unsure if the system is accessible or not because they do not have much experience using it. However, 46.2% felt that the proposed system was easy to use (memorywise-effortless and physically-effortless) and efficient to use.

According to the results of the survey, the majority also felt that the proposed system is generally secure. Generally, most of the users were unsure of the deploy

ability of the graphical system because they are not very savvy with computers. About 84.6% were unfamiliar with the system and felt that the system is not mature yet because it is new and they did not have any experience using this proposed system. However, about 84.6% felt that the system should be non-proprietary and available for free to everyone.

The survey was done on each criteria based on a Likert scale with 1 being "Easier than textual Passwords", 3 being the "Same as textual passwords" and 5 being "Harder than textual passwords". A summary of some of the results are shown in Fig. 3.

From the usability standpoint, most of the respondents (84.6%) would recommend BlindLogin to their friends. 46.2% of the respondents also found the BlindLogin password to be easier to remember than the regular textual password. All of the respondents felt that the time taken for authentication and setting up of a BlindLogin password was short (less than 5 minutes). As for the security perspective, most of the respondents (53.9%) felt that it was much harder to guess the BlindLogin password if you have the knowledge and personal details of the user as compared to the traditional textual password. About 46.2% felt that it is harder to guess the BlindLogin password if the number of guesses is limited and 61.6% felt that it would be harder to get the Blindlogin password by pretending to be a trustworthy website as compared to the traditional textual password.

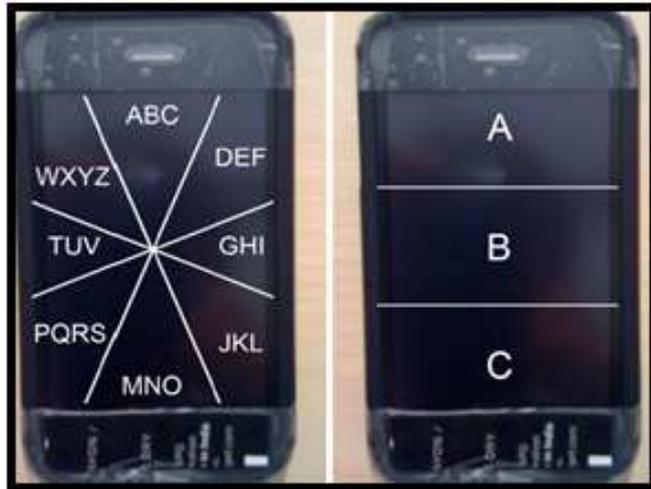


Fig. 1. No-look notes (Bonner *et al.*, 2010)

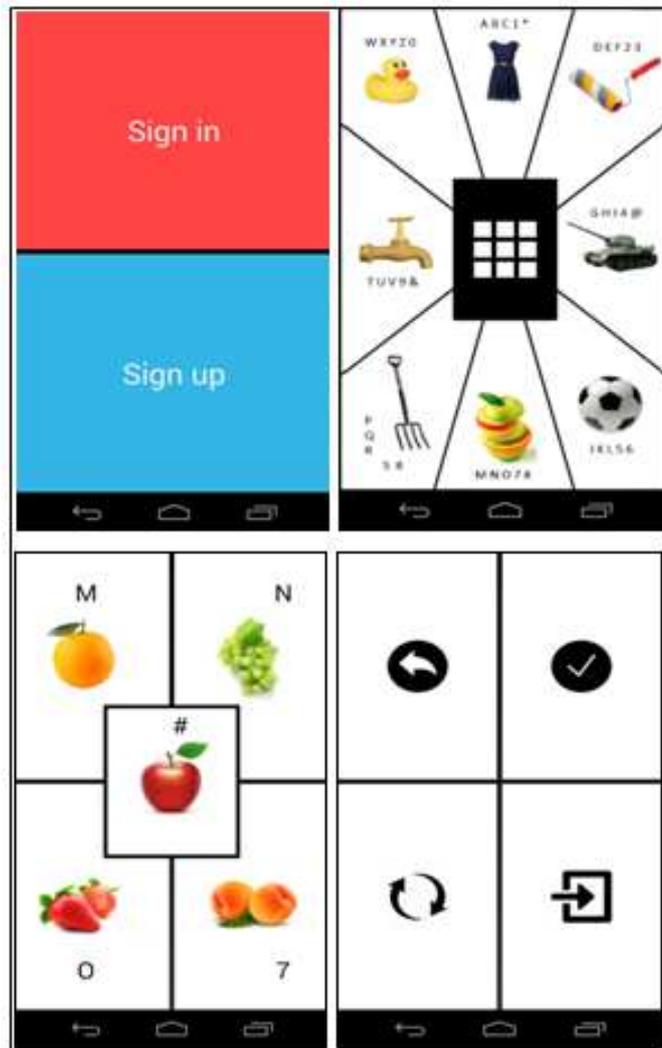
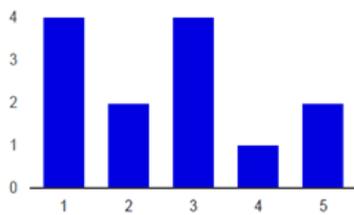
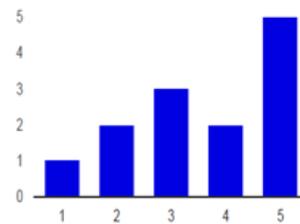


