[Short Paper] Who Did You Call Last?

Hyoungshick Kim
University of British Columbia
2332 Main Mall
Vancouver, BC, Canada
hyoung@ece.ubc.ca

Konstantin Beznosov
University of British Columbia
2332 Main Mall
Vancouver, BC, Canada
beznosov@ece.ubc.ca

ABSTRACT

Providing a secure and usable user authentication scheme for mobile phones is a major challenge. Though there are many proposals for user authentication, PIN or passwords only are popularly used for mobile phones, which are inherently weak since users tend to choose PINs or passwords that are easy to remember and reuse, making it also easy for attackers to guess and compromise them. We introuduce a framework using the personal information stored inside a user's mobile phone – if this information is private and memorable for the phone owner alone, we may use this for user authentication. To verify this idea, we performed a pilot study to observe the knowledge gap between the phone owner and the other people. Findings from this study confirmed the feasibility of this idea. The proposed idea may give some new angles to old authentication problems.

Categories and Subject Descriptors

H.5.m [**Information Interfaces and Presentation**]: Miscellaneous

General Terms

Human Factors, Security, Usability

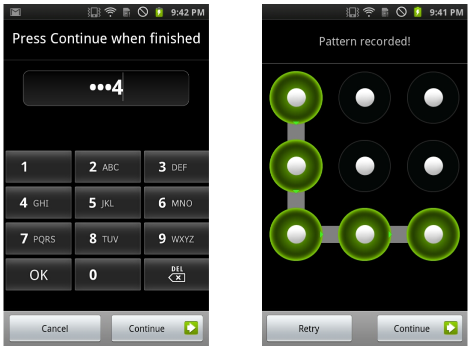
Keywords

Authentication, Personal Knowledge, PIN

1. INTRODUCTION

In recent years, mobile phones have used as a digital-wallet, storing sensitive information like credit cards, identity cards, vouchers, and mobile banking tokens [1]. Just as one would try to safeguard a wallet full of cash and credit cards from strangers, a digital-wallet user also wants to protect its contents through user authentication mechanisms.

Among many authentication mechanisms available, Personal Identification Number (PIN) or graphical passwords [11] are dominantly used. Some practical examples of these are shown in Figure 1.



(a) PIN (b) Graphical Password

Figure 1: Two examples of conventional authentication mechanisms for mobile phones.

However, all of these authentication methods too have their own inherent limitations [5, 11, 4, 12, 3, 7] – many users naturally choose PINs or passwords that are easy to remember without really paying close attention to the security implications. Such a trend implies that the actual spaces of PINs or passwords used are much smaller than the theoretical spaces, dramatically increasing the likelihood of an attacker guessing the victim's PIN or password. To prevent users from choosing weak PINs or passwords, devices/applications may disallow short, simple, and typical PINs or passwords; however, the effects of such restrictions are rather limited or still unclear [7]. The motivation of our work is to escape from this trap of poor password practices. This paper contributes in the following areas:

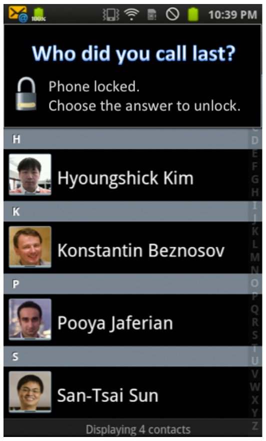
- We propose a user authentication concept based on *personal knowledge questions*. Unlike conventional personal knowledge questions [16, 9], we use the knowledge about the phone owner's personal information which is stored inside her mobile phone and also dynamically updated over time. We particularly explored what types of information can be used for user authentication (see Section 2).
- We performed a pilot study involving 6 participants to observe the knowledge gap in the information stored in mobile phone between the phone owner and the other people. In this pilot study, we observed that there might be a reasonably large gap between the phone

Symposium on Usable Privacy and Security (SOUPS) 2012, July 11-13, 2012, Washington, DC, USA.

owner and pure strangers. For user authentication, however, challenge questions must be designed more carefully against frenemies in the phone owner's social circle. For user authentication, our recommendation would be use the personal knowledge questions about applications and web browsing history on mobile phone (see Section 3).

