Preliminary Findings from an Exploratory Qualitative Study of Security-Conscious Users of Mobile Authentication

Flynn Wolf
Department of Information Systems
UMBC
Baltimore, MD 21250
flynn.wolf@umbc.edu

Ravi Kuber
Department of Information Systems
UMBC
Baltimore, MD 21250
rkuber@umbc.edu

Adam J. Aviv
Department of Computer Science
USNA
Annapolis, MD 21402
aviv@usna.edu

ABSTRACT
Authentication on mobile devices is a research priority for the development of usable and trustworthy platforms. However, users may struggle to understand how to balance security and usability for the broad range of important data-driven social and financial transactions on their devices. This concern is especially prevalent in security information workers sensitized to mobile technology vulnerabilities by information about security risk. The purpose of this study is to better understand the mental models and practices of those security conscious users from academia, industry, and government, from an explorative qualitative approach, noting that mobile authentication studies have largely overlooked the mindset of users who have considered their behavior in terms of detailed knowledge of risk. A preliminary analysis of findings is presented in this paper. Participants described usability and situational impairment issues, and concern for data security arising from highly contextual combinations of technology and situational risk. Implications for development of security methods derived from these views are discussed, such as the need for authentication rigor to be driven by more contextualized understanding of task and location-based risk.

CCS Concepts
• **Human-centered computing → Empirical studies in HCI**

Keywords
Authentication; empirical study; mobile technology; security

1. INTRODUCTION
As more data driven functions of everyday life transfer onto mobile platforms, authentication of user credentials becomes more important to protecting sensitive user information and maintaining trust in mobile systems. The mental models of the underlying mechanisms of authentication and mobile communication, and the changes in usage behavior they produce may be a significant influence in how users choose, use, and maintain mobile platforms such as smartphones, tablets, or wearables as part of their personal and professional activities. Many authentication studies draw upon available populations that may be skewed towards knowledge of IT and comfort with mobile consumer services, but not necessarily include direct understanding of mobile authentication involved in their activity across multiple services, networks, and devices. The influence that concern may have on the behavior of threat-conscientious users should offer insight into how authentication may better serve the needs of everyday users. The intent of this inquiry is to elicit authentication experiences and opinions from security conscious participants who have engaged in a deliberate balancing act between usability and security in accessing networked personal data.

To address these perspectives, our study drew upon a sample of nineteen industry, government, and academic practitioners. We have defined "security conscious" as those who have learned about mobile security in those professional venues, and modified or reconsidered their own authentication behavior as a result. The study was initiated with a broad set of research questions, addressing security aware users' models of mobile authentication. In response, users offered rich description of their conceptualization of experiences and motivations, and from this two challenges to mobile authentication were derived. Firstly, participants identified authentication behavior as part of a larger effort to control access to their data, which was hampered by doubt about underlying mobile technology, and, secondly, doubt existed regarding the intentions of major mobile technology providers that supply devices and software. These challenges are the basis for several design implications for authentication, such as how authentication might better adapt to users' task-related data sensitivity and circumstantial usability and security needs.

2. RELATED WORK
Mental models were made a central concept to human factors research by Donald Norman [10], and are an important framework for describing user behavior in complex domains, such as mobile security. Several studies have explored how users of IT conceptualize its functionality and vulnerabilities. Volkamer and Renaud [14] identified the potential value in aligning users' mental models of security enhanced systems with key points of interaction, but noted the difficulties in discovering and describing those security models. Bravo-Lillo et al. [2] found that expert users of security warnings differed from novices in how they interpreted context and chose to respond to the warnings, based upon their more detailed expert models of risk. Kang et al. [6] also estimated motivations for security conscious behavior, finding that advanced mental models of the Internet did not translate into more secure habits. Similarly, Friedman et al. [5] surveyed Internet users from rural, suburban, and high tech sectors of the United States regarding web security features, such as firewalls and encryption, finding all three were generally bad at both interpreting security features and articulating accurate models of security technologies. Ur et al. reached similar conclusions about typical user perceptions of password strength,

concluding that many weaknesses were not well understood. Offering specific suggestions for improving password strength during authoring was deemed a useful affordance [13]. Karatzouni et al. [7] probed smartphone users' understanding of security through a focus group, finding concern dependent on the work being done, and little use of authentication unless dictated by risk. Adams and Sasse also examined the user mental models that impact password-based authentication, finding many approaches much less secure than assumed. Users circumvented security procedures due to misunderstanding or because of issues such as recall, indicating that greater human factors consideration would mitigate some usability problems [1]. In contrast, Renaud et al. [11] found that university-aged Computer Science students had incomplete models of email security risks and encryption methods, suggesting that relevant mental models would need reform before users would use safeguards. Ferreira et al. [4] also surveyed university Android users, finding poor understanding of app security issues. Lin et al. [8] approached the same issue, assessing user acceptance of app actions, based upon "privacy nutrition labels."