Fig. 2. BlindLogin interfaces

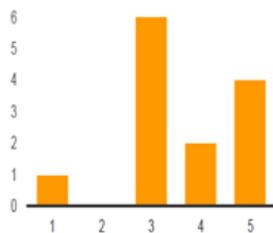
Remembering your BlindLogin password



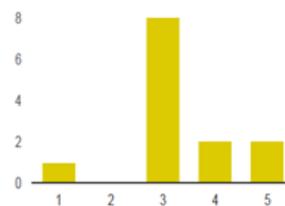
Ability to guess a BlindLogin password if you have the knowledge and personal details of the user?



Ability to guess a BlindLogin password if number of guesses is limited?



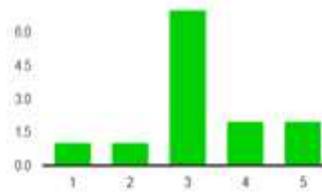
Ability to guess your BlindLogin password on one system if your BlindLogin password on another system is stolen?



Time taken for authentication and setting up of a BlindLogin password is



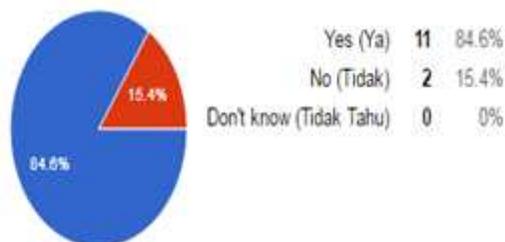
Using BlindLogin with disabilities or other physical conditions



Very short (a few seconds) - Sangat pendek (beberapa saat)	Count	Percentage
1	3	23.1%
2	3	23.1%
3	5	38.5%
4	2	15.4%
5	0	0%

Easier than Textual Passwords (Lebih Mudah Daripada Kata Laluan Teks)	Count	Percentage
1	1	7.7%
2	1	7.7%
3	7	53.8%
4	2	15.4%
5	2	15.4%

Do you think it is suitable for BlindLogin to be free to use by anyone?



Would you recommend BlindLogin to your friend?

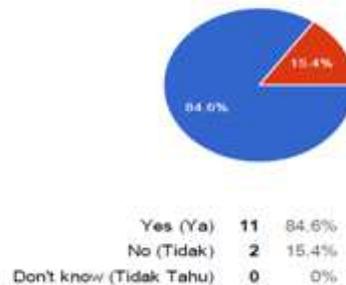


Fig. 3. Summary of selected results from the survey

Conclusion

We introduce BlindLogin as a proof of concept to show that graphical passwords can also be used to support not only sighted users but also the blind and visually impaired users with the aid of screen readers like Talkback as well as haptic feedback like vibrations for every selection. BlindLogin is a viable system to be used as a universal interface for password systems on a mobile platform. Its graphical features enable the user to remember the graphical password better with the creation of a story based on the categories of objects. This feature combined with the clock face location of the graphics, corners and edges makes the system more usable for both sighted users as well as the visually impaired while maintaining the security of the password as described above. The results of the user study shows that the proposed graphical system is generally acceptable to the visually impaired users in terms of usability and security. In terms of deployability, most of the respondents were unsure because they were not computer savvy.

