User Preferences and Situational Needs of Mobile User Authentication Methods

Kanlun Wang
Department of Business Information Systems and Operations Management
UNC Charlotte
Charlotte, USA
kwang17@uncc.edu

Lina Zhou
Department of Business Information Systems and Operations Management
UNC Charlotte
Charlotte, USA
lzhou8@uncc.edu

Dongsong Zhang
Department of Business Information Systems and Operations Management
UNC Charlotte
Charlotte, USA
dzhang15@uncc.edu

Abstract **— As it becomes commonplace to use mobile devices to store personal and sensitive data, mobile user authentication (MUA) methods have witnessed significant advancement to improve data and device security. On the other hand, traditional MUA methods such as password (or passcode) are still being widely deployed. Despite the growing body of knowledge on technical strengths and security vulnerabilities of various MUA methods, the perception of mobile users may be different, which can play a decisive role in MUA adoption. Additionally, user preferences for MUA methods may be subject to the influence of their demographic factors and device types. Furthermore, the pervasive use of mobile devices has generated many situations that create new usability and security needs of MUA methods such as support of one-handed and/or sight-free interaction. This study investigates user perception and situational needs of MUA methods using a survey questionnaire. The research findings can guide the design and selection of MUA methods.**

Keywords — Mobile user authentication; security; user perception; situational needs; one-handed authentication; sight-free authentication

I. Introduction

Mobile handheld devices such as smartphones and tablets are increasingly used to support personal tasks such as communication, online banking, shopping, stock trading, and bill payment as well as work-related activities. As a result, personally identifiable, sensitive, and even classified data are stored on those devices. The nature of such stored data and mobility of the devices make unauthorized access or even loss of the devices particularly concerning. This pressing security concern has motivated efforts in developing new and enhancing existing MUA methods.

MUA refers to the verification of a user's identity in accessing a mobile device to prevent and minimize attacks and unauthorized access. A variety of MUA methods have been proposed to date, such as passwords and biometrics [1]. Regardless of their strengths and security vulnerabilities, MUA methods are generally subject to security-usability trade-offs. For example, a more complex password will be more secure, but more difficult to remember and enter on a mobile device (i.e., low usability), or vice versa. After long-time deployment in commercial and law enforcement domains [2], facial recognition has received rapid adoption in MUA in recent years due to its potential usability and security benefits. However, the realization of those benefits in a mobile device setting still faces significant usability and security challenges such as lighting variability, facial disguises [3]. General mobile users may not be aware of the trade-offs or security vulnerabilities of specific MUA techniques. As a result, users may not choose the techniques that best fit their needs.

In addition to the general security and usability features of MUA methods, their adoption may also be dependent on mobile users' individual characteristics and usage context. Individual characteristics include demographic information, mobile experience, and interaction style. For instance, a few studies reported that approximately half of users would prefer to interact with their mobile devices using one hand [4, 5]. Users also likely to perform MUA or accessing the device in a variety of situations, such as sitting next to a family member, a co-worker, or a stranger in a crowded public space, or entering confidential information without looking at the device, namely sight-free authentication [6, 7]. Current design of MUA methods is mainly focused on normal usage condition while giving little attention to situational impairments, which refers to users' temporary difficulty in accessing mobile devices due to specific context or situations that they are in (e.g., holding a cup of coffee in one hand and watching incoming traffic [1]). Hence, it is of critical needs to understand how MUA methods are being used in different situations.

To address the above knowledge gap, this study aims to answer the following research questions: *1) How do mobile users perceive MUA methods with respect to their security and usability?* and 2) *How do user perceptions vary with their individual characteristics and usage contexts, particularly under sight-free and one-handed situations?*

This research aims to answer the above questions using a survey questionnaire. Its primary contributions are two folds. First, it is the first research study that incorporates a variety of influential factors to prob the needs of sight-free and one-handed MUA. Second, the findings of this research provide new research and practical insights and guidance for designing more secure, effective, usable, and accessible MUA methods.

II. RELATED WORK

This section reviews different types of MUA methods and studies on one-handed and sight-free situations.