2. USING PERSONAL INFORMATION STORED IN A MOBILE PHONE

In general, a user and her mobile phone may already share some personal knowledge such as 'phone call history' and 'address book' [10, 13]. If this knowledge is private and memorable for the phone owner alone, we can use this for user authentication without a prior agreement them – the phone owner must verify herself by answering the *personal knowledge questions* automatically generated by her mobile phone with the knowledge. This is essentially the same as the existing personal knowledge questions such as "What is your mother's maiden name?" except that we use a simple challenge-response protocol with a dynamically updated shared secret between the phone owner and her mobile phone rather than a fixed password that users must unavoidably choose when creating their accounts. To further clarify our idea, we illustrate by the example in Figure 2.



10:39 PM

Who did you call last?

Phone locked.
Choose the answer to unlock.

H

Hyoungshick Kim

K

Konstantin Beznosov

P

Pooya Jaferian

S

San-Tsai Sun

Displaying 4 contacts

Figure 2: An example of the proposed idea. To unlock the phone, a user tries to choose the correct answer to the question "Who did you call last?" from her contacts.

In this example, the question "Who did you call last?" is designed to test the knowledge about the phone owner's latest call. Probably, the phone owner can remember her latest call while a stranger cannot. We empirically verify this knowledge gap through a small pilot study in the following section.

The most important factor in implementing the proposed idea is to make the guessability (or memorability) gap large between the phone owner and attackers in their answers by finding appropriate personal knowledge questions. Here we consider four types of (potential) attackers with different knowledge levels about the phone owner: 'close family members', 'close friends', 'co-workers' and 'strangers'. If the attacker is a close family member or friend, she might have accumulated some knowledge about the phone owner while a stranger might not at all. We will discuss some evidence on this knowledge gap between the phone owner and these attackers in Section 3.

3. IS THERE A REASONABLE GAP BETWEEN PHONE OWNERS AND POTENTIAL ATTACKERS?

To investigate the feasibility of the proposed idea in Section 2, we conducted a pilot study. The goal of this pilot study was to compare the knowledge levels of people around the phone owner.

An online questionnaire survey was used to collect data. The 17 grid questions (see Appendix A) were carefully used for the 9 major categories of personal information stored in a mobile phone: phone call history, address book, email, text messages, calendar, web browsing history, phone location, photos, and applications. For each question, the participants were asked to rate how likely the participant himself/herself or people around the participant would correctly answer the question about some personal information stored in the participant's mobile phone through a 4-point Likert-scale (Never–Occasionally–Frequently–Always).

We invited the 6 participants in the University of British Columbia; all were graduate students who are studying information security; the 4 participants were males the 25–34 years age group while the other 2 male participants in the 35–44 years age group; the 2 participants used their mobile phones several times an hour, the 3 participants several times a day, and the 1 participant rarely used his mobile phone. The questionnaire results are shown from Figure 3 to 19.

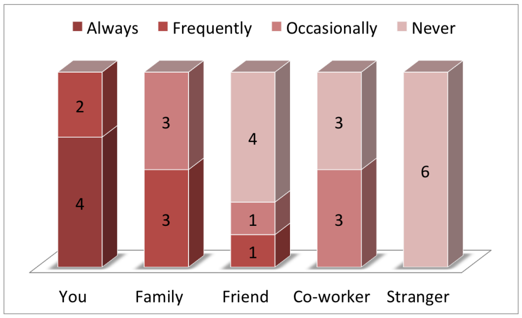


Figure 3: Questionnaire results on the pilot study for knowledge estimation about the most recent call.