Future Enhancement

Future works will include some modifications to be made to the system based on feedback received from the pilot study and a new more complete study will be carried out with a larger set of respondents to obtain more accurate results. An additional feature to support a black or blank screen when the system is used by the visually impaired will be implemented to improve security of the system for use by the visually-impaired and blind users. Thus the blind and visually impaired users who are familiar with the location of the buttons and objects will be able to use the system without worrying about passers-by observing their input and this will also eliminate the shoulder-surfing problem for the blind and visually impaired users. The blind and visually impaired users can use the additional features of Talkback to accompany the system with headphones in order to receive verbal feedback when using the system. Sighted users however, will not need to use Talkback and this accessibility feature may be disabled for sighted users. Feedback will be collected from the visually impaired, the blind as well as sighted users to obtain more comprehensive results.

Acknowledgement

We would like to acknowledge the Society of the Blind for providing us with test subjects to conduct a user training and user study of the proposed system. We would also like to acknowledge Multimedia University for providing the funding to carry out this study.

Funding Information

This work was supported by Multimedia University Mini Fund [WBS MMUI /150066].

Author's Contributions

Yean Li Ho: The design of BlindLogin, conducted user training and user study and the development, analysis and publication of this manuscript.

Bachir Bendrissou: The development of the BlindLogin app and the security testing of the app.

Afizan Azman: Review of the manuscript critically for significant intellectual content and final approval of the version to be submitted and any revised version.

Siong Hoe Lau: Review of the manuscript critically for significant intellectual content and final approval of the version to be submitted and any revised version.

Ethics

All articles published in this manuscript are written and researched by the Authors, unless otherwise indicated. Any parties intending to quote or include any ideas represented in the articles are welcome by providing appropriate acknowledgment in their reference list.

References

- Alnfai, M. and S. Sampalli, 2016. An evaluation of single tap Braille keyboard: A text entry method that utilizes Braille patterns on touchscreen devices. Proceedings of the 18th International ACM SIGACCESS Conference on Computers and Accessibility, (IASC'16), ACM, New York, pp: 161-169. DOI: 10.1145/2982142.2982161
- Azenkot, S., J.O. Wobbrock, S. Prasain and R.E. Ladner, 2012a. Input finger detection for nonvisual touch screen text entry in Perkinput. Proceedings of the Graphic Interface, May 28-30, Toronto, Ontario, pp: 121-129.
- Azenkot, S., K. Rector, R. Ladner and J. Wobbrock, 2012b. Passchords: Secure multi-touch authentication for blind people. Proceedings of the 14th international ACM SIGACCESS Conference on Computers and Accessibility, Oct. 22-24, Colorado, pp: 159-166. DOI: 10.1145/2384916.2384945
- Blonder, G., 1996. Graphical password. U.S. patent 5,559,961.
- Bonneau, J., C. Herley, P.C. Van Oorschot and F. Stajano, 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. Proceedings of the IEEE Symposium on Security and Privacy, May 20-23, pp: 553-567. DOI: 10.1109/SP.2012.44