A. Mobile User Authentication Methods

According to [1], existing MUA methods can be classified into three major categories: knowledge-based, object- or token-based, and biometrics-based. Each type of methods has its strengths and weaknesses with regard to security and usability [8]. Knowledge-based methods are classic MUA methods that require a user to portray his/her credential as secret knowledge. They include, but not limited to, textual or graphical passwords and PIN. The traditional security-usability tradeoff lies in that a more complex or longer password is more secure and less vulnerable to malicious or unauthorized access, but would also be more difficult to remember and use on a mobile device [9], making users tend to select passwords that are dictionary trackable or easy to enter (e.g., shorter textual passwords) [10]. The lower usability of more secure MUA methods may make some users hesitated to adopt MUA, while MUA methods with high usability but low security will not achieve the fundamental goal of MUA [11].

Token-based MUA methods usually require a physical object (e.g., smart cards, QR codes) to authenticate a user, which is relatively more secure than knowledge-based MUA methods. However, users must keep the object with them or place it at a safe location [12], which might introduce additional security risks if users share the token with someone else or get the token lost or stolen.

A biometrics method is based on the assumption that physiological or behavioral characteristics used as biometric measures should possess universality, distinctiveness, permanence, ease in collectability, and robustness, and thus should be immune to spoofing [13]. Biometrics can be further divided into physiological and behavioral biometrics. Physiological attributes refer to physical and intrinsic parameters of a specific part of an individual [14], such as fingerprint, face , iris, retinal, palm and vein, hand geometry, ear shape, lip-print, dental radiograph, tongue print , ECG, auditory biometrics [15, 16], and facial thermogram. On the other hand, behavioral biometrics adopts identity-invariant features of human behavior to authenticate users [17-20], which includes, but is not limited to, typing, keystroke progression, gait patterns, body movement, and finger touches when interacting with a touch-screen smartphone. However, many biometric schemes raise cost, acceptability, and privacy concerns [12]. They are also vulnerable to direct attacks by the use of synthetic biometric samples (e.g., fingerprints or face images) [13].

B. *Supportive of One-Handed and Sight-Free Interactions*

According to the search results from ACM and IEEE digital libraries, Google Scholar, and Research Gate, the prior work related to one-handed and sight-free interactions are very limited.

The study of one-handed interaction can be dated back to 1960s [21]. Recent studies have focused on designing tools or techniques to support or improve one-handed interaction, such as developing one-handed zooming techniques [22], creating a very small touch device to enable back-of-device interaction [23], capturing sequentially coordinated input [24], and leveraging behavioral dynamics of thumb interaction with the touch-screen of a smartphone [1]. Some recent research has tried to combine touch input and screen reader [25], as well as using finger-drawn PIN or thumb-to-fingers touch interfaces [26, 27] to support sight-free interaction.

Based on the systematic review of literature on MUA methods, there seems a lack of studies on MUA that enables user authentication during users' one-handed and sight-free interactions with mobile devices. Given the findings of previous research that has demonstrated the needs of one-handed and sight-free interactions with mobile devices [1, 21, 22, 23, 24, 25, 26, 27], it is necessary and beneficial to understand how users perceive with MUA methods that support one-handed and sight-free use.

III. METHOD

To answer the research questions, we adopted the survey method, which is the best approach to obtain personal beliefs, perceptions, and attitudes, while enhancing the universality of research findings [28]. The study was approved by the Institutional Review Board of the authors' home university.

A. *Questionnaire Design*

The survey consisted of two parts. The first part covered participants' demographic information, preferences for hand posture, and mobile use experience. The second part of the survey asked about participants' preferences and perception of MUA methods under different device and usage contexts such as one-handed and sight-free authentication.

It was very difficult, if not entirely impossible, to identify an existing MUA method that offers high levels of security, usability, and privacy protection simultaneously. In order to gain an initial understanding of user preferences, we asked the participants to rank a list of existing MUA methods (see next section) with respect to their security and usability. In addition, we asked participants to choose their most preferred MUA methods in general.