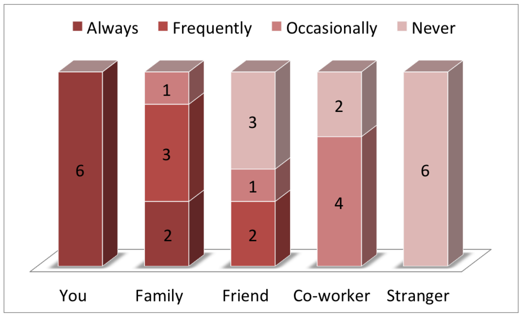


Figure 4: Questionnaire results on the pilot study for knowledge estimation about the most popular call.

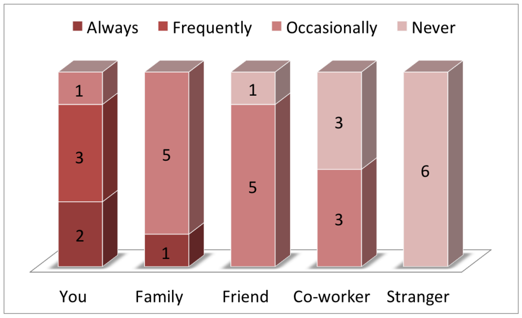


Figure 5: Questionnaire results on the pilot study for knowledge estimation about contact information.

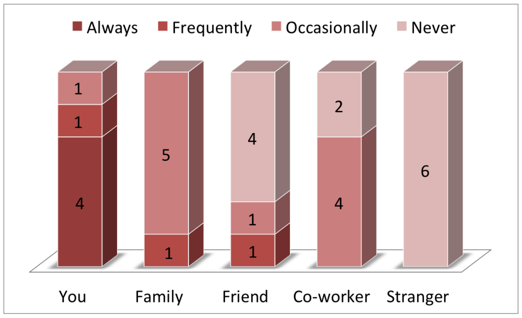


Figure 6: Questionnaire results on the pilot study for knowledge estimation about the most recently used email address.

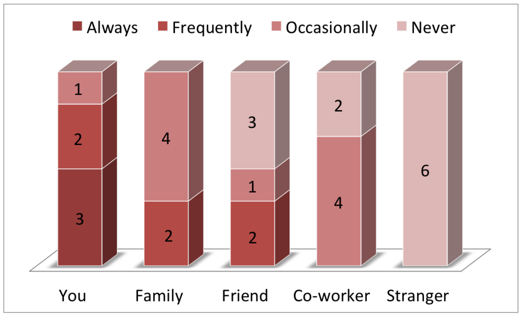


Figure 7: Questionnaire results on the pilot study for knowledge estimation about the most popularly used email address.

For most questions, the knowledge gap is clearly observed between phone owner (i.e. 'You' in the figures) and stranger. In particular, for the knowledge about 'the most popular call' (see Figure 4), 'the most popular location' (see Figure 13), and 'the location at a given time' (see Figure 14), all the participants answered that they can always choose the correct answers for each question while strangers' choices are not better than the random selection. That is, these types of questions might be effectively used to prevent strangers from accessing the participants' mobile phones. We expect that these questions might be effectively used for at least an additional measure with traditional authentication mechanisms (e.g. the use of PINs) to enhance security against strangers.

However, if the threat model includes family members, the phone owner's knowledge about these is not private any-

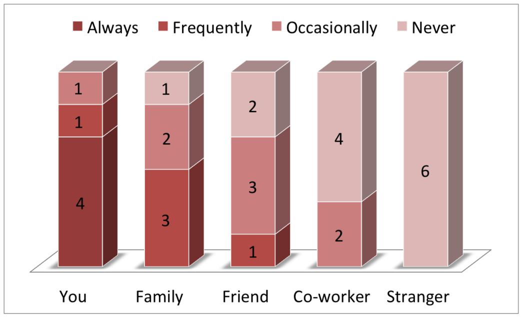


Figure 8: Questionnaire results on the pilot study for knowledge estimation about the most recently used phone number for text message.