- Bonner, M., J. Brudvik, G. Abowd and W.K. Edwards, 2010. No-look notes: C accessible eyes-free multi-touch text entry. Proceedings of the 8th International Conference on Pervasive Computing, May 17-20, Helsinki, Finland pp: 409-426.
DOI: 10.1007/978-3-642-12654-3_24
- Boyd, L.H., W.L. Boyd and G.C. Vanderheiden, 1990. The graphical user interface: Crisis, danger and opportunity. J. Visual Impairment Blindness, 84: 496-502.
- Buzzi, M.C., M. Buzzi, B. Leporini and A. Trujillo, 2014. Designing a text entry multimodal keypad for blind users of touchscreen mobile phones. Proceedings of the 16th International ACM SIGACCESS Conference on Computers and Accessibility, Oct. 20-22, New York, pp: 131-136. DOI: 10.1145/2661334.2661354
- Callahan, J., D. Hopkins, M. Weiser and B. Shneiderman, 1988. An empirical comparison of pie vs. linear menus. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, May 15-19, Washington, D.C., pp: 95-100.
DOI: 10.1145/57167.57182
- Edwards, A., A. Edwards and E. Mynatt, 1994. Enabling technology for users with special needs. Proceedings of the Conference Companion on Human Factors in Computing Systems, Apr. 24-28, Boston, Massachusetts, pp: 405-406.
DOI: 10.1145/259963.260528
- Façanha, A.R., W. Viana, M.C. Pequeno, M.B. Campos and J. Sánchez, 2014. Touchscreen mobile phones virtual keyboarding for people with visual disabilities. Proceedings of the International Conference on Human-Computer Interaction Applications and Services, Jun. 22-27, Springer, Greece, pp: 134-145.
DOI: 10.1007/978-3-319-07227-2_14
- Griffeth, N., 1996. Making a simple interface complex: interactions among telephone features. Proceedings of the Conference on Human Factors in Computing System, Apr. 13-18, Vancouver, British Columbia, pp: 244-245. DOI: 10.1145/257089.257303
- Grussenmeyer, W. and E. Folmer, 2017. Accessible touchscreen technology for people with visual impairments: A survey. J. Tran. Accessible Comput., DOI: 10.1145/3022701
- Guerreiro, T., P. Lagoá, H. Nicolau, D. Gonalves and J.A. Jorge, 2008. From tapping to touching: Making touch screens accessible to blind users. IEEE Mult. Media, 4: 48-50.
- Guerreiro, T., H. Nicolau, J. Jorge and D. Gonçalves, 2009. NavTap: A long term study with excluded blind users. Proceedings of the 11th International ACM SIGACCESS Conference on Computers and Accessibility, Oct. 25-28, ACM, New York, pp: 99-106. DOI: 10.1145/1639642.1639661
- Ho, Y.L., A. Azman and S.H. Lau, 2015. An analysis of graphical user authentication systems. Proceedings of the 9th International Conference on IT in Asia, (CITA '15).
- Isokoski, P., 2004. Performance of menu-augmented soft keyboards. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Apr. 24-29, Vienna, pp: 423-430. DOI: 10.1145/985692.985746
- Jayant, H., C. Acuario, W. Johnson, J. Hollier and R. Ladner, 2010. V-Braille: Haptic Braille perception using a touch-screen and vibration on mobile phones. Proceedings of the 12th International ACM SIGACCESS Conference on Computers and Accessibility, Oct. 25-27, ACM, Orlando, pp: 295-296.
DOI: 10.1145/1878803.1878878
- Jhaveri, N., 2003. Two Characters Per Stroke-a Novel Pen-Based Text Input Technique. In: New Interaction Techniques, Evreinov, G. (Ed.), Department of Computer and Information Sciences, University of Tampere (Report B-2003-5), pp: 10-15.
- Kamel, H.M. and J.A. Landay, 2002. A study of blind drawing practice: Creating graphical information without the visual channel. Proceedings of the 4th International ACM Conference on Assistive Technologies, Nov. 13-15, ACM, New York, pp: 34-41. DOI: 10.1145/354324.354334
- Kane, S.K., J.O. Wobbrock and R.E. Ladner, 2011. Usable gestures for blind people: Understanding preference and performance. Proceedings of the Conference on Human Factors in Computing Systems, May 07-12, New York, pp: 413-422.
DOI: 10.1145/1978942.1979001
- Kimwele, M., W. Mwangi and S. Kimani, 2009. Strengths of a colored graphical password. Int. J. Rev. Comput.
- Li, F.C.Y., R.T. Guy, K. Yatani and K.N. Truong, 2011. The 1line keyboard: A qwerty layout in a single line. Proceedings of the 24th Annual ACM Symposium on User Interface Software and Technology, Oct. 16-19, Santa Barbara, pp: 461-470.
DOI: 10.1145/2047196.2047257
- Lucas, D., H. Nicolau, T. Guerreiro and J.A. Jorge, 2010. NavTilt: Interface gestual para cegos. Proceedings of the 4th National Conference on Human-Computer Interaction, (NCH' 10).
- Mankoff, J. and G.D. Abowd, 1998. Cirrin: A word-level unistroke keyboard for pen input. Proceedings of the 11th Annual ACM Symposium on User Interface Software and Technology, Nov. 01-04, ACM, San Francisco, pp: 213-214. DOI: 10.1145/288392.288611
- Mascetti, S., C. Bernareggi and M. Belotti, 2011. TypeInBraille: A braille-based typing application for touchscreen devices. Proceedings of the 13th International ACM SIGACCESS Conference on Computers and Accessibility, Oct. 24-26, Scotland, pp: 295-296. DOI: 10.1145/2049536.2049614