Most of the survey questions were measured on a 7-point Likert scale. The rankings of MUA methods in terms of security and usability were generated based on the average of individual participants' rankings. To address the potential bias that may be introduced by the listed ranking of MUA methods, we also measured the change in rank order in relation to the initial listing. Moreover, the device context was measured by mobile operating systems, which were categorized into three categories: IOS, Android, and mixed (using different operating systems in parallel). The entire survey took about 25 minutes on average to complete.

B. *A List of MUA Methods*

Based on a systematic literature review (see Section II), we created the list of MUA methods, including passcode (e.g., PIN), text password (e.g., using characters to form a password), graphical password (e.g., draw-a-secret), drawing a pattern (connecting dots to complete a pattern), facial recognition, fingerprint recognition (e.g., Touch ID), iris scan, other physiological biometrics (e.g., based on palm, ear, voice), system encrypted authentication (e.g., one-time passcode, duo authentication such as sending one-time passcodes via email), keystroke dynamics (based on the manner and rhythm of typing characters using a keyboard or keypad), touch dynamics (based on the manner and the rhythm of fingers touching on a touchscreen), other behavioral biometrics (e.g., haptic, gait, handwriting), token-based authentication (e.g., smart card, USB dongle), and visual or tactile challenges (e.g., answering several challenges). The survey also offers "Other" as a catch-all option for MUA methods.

C. *Participants*

We recruited participants mainly from the university mailing lists and relevant online communities. A total of 249 participants responded to the survey, and 232 completed all the questions with valid responses. Among them, 63.8% were female, 34.5% were male, and 1.7% were other (e.g., non-binary); 57.3% were between 18 to 24 years old, 33.2% between 25 to 39 years old, and the rest between 40 to 65 years old. Student and employed participants were divided roughly equally. All of the qualified participants owned at least one smartphone and had experience with a touch-screen mobile device.

IV. RESULTS AND DISCUSSION

A. Security Perception

A radar figure (Fig. 1) is used to present the average of individual participants' rankings, the centroid shows the highest perceived ranking, and the boundary shows the lowest.

Fingerprint authentication was ranked as the most secure method, followed by iris scan and facial recognition. All of the three top-ranked MUA methods belong to biometrics, indicating the participants' strong belief in biometrics to secure their mobile devices. The next set of MUA methods in the rank are dominated by knowledge-based methods such as text password, passcode, and graphical passwords. The results suggest that those methods remain as secure alternatives for MUA by the participants. On the other hand, other behavioral biometrics, token-based methods, and visual or tactile challenges raise high-security concerns. For instance, a user might lose a token-based object, causing authentication failure and potential attacks using the stolen token.

The results of the change in the ranking are reported in Fig. 2, where the corresponding initial rankings are labelled from 1 to 15. Based on the results, traditional authentication methods, including passcode, text password, graphical password, and pattern drawing, seem to have a major concern with respect to security, as the order of those MUA methods was ranked greater than their initial order. In contrast, most of the biometrics-based MUA methods were ranked higher, especially fingerprint authentication and iris scan, showing a strong perception and preference. In reality, as two emerging methods, both fingerprint and iris scan based MUA methods have caught a lot of attention.