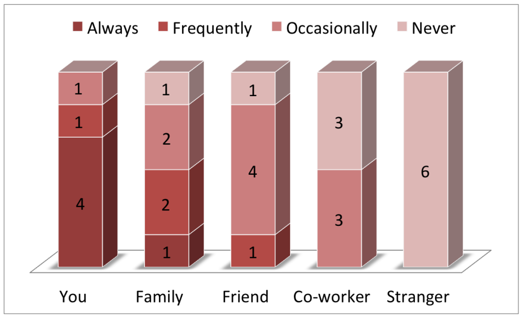


Figure 9: Questionnaire results on the pilot study for knowledge estimation about the most popularly used phone number for text message.

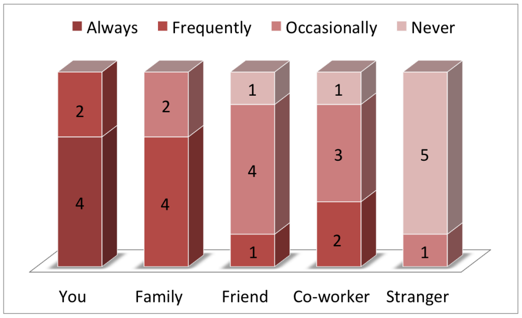


Figure 10: Questionnaire results on the pilot study for knowledge estimation about the most recent event in the callendar.

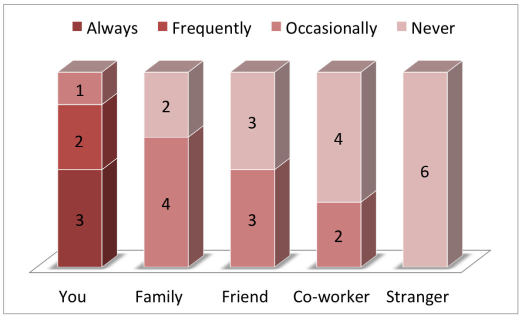


Figure 11: Questionnaire results on the pilot study for knowledge estimation about the most recently visited website using a participant's mobile phone.

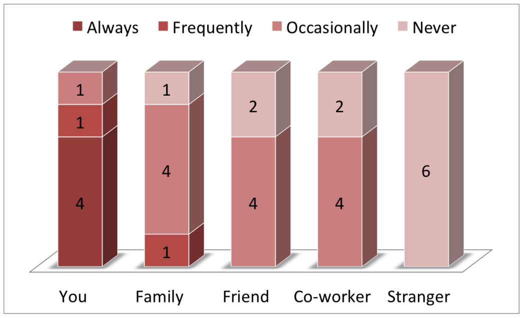


Figure 12: Questionnaire results on the pilot study for knowledge estimation about the most popularly visited website using a participant's mobile phone.

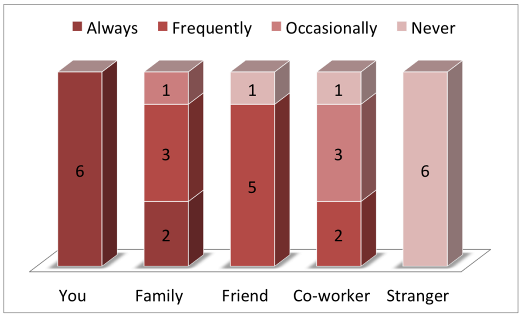


Figure 13: Questionnaire results on the pilot study for knowledge estimation about the most popular location of a participant's mobile phones.

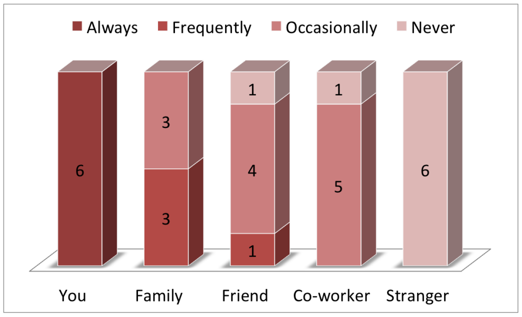


Figure 14: Questionnaire results on the pilot study for knowledge estimation about a participant's mobile phone location at a given time.