- Mattheiss, E., G. Regal, J. Schrammel, M. Garschall and M. Tscheligi, 2015. EdgeBraille: Braille-based text input for touch devices. *J. Assistive Technol.*, 9: 147-158.
- Narender, M., M.Y. Babu and M. Mohan Rao, 2010. Towards secure design choices for implementing graphical passwords. Proceedings of the 20th Annual Computer Security Applications Conference, Dec. 6-10, IEEE Xplore Press, pp: 24-27. DOI: 10.1109/CSAC.2004.44
- Nesbat, S.B., 2003. A system for fast, full-text entry for small electronic devices. Proceedings of the International Conference on Multimodal, Nov. 05-07, Vancouver, British Columbia, pp: 4-11. DOI: 10.1145/958432.958437
- Oliveira, J., T. Guerreiro, H. Nicolau, J. Jorge and D. Gonçalves, 2011. BrailleType: Unleashing braille over touch screen mobile phone. Proceedings of the 13th IFIP TC 13 International Conference on Human-Computer Interaction, Sep. 05-09, Lisbon, pp: 100-107.
- Oulasvirta, A., A. Reichel, W. Li, Y. Zhang and M. Bachynskiy *et al.*, 2013. Improving two-thumb text entry on touchscreen devices. Proceedings of the Annual Conference on Human factors in Computing Systems, Apr. 27-May 02, Paris, pp: 2765-2774. DOI: 10.1145/2470654.2481383
- Perlin, K., 2005. Quikwriting: Continuous stylus-based text entry. Proceedings of the 11th Annual ACM Symposium on User Interface Software and Technology, Nov. 01-04, ACM, San Francisco, pp: 215-216. DOI: 10.1145/288392.288613
- RBS, 2005. Royal Blind Society.
- Sánchez, J. and F. Aguayo, 2006. Mobile messenger for the blind. Proceedings of the 9th Conference on User Interfaces for all, Sept. 27-28, Königswinter, pp: 369-385.
- Sazawal, V., R. Want and G. Borriello, 2002. The unigesture approach: One-handed text entry for small devices. Proceedings of the International Conference on Mobile Human-Computer Interaction Mobile, (HCI '02), Pisa, pp: 256-270.
- Šepić, B., A. Ghanem and S. Vogel, 2015. BrailleEasy: One-handed Braille keyboard for Smartphones. *Stud. Health Technol. Inform.*, 217: 1030-1035. PMID: 26294606
- Southern, C., J. Clawson, B. Frey, G. Abowd and M. Romero, 2012. An evaluation of BrailleTouch: Mobile touchscreen text entry for the visually impaired. Proceedings of the 14th International Conference on Human-Computer Interaction with Mobile Devices and Services, Sept. 21-24, San Francisco, pp: 317-326. DOI: 10.1145/2371574.2371623
- Thorpe, J. and P.C. van Oorschot, 2004. Towards secure design choices for implementing graphical passwords. Proceedings of the 20th Annual Computer Security Applications Conference, Dec. 06-10, pp: 50-60. DOI: 10.1109/CSAC.2004.44
- Venolia, D. and F. Neiberg, 1994. T-Cube: A fast, self-disclosing pen-based alphabet. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Apr. 24-28, Boston, pp: 265-270. DOI: 10.1145/191666.191761
- Xiong, X.N. and J.A. Sanford, 2013. Slide type: Universal design text-entry interface for touchscreen devices. Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility, Oct. 21-23, ACM, Bellevue. DOI: 10.1145/2513383.2513429
- Yfantidis, G., 2005. Blind interaction technique for touchscreens "a full keyboard under the fingertip. MSc. Thesis, University of Tampere, Department of Computer Sciences Interactive Technology.
- Yfantidis, G. and G. Evreinov, 2006. Adaptive blind interaction technique for touchscreens. *J. Universal Access Inf. Soc.*, 4: 328-337. DOI: 10.1007/s10209-004-0109-7