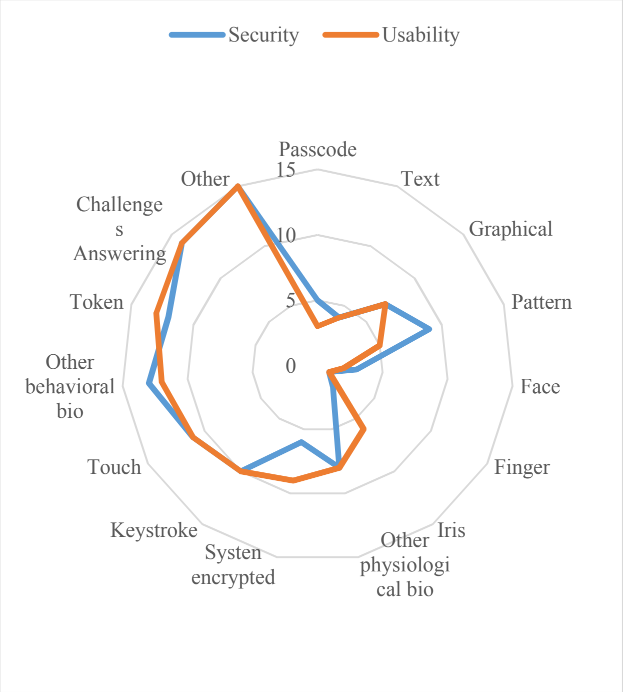

Fig. 1. Rankings of MUA Methods in Security and Usability

B. Usability Perception

Like the security ranking, fingerprint and facial recognition were ranked as the top two in terms of usability of MUA. The results confirm user preference of biometrics over traditional authentication methods such as draw-a-secret and text passwords [29]. Unlike the security ranking, however, passcode was ranked among the knowledge-based MUA methods with the highest usability. Other knowledge-based methods received a moderate ranking, which confirmed the findings from one of the prior studies [11]. In addition, the participants did perceive other behavioral biometrics, token-based methods, and visual or tactile challenges as poor in terms of usability. For instance, biometric gait authentication requires special sensor(s) attached to the body to operate. It may not be convenient for a user to carry a physical token such as a smart card or key with him/her.

Contrary to our prediction, some knowledge-based and object- or token- based MUA methods, such as touch dynamics and visual or tactile challenges, were ranked relatively lower than the initial order. For instance, system encrypted authentication was considered weak in terms of usability. One of the explanations from the participants was that system encrypted authentication might take relatively a long time to authenticate a user.

Surprisingly, most of the MUA methods received consistent rankings between security and usability except pattern drawing. In other words, the participants' responses did not reflect the security-usability tradeoffs that are widely recognized in the authentication literature. There are two alternative explanations for the results. One is that MUA techniques have been advancing in such a way that both security and usability are improved simultaneously. The other is that user perceptions of MUA methods are limited by their own experience, who may not have the full knowledge of the advantages and vulnerabilities of individual methods. The results show that the participants did not feel that pattern drawing was secure despite its average usability. The finding may be attributed to the low familiarity of users with the method.

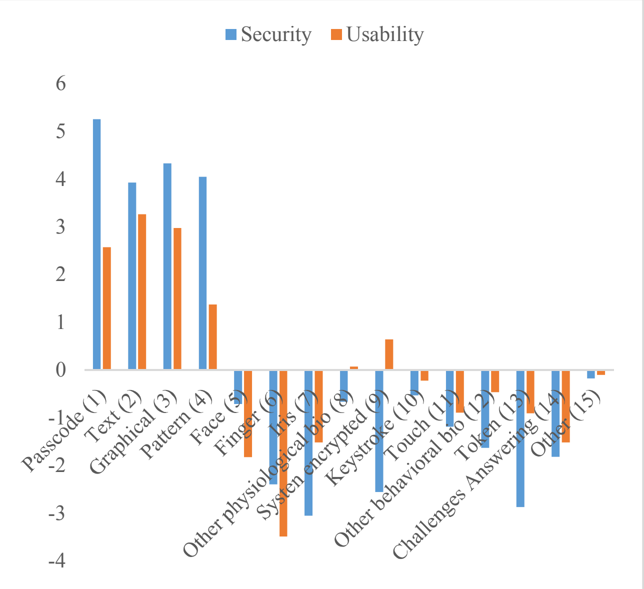

Fig. 2. Variances of MUA Methods in Security and Usability

Among the list of MUA methods, 9 were chosen as the most preferred methods by at least one participant (see Fig. 3). The top-3 methods in descending order of its frequency of participant selection are fingerprint recognition, passcode, and facial recognition. It is worth noting that the selected is a mixture of both traditional and recent MUA methods.