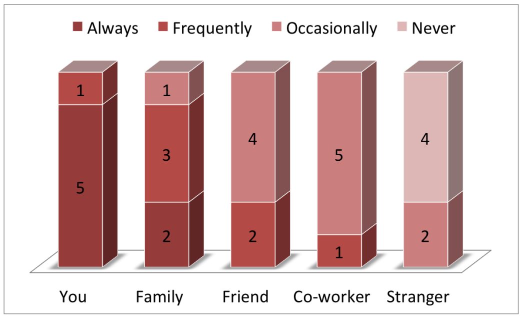


Figure 15: Questionnaire results on the pilot study for knowledge estimation about the tag information on a given photo.

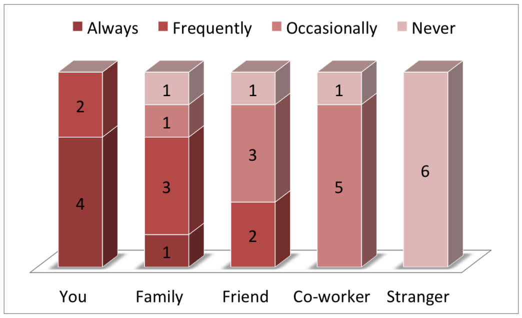


Figure 16: Questionnaire results on the pilot study for knowledge estimation about the time information on a given photo.

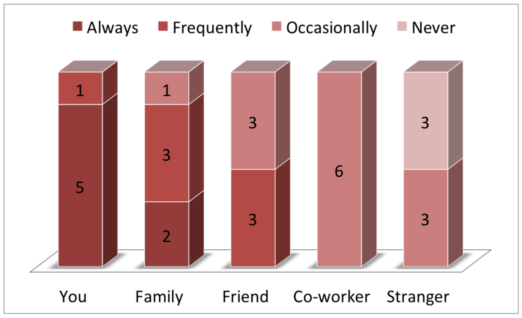


Figure 17: Questionnaire results on the pilot study for knowledge estimation about the location information on a given photo.

more – we can see that a close family member might guess the answers correctly with a high probability; Figure 4 and 13 show that the participants' close family members might sometimes choose the correct answers to the questions for the knowledge about 'the most popular call' and 'the most popular location' (Always: 2, Frequently: 3, Occasionally: 1, Never: 0). Surely, this is a limitation of personal knowledge questions; it is hard to identify memorable knowledge that people hold privately against their close family members since their personal stories are frequently shared with their family members. Note that people who most want to intrude on our privacy are likely to be in our own social circle (e.g. ex-spouse). So, for the purpose of user authentication, these questions would not be our top recommendation.

Our top recommendation against insider attackers would be to use the questions about applications (see Figure 18 and 19) and web browsing history (see Figure 11 and 12) on mobile phone. In particular, the use of questions about applications used in mobile phones provided a better mobile phone protection against not only insider attackers such as close family members (Always: 0, Frequently: 0, Occasionally: 6, Never: 0) but strangers (Always: 0, Frequently: 0, Occasionally: 0, Never: 6) as shown in Figure 11 and 12. This implies that we might design proper personal knowledge questions for user authentication when we use the knowledge about the used applications. For example, a user may be asked to answer more than one challenge (e.g. the most popularly/recently used application) since increasing the number of questions will lead to an exponential decrease in an adversary's guessing probability. Also, we

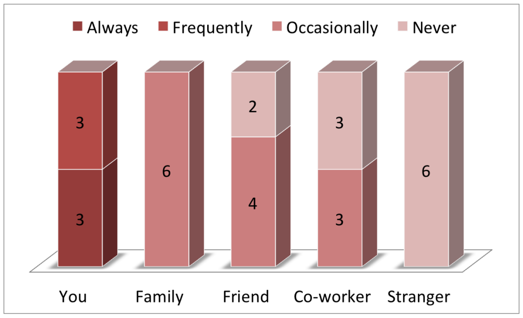


Figure 18: Questionnaire results on the pilot study for knowledge estimation about the most recently used application.

