Evaluating Smartphone Authentication Schemes with Older Adults

Hassan Khan
Cheriton School of Comp. Sci.
University of Waterloo,
Waterloo, ON, Canada
h37khan@uwaterloo.ca

Kelly Grindrod
School of Pharmacy
University of Waterloo,
Waterloo, ON, Canada
kgrindrod@uwaterloo.ca

Urs Hengartner
Cheriton School of Comp. Sci.
University of Waterloo,
Waterloo, ON, Canada
urs.hengartner@uwaterloo.ca

Daniel Vogel
Cheriton School of Comp. Sci.
University of Waterloo,
Waterloo, ON, Canada
dvogel@uwaterloo.ca

Abstract

We present results of the first ever quantitative and qualitative evaluation of four diverse smartphone authentication schemes with older adults to uncover a host of usability issues unique to them. We show that older adults spend significantly more time to configure the authentication schemes and to authenticate; however, unlike their young counterparts, speed is not a concern to them. Older adults prefer easy to remember and non-dexterous authentication schemes. Consequently, their usability preferences in terms of annoyance and fatigue are significantly different from the preferences of young adults.

Introduction

Older adults (50 years or older) are more likely to suffer from chronic conditions including arthritis, Parkinson's disease, and osteoporosis. These conditions have an adverse affect on dexterity (fine motor skills). Consequently, age-related differences may result in different usability preferences for authentication. Several research efforts have evaluated the usability of the available authentication mechanisms on smartphones [2, 3]. Despite the increasing number of older adults who use smartphones [4], they are not represented in the existing evaluation studies. We bridge this gap by conducting a study to perform a quantitative and qualitative comparison of young (18-30 years) and older adults for authentication.

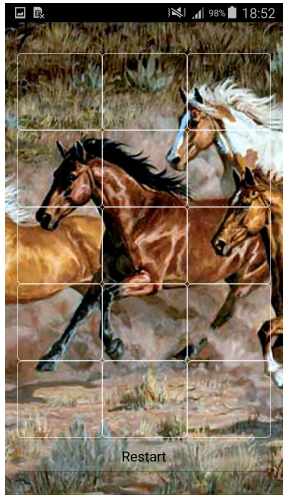

Figure 1: Cued click points.

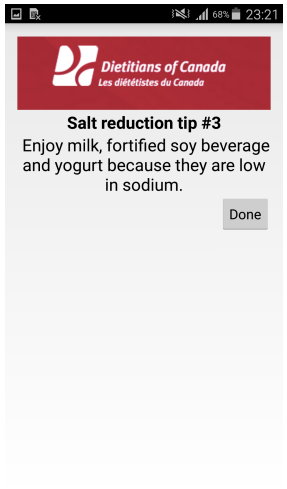

Figure 2: Distraction task.

Related Work

A few studies have evaluated non smartphone authentication schemes with older adults. Vu and Hill [7] showed that older adults are more likely to forget text-based passwords and image-based mnemonic techniques are useful as cues for password recall for web services. Renaud and Ramsay [5] proposed and evaluated a graphical password scheme for web services. Their showed that their scheme is better in terms of usability and error rate than PINs. Sreeramareddy et al. [6] proposed a draw-a-secret based graphical password scheme for web services. Their showed that their scheme is accurate and usable and can be used as an alternate form of authentication by older adults. The existing literature evaluates novel authentication proposals for web services. To the best of our knowledge, a comparative evaluation of popular authentication schemes on smartphones with older adults has not been performed.

Study Goals

The main objective of this study is to determine whether age-related differences play a role in the usability of smartphone authentication options. We capture this goal through the following research questions: (1) Are there differences between young and older adults in terms of time-to-authenticate and authentication errors? (2) Do older adults provide different system usability scale (SUS) ratings for authentication schemes than young adults? (3) Are the (dis)like factors for authentication schemes between older and young adults different? If the answers are affirmative, then age-related differences play an important role in the usability preferences for authentication on smartphones. We admit that memorability issues due to chronic conditions may affect the usability experience. While we note participants' concerns surrounding memorability issues, we do not measure them since it requires a longitudinal study.

Study Design

We evaluated four authentication schemes: (1) a four-digit PIN, where all ascending or repeating digits were not allowed; (2) Android's pattern-lock with standard restriction; (3) a fingerprint scanner (Samsung S5's scanner, which requires sliding a finger across the home button); and (4) cued click points (CCP) [1] where users tap a secret location on a sequence of five images (same location not allowed across five images). We chose the PIN and pattern-lock schemes because they are widely available. We chose fingerprint as the canonical biometric scheme. A Samsung device was used since it provides an API for its fingerprint scanner. CCP was selected because older adults preferred graphical passwords for web services [5, 6, 7]. For CCP, a 3x5 grid was superimposed on each image to cater impaired motor skills (see Figure 1).