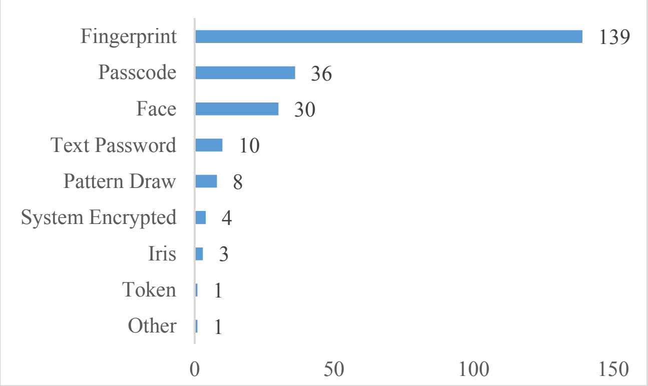

Fig. 3. Frequencies of the Most Preferred MUA Methods

C. *Effects of Demographic Factors*

For participants in the age range of 39 years old and below, fingerprint biometrics was the most preferred method, followed by passcode and facial recognition, which was aligned with the main trend [20]. For participants in the next age group (40~65 years old), text password was among the most preferred second only to fingerprint biometrics. Thus, the results show that age influences the selection of MUA methods. The younger users seemed more inclined toward adopting emerging MUA methods.

The data shows little gender difference in their preferred methods for MUA except that females seemed to be slightly in more favor of fingerprint biometrics than males. Similarly, the distribution of preferred MUA methods did not seem to vary with education except for those who obtained Ph.D. or other terminal degrees. The latter preferred fingerprint and facial recognition biometrics most and equally, followed by text password and pattern drawing. Other users showed a strong preference for fingerprint biometrics and little interest in text password and pattern drawing.

D. *Device Context*

It is shown from TABLE I that user preferences of MUA methods are similar regardless of the type of mobile operating system, despite that their preferences of fingerprint and facial biometrics are relatively stronger for the IOS device and their preferences for passcode are relatively stronger for the Android device. The findings can be explained with the default MUA methods that mobile devices are equipped with. For instance, Apple devices have a facial recognition system embedded in their advanced devices, which is not so widely used as in Android systems. Interestingly, drawing a pattern is the second favorite of participants who used a mixture of two types of mobile operating systems. The findings added a great addition to the prior work that was investigating the willingness of adopting MUA methods with higher error rate [30].

E. *Sight-free Situation*

To gain insights into sight-free MUA and to identify future research opportunities, we asked the participants about the frequency and difficulty in performing MUA sight-free (i.e., without looking at the device screen). The results reveal that the majority (73%) of the participants have engaged in sight-free interactions with mobile devices occasionally or more often. In addition, most participants rated sight-free MUA as neutral or slightly leaning toward ease of use, which was contradictory to the findings of a prior study with PIN and pattern lock [6].

We analyzed the effects of user demographics on their actual use and perceived difficulty of sight-free MUA using correlation analyses. The results are reported in Table II. They show that education has a negative effect on both use and ease of use of sight-free MUA ($p<0.05$). Nevertheless, online experience did not yield any significant effect (p=*n.s.*).

	Demographic Factors	Finger	Passcode	Face	Text	Pattern	System Encrypted	Iris	Other	Token
Age	18-24 Years Old	62%	15%	14%	3%	2%	2%	2%	0%	1%
	25-39 Years Old	56%	18%	13%	4%	6%	1%	0%	1%	0%
	40-65 Years Old	59%	9%	5%	14%	5%	5%	5%	0%	0%
Gender	Male	54%	18%	15%	5%	4%	2%	1%	0%	1%
	Female	63%	14%	12%	4%	3%	1%	1%	1%	0%
Education	High school degree or lower	64%	18%	9%	9%	0%	0%	0%	0%	0%
	Associate degree	63%	14%	11%	3%	4%	3%	3%	0%	0%
	Bachelor's Degree	63%	12%	17%	2%	0%	2%	0%	0%	2%
	Master's Degree	55%	23%	11%	5%	5%	0%	0%	2%	0%
	Completed Ph.D. or other terminal degrees	27%	9%	27%	18%	18%	0%	0%	0%	0%
Occupation	Employed	57%	13%	16%	4%	5%	2%	1%	1%	1%
	Student	60%	18%	12%	5%	3%	1%	1%	0%	0%
Hand posture	One Hand	64%	14%	11%	3%	3%	2%	1%	1%	1%
	Two Hands	46%	20%	19%	7%	6%	0%	2%	0%	0%
Device type	IOS	64%	14%	17%	3%	0%	1%	1%	0%	0%
	Android	50%	22%	9%	7%	5%	3%	2%	0%	2%
	Mixed	58%	10%	3%	6%	16%	0%	3%	3%	0%