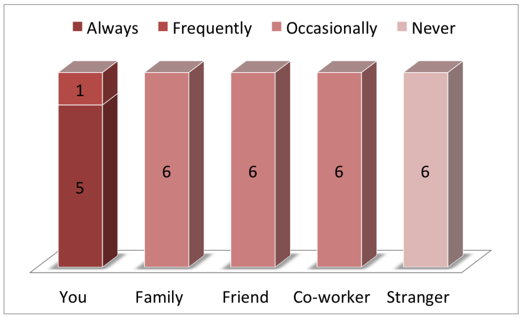


Figure 19: Questionnaire results on the pilot study for knowledge estimation about the most popularly used application.

might test more detailed knowledge (e.g. the most recently used application and then the used time of the application last). Therefore we need to consider extending our work to designing proper questions for user authentication as important lines for future work.

We might want to use images (i.e. the phone owner's photos) instead of asking a user to answer a text-based question since image-based challenges might be made less bothersome to users. Not surprisingly, however, the questions with a photo would be less effective in decreasing the probability of guessing attacks (see Figure 15, 16 and 17). Probably, a given photo in a challenge question would give hints to correctly guess the answer to the question. So, unlike the other types of questions, participants thought that strangers' choices are better than the random selection when the knowledge about a photo is asked (see Figure 15 and 17). Moreover, an attacker can easily collect the information about the given photo through search engine (e.g. "Google Image Search"). Considering how easy it is to collect the information about photos, the use of photos would not be our recommendation.

4. RELATED WORK

Originally, personal knowledge questions were introduced under the belief that a user's personal information can be stored securely in her long-term memory without imposing the burden of memorizing secrets on the user. Despite studies demonstrating weak security, personal knowledge questions have been popularly used for password recovery as a fallback for password authentication.

Zviran and Haga [16] proposed the use of personal knowledge questions for user authentication and discussed how well other people might be able to guess the answers to personal knowledge questions through a user study. Their user study showed that the participants' spouses guessed 33% of the correct answers to the personal knowledge questions about the participants. Schechter et al. [9] confirmed this through another user study – users' acquaintances were able to guess 17% of the participants' answers within 5 guesses. In addition, they showed that the participants didn't remember 20% of their own answers within six months. This implies that personal knowledge questions (e.g. names of relatives, names of schools attended) are very vulnerable with respect to targeted attacks. An acquaintance can impersonate a victim by exploiting knowledge of her personal details [2].

Unlike conventional personal knowledge questions with fixed answers, we discuss a novel type of personal knowledge questions which are dynamically and implicitly updated over time even if there is no a prior agreement between the prover and the verifier of questions. To achieve a similar goal, Yardi et al. [14] proposed a framework using social networks to authenticate users via their knowledge to identify friends from given photos. However, the use of the knowledge about friends might not be a good idea for authentication – Kim et al. [8] showed that being able to recognize friends is not effective against frenemies within a victim's social circle. Our work is an extension of the studies described here: instead of the knowledge about friends, the focus is on the personal knowledge stored in a mobile phone and studying what types of knowledge could be used for user authentication through a pilot study.

5. CONCLUSION AND FUTURE WORK

We proposed an interesting idea to develop a secure and usable user authentication scheme for mobile phones. The main idea is that the phone owner's personal information such as 'phone call history' and 'address book' might already be stored in her mobile phone. In terms of privacy concerns, we always claim that personal information stored on mobile phone should be protected since it is highly private and sensitive information to outsiders [6, 15]. This implies that some information stored inside a user's phone is private. We are wondering whether this personal information is not only private enough against guessing attacks but easily memorable for the phone owner.

We performed a pilot study to show the feasibility of this idea. We discussed the possible knowledge levels of users (the phone owner: `OW`, close family members:`FA`, close friends: `FR`, co-workers: `CO` and strangers: `ST`). Table 1 shows our observation.