We developed an Android app, which provided the four authentication schemes and logged time to configure, time to authenticate and the number of errors. The app presented tips on healthy lifestyle as a distraction task (see Figure 2). To evaluate each scheme, the app first asked the user to configure the scheme (participants were allowed to note the secret on a paper if they desired). It then asked the user to turn off the screen and wait for the device to ring (with vibrate) to indicate it was time to perform a task. When the device rang, the user authenticated, read the tip and then turned off the screen. The user performed 20 authentications in this fashion for each authentication scheme.

Experiment Protocol

Older adults were recruited through public libraries, senior education sessions, senior computer clubs, and community centres. Young adults were recruited through university-wide mailing lists and through Kijiji (similar to Craigslist). To be eligible for the study, participants had to have prior expe-

	Young	Older
Conf. time		
PIN*	16 (9)	30 (15)
Pattern*	19 (22)	42 (24)
Fingerprint*	52 (18)	65 (20)
CCP*	46 (13)	81 (45)
Auth. time		
PIN	3.7 (0.8)	7.7 (10)
Pattern*	3 (0.8)	4.5 (1.3)
Fingerprint*	18.7 (24)	38 (41)
CCP*	5.7 (1.3)	8.5 (3)
Auth. err		
PIN	0.3 (0.6)	0.47 (1)
Pattern	1.3 (1.6)	0.53 (0.98)
Fingerprint	4 (4.3)	7.2 (11)
CCP	0.3 (0.6)	0.5 (1.5)

Table 2: Avg. (std. dev.) configuration and authentication times in seconds and avg. (std. dev.) of authentication errors (*p-value < 0.05).

	Young (n=23)	Older (n=59)
Avg. age (range)	22 (18–29)	67 (50–84)
Female	18 (78%)	30 (52%)
Highest Education		
High school	2 (8%)	8 (14%)
College	0 (0%)	8 (14%)
University	21 (91%)	43 (73%)
Chronic health cond. $\geq$1*	3 (13%)	18 (30%)
Prescription medicine $\geq$1*	5 (22%)	41 (70%)

Table 1: Participants at a glance (*p-value < 0.05).

rience using a smartphone or tablet. An hour long study session was conducted at the university, a participant's home (for older adults) or a coffee shop according to the participant's preference. Participants were paid $10.

We first collected demographics and data on chronic conditions of the recruited participants (see Table 1). A researcher introduced and demonstrated each scheme to participants. Participants then tested four authentication schemes in a random order. After testing each scheme, participants answered a questionnaire regarding their overall usability experience, their experience in terms of time consumption, annoyance, tiresomeness, and SUS ratings. A semi-structured interview was also conducted to explore what participants (dis)liked about each scheme.

Results

Authentication metrics

In Table 2, we report time to configure authentication, time to authenticate and the number of authentication errors for the four schemes. ANOVA and post hoc Boneferroni tests indicate that all techniques are different from one another for both groups in terms of time to configure authentication and time to authenticate. However, only the fingerprint scheme is different from the other schemes in terms of the number of authentication errors. It also shows that PIN is the fastest scheme in terms of time to configure authentication (*avg=28s*); pattern-lock is the quickest authentication scheme (*avg=28s*); and fingerprint is the most error prone scheme with an average of six errors per participant.

Our evaluation shows that young adults are approximately twice as fast to configure authentication schemes. T-tests indicate that the time to configure authentication between young and older adults is significantly different across all schemes ($p < 0.01$). Older adults are at least 40% slower in terms of time to authenticate for all schemes except PIN and t-tests indicate significant differences for all schemes ($p < 0.04$) except PIN ($t = 1.86, p = 0.06$). While no significant differences are observed between young and older adults in terms of authentication errors, the reported numbers exclude participants who failed to successfully complete a session. For the fingerprint scheme, only one young adult whereas 13 (22%) older adults failed to complete the session after encountering a large number of errors (no restriction was imposed; participants gave up after several retries). The large number of failed attempts by older adults might be specific to the device used, which required sliding a finger on the home button. A subsequent study needs to be performed to confirm this suspicion.