TABLE I. Cross-tabulation of Demographic Factors with MUA Methods

	Actual Use	Ease of Use
Education	- 0.248 *	- 0.256 *
Online Experience	- 0.003	- 0.058

*$p < 0.05$

TABLE II. Effects for Sight-free MUA

F. Hand Posture Preference in MUA

The survey responses show that more participants interacted with mobile devices for MUA using one hand than two hands. In addition, the majority (84%) of the participants performed MUA using one hand frequently or very frequently. Further, most participants perceived one-handed MUA as somewhat easy to use.

We analyzed the effects of user demographics on their actual use and perceived difficulty of one-handed MUA using correlation analyses. The results are reported in Table III. They show that education has a negative effect on the ease of use of one-handed MUA ($p<0.05$). Nevertheless, the online experience did not yield any significant effect (p=*n.s.*).

By cross-referencing hand posture and demographic factors, we found that the participants preferred performing MUA using one hand regardless of their age groups. Specifically, the participants aged between 25 and 39 years used one-handed interaction the most, followed by those aged between 18 and 24 years old and those aged between 40 and 65 years old. There was no significant difference in distributions of one-handed MUA with mobile device across gender and occupation.

	Actual Use	Ease of Use
Education	- 0.163 †	- 0.221 *
Online Experience	0.027	- 0.021

$^{\dagger}p < 0.10$; *$p < 0.05$.

TABLE III. Effects for One-handed MUA

V. CONCLUSION

This study investigated user perception of different types of MUA methods in terms of security and usability and their preferences and use of MUA methods under different contexts. The research findings have implications for the design of MUA methods that can better meet user needs and their preferences.

The findings cast a favorable light to physiological biometrics due to security and usability benefits. In particular, fingerprint biometrics is the most dominant MUA method. On the other hand, passcode remains one of the frequently used and easiest-to-use methods. In addition, the participants prefer one-handed to two-handed MUA, which calls for research efforts in the design and development of one-handed MUA. The participants were generally neutral or slightly in favor of sight-free MUA. Future research may look into situations where sight-free MUA is desired. This study can be extended by examining the effects of interactions among user demographics and among different MUA contexts on user perception and adoption of MUA methods.

ACKNOWLEDGMENT

This work is supported in part by two grant awards from the National Science Foundation (Award #s: CNS 1704800 and SES 1527684). Any opinions, findings or recommendations expressed here are those of the authors and are not necessarily those of the sponsor of this research. The authors would also like to thank Neel Nayak for participating in an early discussion of this research.

REFERENCES

[1] L. Zhou, Y. Kang, D. Zhang, and J. Lai, "Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones," Decision Support Systems, vol. 92, pp. 14-24, 2016.

[2] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," ACM Comput. Surv., vol. 35, pp. 399-458, 2003.

[3] A. M. Guzman, M. Goryawala, J. Wang, A. Barreto, J. Andrian, N. Rishe, et al., "Thermal Imaging as a Biometrics Approach to Facial Signature Authentication," IEEE Journal of Biomedical and Health Informatics, vol. 17, pp. 214-222, 2013.

[4] S. Hoober, (2013, Feb. 10, 2018), How Do Users Really Hold Mobile Devices? UX Matters, Available at https://www.uxmatters.com/mt/archives/2013/02/how-do-users-really-hold-mobile-devices.php

[5] Cornelia, "How does the location affect user interactions with their mobile devices," in Game usability and player experience blog vol. 2016, ed. Réalités Parallèles 2014.

[6] F. Wolf, A. J. Aviv, and R. Kuber, "Performance of Eyes-Free Mobile Authentication Work in Progress," USEC, 2018.

[7] F. Wolf, A. J. Aviv, and R. Kuber, "It's all about the start" classifying eyes-free mobile authentication techniques," Journal of Information Security and Applications, vol. 41, 2018, pp. 28-40.