This brief observation shows that personal knowledge questions based on private information stored in a mobile phone may be effective against pure strangers. However, against close enemies (e.g. the phone owner's spouse) who share much information with the phone owner, these questions are much less effective. To overcome this weakness, a possible approach is to use a combination of different types of personal information (e.g. applications and web browsing history), a series of more detailed related questions (e.g. the most recently used application and then the used time of the application last) and/or other specific knowledge such as 'most recently listened songs' and 'most recently read books' since it will lead to an exponential decrease in the probabil-

Table 1: Possible knowledge levels of the phone owner (`OW`), family members (`FA`), friends (`FR`), co-workers (`CO`) and strangers (`ST`) for the nine major categories of information stored in a mobile phone. For improved visualization, the level for each item is averaged over the participants in the pilot study.

Information	Question	`OW`	`FA`	`FR`	`CO`	`ST`
Phone call history	Latest	●	◐	○	○	
	Popularity	●	◐	○	○	
Address book	Attributes	◐	○	○	○	
Email	Latest	●	○	○	○	
	Popularity	◐	○	○	○	
Text messages	Latest	●	○	○		
	Popularity	●	◐	○	○	
Calendar	Latest	●	◐	○	○	
Web browsing history	Latest	◐	○	○		
	Popularity	●	○	○	○	
Phone location	Popularity	●	◐	◐	○	
	Time	●	◐	○	○	
Photos	Tag	●	◐	○	○	
	Time	●	◐	○	○	
	Location	●	◐	◐	○	○
Applications	Latest	●	○	○	○	
	Popularity	●	○	○	○	

●=always; ◐=frequently; ○=occasionally;*no-circle*=never.

ity of successfully guessing the answers. To explore what types of questions might give a good balance between memorablity and security in a practical environment, we plan to conduct an intensive user study.

6. ACKNOWLEDGMENTS

We thank members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) who participated in the pilot study and provided valuable feedback on the earlier drafts of this paper.

7. REFERENCES

[1] R. Anderson. Can we fix the security economics of federated authentication? In *SPW 2011, 19th International Workshop on Security Protocols*, London, UK, Mar. 2011.

[2] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *2012 IEEE Symposium on Security and Privacy*, May 2012.

[3] J. Bonneau, S. Preibusch, and R. Anderson. A birthday present every eleven wallets? The security of customer-chosen banking PINs. In *FC '12: Proceedings of the the 16th International Conference on Financial Cryptography*, March 2012.

[4] N. Clarke and S. Furnell. Authentication of users on mobile telephones – a survey of attitudes and practices. *Computers I& Security*, 24(7):519–527, 2005.

[5] D. Davis, F. Monrose, and M. K. Reiter. On user choice in graphical password schemes. In *Proceedings of the 13th conference on USENIX Security Symposium*, pages 151–164, Berkeley, CA, USA, 2004. USENIX Association.

[6] A. K. Karlson, A. B. Brush, and S. Schechter. Can i borrow your phone?: understanding concerns when sharing mobile phones. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, pages 1647–1650, New York, NY, USA, 2009. ACM.

[7] H. Kim and J. H. Huh. Pin selection policies: Are they really effective? *Computers I& Security*, 2012.

[8] H. Kim, J. Tang, and R. Anderson. Social Authentication: Harder than it Looks. In *FC '12: Proceedings of the the 16th International Conference on Financial Cryptography*, March 2012.

[9] S. Schechter, S. Egelman, and R. W. Reeder. It's not what you know, but who you know: a social approach to last-resort authentication. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, pages 1983–1992, New York, NY, USA, 2009. ACM.

[10] T. Sohn, K. A. Li, W. G. Griswold, and J. D. Hollan. A diary study of mobile information needs. In *Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, CHI '08, pages 433–442, New York, NY, USA, 2008. ACM.

[11] X. Suo, Y. Zhu, and G. S. Owen. Graphical passwords: A survey. In *Proceedings of the 21st Annual Computer Security Applications Conference*, ACSAC '05, pages 463–472, Washington, DC, USA, 2005. IEEE Computer Society.