Usability ratings

Participants rated usability of each scheme in terms of time consumption, annoyance, and fatigue on a five-point Likert-type scale. Participants' responses indicate that significantly more (32% more) young adults consider CCP to be annoying ($\chi^2(1) = 17.3, p < 0.001$) whereas, significantly more (15% more) older adults consider fingerprint to be annoying ($\chi^2(1) = 5.5, p = 0.01$). Furthermore, significantly more (17% and 25% more) older adults consider PIN and

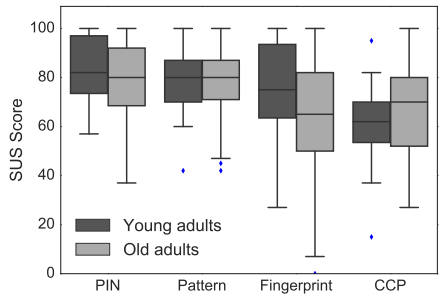

Figure 3: Participants' SUS ratings (p-value < 0.05 only for Fingerprint).

	Young	Older
PIN	7.3 (2.3)	6.9 (2.3)
Pattern	7 (1.9)	6.8 (2.2)
Fingerprint*	8.3 (2.5)	6 (3.5)
CCP	4.6 (3.3)	6 (2.6)

Table 3: Avg. (std. dev.) ratings on a ten-point Likert-type scale (*p-value < 0.05).

pattern-lock to be tiring, respectively (for $\chi^2, p < 0.001$). Finally, significantly fewer older adults (16% and 22% fewer) consider PIN and pattern-lock, respectively, to be time consuming than young adults whereas, significantly fewer (20% fewer) young adults considered fingerprint to be time consuming than older adults (for $\chi^2, p < 0.01$).

In terms of SUS scores (see Figure 3), t-tests between SUS scores for young and older adults indicate no statistically significant differences across PIN, pattern-lock and CCP. However, significantly more young adults rated fingerprint higher than older adults ($t = 2.3, p = 0.04$) . The ten-point Likert-type scale rating of overall usability for each scheme is provided in Table 3. Similar to the SUS scores, we observe that significantly more young adults rated fingerprint higher than older adults ($t = 1.8, p = 0.02$).

Feedback from interviews

During the exit interview, participants were asked what they (dis)liked about each scheme. Their responses were coded by a researcher. Among all participants, the most cited reason to like PIN and pattern-lock was "easy to use" and for fingerprint and CCP it was secure and "fun to use", respectively. The most cited reason to dislike PIN, pattern, fingerprint and CCP was "difficult to remember", insecure, inconsistent and "time consuming", respectively. We now present interesting differences in terms of participants reasons to (dis)like particular schemes.

We compared the responses of young and older adults in terms of their (dis)likes. Speed was a critical factor for young adults and one of the top three reasons they liked PIN, pattern-lock and fingerprint was "quick". Similarly, 67% young adults indicated that the most disliked factor for CCP was "time consuming". On the other hand, for older adults, "easy to remember" was one of the top three reasons to like PIN, pattern-lock and CCP. Few unique dis(likes) were reported by older adults: six disliked that they required dexterity for pattern-lock (comments were similar to: *"[pattern] requires me to slide without missing those points"*); and five raised the concern that pattern-lock and CCP were difficult to note down for safe keeping like their other passwords.

Discussion & Conclusion

Our evaluation shows that there are significant differences between young and older adults in terms of time to configure authentication and time to authenticate across all schemes. It further shows that older adults perceive usability in terms of annoyance, fatigue and time consumption differently than young adults. The semi-structured interviews suggest that the speed focus of young and memorability focus of older adults might be responsible for these differences. Contrary to previous studies, older adults did not rate CCP higher than other schemes. Our evaluation signifies the importance of the usability evaluation of authentication schemes across young and older adults.

Acknowledgement

We thank the Office of the Privacy Commissioner of Canada for their support.

REFERENCES

1. Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. 2007. Graphical password authentication using cued click points. In *Computer Security–ESORICS 2007*. Springer.
2. Serge Egelman, Sakshi Jain, Rebecca S Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are You Ready to Lock?. In *ACM SIGSAC Conference on Computer & Communications Security*. ACM.
3. Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *Symposium on Usable Privacy and Security*.
4. PEW Research Center. 2016. Older Adults and Technology Use. `http://www.pewinternet.org/2014/04/03/older-adults-and-technology-use/`. (March 2016).
5. Karen Renaud and Judith Ramsay. 2007. Now what was that password again? A more flexible way of identifying and authenticating our seniors. *Behaviour & Information Technology* 26, 4 (2007), 309–322.
6. Lakshmidevi Sreeramareddy, Pewu Mulbah, and Jinjuan Heidi Feng. 2015. Investigating the Use of Gesture-Based Passwords by the Seniors. In *Human Aspects of Information Security, Privacy, and Trust*. Springer.
7. Kim-Phuong L Vu and Martina M Hills. 2013. The influence of password restrictions and mnemonics on the memory for passwords of older adults. In *Human Interface and the Management of Information. Information and Interaction Design*. Springer.