[8] L. O. Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol. 91, pp. 2021-2040, 2003.

[9] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password Memorability and Security: Empirical Results," IEEE Security & Privacy, 2004.

[10] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, et al., "Of Passwords and People: Measuring the Effect of Password-Composition Policies," in Proceedings of the International Conference on Human Factors in Computing Systems, ser. CHI '11, 2011, pp. 2595–2604.

[11] F. Wolf, R. Kuber, and A. J. Aviv, "An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication," Behaviour & Information Technology, 2018, 37:4, pp. 320-334.

[12] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive authentication: deciding when to authenticate on mobile phones," presented at the Proceedings of the 21st USENIX conference on Security Symposium, Bellevue, WA, 2012.

[13] S. Chauhan, A. S. Arora, and A. Kaul, "A survey of emerging biometric modalities," Procedia Computer Science, vol. 2, pp. 213-218, 2010/01/01 2010.

[14] C. Holz, S. Buthpitiya, and M. Knaust, "Bodyprint: Biometric User Identification on Mobile Devices Using the Capacitive Touchscreen to Scan Body Parts," presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, Republic of Korea, 2015.

[15] Y. Guo and A. Tyagi, "Voice Based User-Device Physical Unclonable Functions for Mobile Device Authentication," in 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2016, pp. 512-517.

[16] Z. Yan and S. Zhao, "A Usable Authentication System Based on Personal Voice Challenge," in 2016 International Conference on Advanced Cloud and Big Data (CBD), 2016, pp. 194-199.

[17] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010, pp. 306-311.

[18] P. S. Teh, A. B. J. Teoh, and S. Yue, "A Survey of Keystroke Dynamics Biometrics," The Scientific World Journal, 2013.

[19] X. Zhao, T. Feng, and W. Shi, "Continuous mobile authentication using a novel Graphic Touch Gesture Feature," in 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1-6.

[20] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones,"

IEEE Communications Surveys & Tutorials, vol. 17, pp. 1268-1293, 2015.

[21] D. C. Engelbart, SRI-ARC, A technical session presentation at the Fall Joint Computer Conference (NLS demo: The computer mouse debut), 1968, Engelbart Collection, Stanford University Library, Menlo Park (CA).

[22] A. K. Karlson, B. B. Bederson, and J. SanGiovanni, "AppLens and LaunchTile: Two designs for one-handed thumb use on small devices," Proc. CHI '05, New York: ACM Press, 2005, 201-210.

[23] P. Baudisch and G. Chu, "Back-of-device interaction allows creating very small touch devices," In Proc. CHI'09, 2009, 1923–1932.

[24] X. D. Yang, E. Mak, P. Irani, and W. F. Bischof, "Dual-surface input: augmenting one-handed interaction with coordinated front and behind-the-screen input," In MobileHCI '09, ACM, 2009, 5:1–5:10.

[25] C. Law and G. Vanderheiden, “The development of a simple, low cost set of universal access features for electronic devices,” Proceedings on the 2000 conference on Universal Usability (CUU ’00), ACM Press (2000), 118–123.

[26] T. V. Nguyen, N. Sae-Bae, and N. Memon, “DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices,” Journal of Computers & Security, 2017, pp. 115-128.

[27] D-Y. Huang, L. Chan, S. Yang, F. Wang, R-H. Liang, Y-Ping Hung, et al., “DigitSpace: Designing Thumb-to-Fingers Touch Interfaces for One-Handed and Eyes-Free Interactions,” CHI, 2016.

[28] F. N. Kerlinger, 1973, Foundations of Behavioral Research (2nd ed.), New York: Holt, Rinehart & Winston.

[29] H. P. D. Silva, A. Fred, A. Lourenço, and A. K. Jain, "Finger ECG signal for user authentication: Usability and performance," in 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1-8.

[30] A. Mahfouza, I. Muslukhova, and K. Beznosova, “Android users in the wild: Their authentication and usage behavior,” Pervasive and Mobile Computing, 2016, pp. 50-61.