[12] J. Thorpe and P. C. van Oorschot. Human-seeded attacks and exploiting hot-spots in graphical passwords. In *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, pages 8:1–8:16, Berkeley, CA, USA, 2007. USENIX Association.

[13] L. Ventä, M. Isomursu, A. Ahtinen, and S. Ramiah. "my phone is a part of my soul" - how people bond with their mobile phones. In *Proceedings of the Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, UBICOMM '08, pages 311–317, Washington, DC, USA, 2008. IEEE Computer Society.

[14] S. Yardi, N. Feamster, and A. Bruckman. Photo-based authentication using social networks. In *WOSP '08: Proceedings of the first Workshop on Online Social Networks*, pages 55–60, New York, NY, USA, 2008. ACM.

[15] Y. Zhou, X. Zhang, X. Jiang, and V. W. Freeh. Taming information-stealing smartphone applications (on android). In *Proceedings of the 4th international conference on Trust and trustworthy computing*, TRUST'11, pages 93–107, Berlin, Heidelberg, 2011. Springer-Verlag.

[16] M. Zviran and W. J. Haga. User authentication by cognitive passwords: an empirical assessment. In *Proceedings of the fifth Jerusalem conference on Information technology*, JCIT, pages 137–144, Los Alamitos, CA, USA, 1990. IEEE Computer Society Press.

APPENDIX

A. USER QUESTIONNAIRE

Table 2: User questionnaire of the 17 grid questions with X = 'you', 'a close family member', 'a close friend', 'a co-worker', and 'a stranger'. For each question, the participants were prompted to estimate the likeness of the event described in the question using a 4-point Likert-scale (Never–Occasionally–Frequently–Always).

1. When we show the most "recently" used phone number and 4 randomly selected other phone numbers from your phone call history, can X choose the most "recently" used phone number (better than random selection)?

2. When we show the most "frequently" used phone number and 4 randomly selected other phone numbers from your phone call history, can X choose the most "frequently" used phone number (better than random selection)?

3. When we show a randomly selected contact's phone number from your address book, can X choose the contact's name from among five answer choices (better than random selection)?

4. When we show the most "recently" used email address and 4 randomly selected other email addresses from your emails, can X choose the most "recently" used email address (better than random selection)?

5. When we show the most "frequently" used email address and 4 randomly selected other email addresses from your emails, can X choose the most "frequently" used email address (better than random selection)?

6. When we show the most "recently" used phone numbers and 4 randomly selected other phone numbers from your text messages, can X choose the most "recently" used phone numbers for text messages (better than random selection)?

7. When we show the most "frequently" used phone numbers and 4 randomly selected other phone numbers from your text messages, can X choose the most "frequently" used phone number for text messages (better than random selection)?

8. When we show the most "recent" event and 4 randomly selected events from your calendar, can X choose the most "recent" event (better than random selection)?

9. When we show the most "recently" visited website and 4 randomly selected other websites from your web browsing history, can X choose the most "recently" visited website (better than random selection)?

10. When we show the most "frequently" visited website and 4 randomly selected other websites from your web browsing history, can X choose the most "frequently" visited website (better than random selection)?

11. When we show the most "frequently" located mobile phone's location and 4 randomly selected other locations from your mobile phone's location history, can X choose the most "frequently" located mobile phone's location (better than random selection)?

12. When we show a randomly selected specific time within a few days, can X choose the mobile phone's location at the time from among five answer choices (better than random selection)?

13. When we show a randomly selected photo (with tags) from your photo album, can X choose the correct tag from among five answer choices (better than random selection)?

14. When we show a randomly selected photo (with time) from your photo album, can X choose the correct time of taking the photo from among five answer choices (better than random selection)?

15. When we show a randomly selected photo (with location) from your photo album, can X choose the correct location for taking the photo from among five answer choices (better than random selection)?

16. When we show the most "recently" used application and 4 randomly selected other applications from your application history, can X choose the most "recently" used application (better than random selection)?

17. When we show the most "frequently" used application and 4 randomly selected other applications from your application history, can X choose the most "frequently" used application (better than random selection)?