While prior mobile authentication related studies offer critical insight into the relationship between security and usability, a need has been identified for further investigation specifically examining the mental models and behaviors of security conscious mobile IT users. We conducted an explorative quantitative study into this line of inquiry.

3. METHOD

Data collection for this study was conducted using semi-structured interviews and direct observation. These methods were selected to afford flexible, in-depth questioning regarding complex and variable authentication behaviors and their underlying mental models of risk and technical functionality. An interview question instrument was piloted, and iterated to improve efficacy and address emergent themes. Topics included information about participants' basic demographics and mobile authentication usage. Questions also focused on authentication attitudes and goals, confidence in their own security habits, experience and concern with different threats, rationales for differing habits, and perceived downsides to security conscious behavior. Grounded theory was used for purposes of analysis.

3.1 Participant Sampling

Sampling participants with the requisite experience with security issues was a priority given the focus of this study. "Snowball sampling" was a key approach to addressing this challenge, using direct referrals by participants. Participants were also recruited from speakers at university information security student group events, ads placed on university IT security groups, and through direct solicitation and introductions through the Los Angeles Information Systems Security Association (ISSA) chapter at the 2015 Annual Computer Security Applications Conference (ACSAC). Nineteen participants were interviewed, primarily between the ages of 35-44 years, including 3 females.

3.2 Methods of Analysis

Interview data was first reviewed as notes to sensitize to any themes or observations apparent at the time of the conversation, and to inform research memos as an internal record of the research decision making process [3]. After a comparative review of several of the initial transcripts, a choice was made to open code at a moderate level of granularity that would support focus on the research questions that mostly closely related to the motivations of security-conscious users. A shorter, more abstract set of codes was deemed appropriate, and were compared for a combinative set of axial codes which would coalesce the common themes between participants [9]. Findings from a preliminary analysis of the data are presented in this paper. Further analysis is underway.

4. DISCUSSION

4.1 Risk management through a contextual threat model

When asked to describe their thought process behind decisions about mobile authentication, the majority of participants mentioned a balance they try to create between strict security procedures that impose time and access penalties, and the need to permit a reasonable amount of network access and activity (n=18). This negotiation of priorities against a well-articulated mental model of mobile security vulnerability was often carried out by participants (n=10) with the stated understanding that ultimately, against determined adversaries, "*no device is secure*" and that "*everything can be hacked* (P19)." Often, participants based this balance on a mental model of the threat to their data security. These threat models were described in great detail and with abundant context. This context included common risks, such as shoulder surfing or theft of a physical device, that would likely be familiar to all mobile users. However, in almost all cases the individual model of risks to mobile authentication also included more sophisticated concepts that reflected the experience of security information workers, such as keyloggers from email-attached malware, compromised applications downloaded from app stores, and spoofed cell towers, password manager sites, or public wireless connections. Additionally, the severity of these threats was modulated for participants by their knowledge of the types of potentially sensitive data access required to carry out specific tasks on their mobile devices, and how dire the potential consequences of compromise of that data could be. This mental model of how a task and its associated personal data might relate to security threats forms the basis of a design implication, discussed later (Section 4.5), that suggests considering authentication as a layered process informed by the same view of contextual risk.

4.2 Drawbacks, and frustration with security-conscious behavior

Participants reported numerous frustrations with authentication generally, and unfavorable consequences to their contextual threat model. Participants disliked the usability impacts imposed by frequently entering long, complex passcodes, as well as the penalties associated with limiting the number of authentication attempts allowed before locking an account (P17). Opinions on biometric methods such as fingerprint readers varied, with some hopeful about their impact and others concerned with the potential long term implications of their biometric credentials being compromised. Many also related to strictly limiting types of data stored on their mobile devices, or uploaded to cloud services. Participants also avoided many common mobile activities in order to satisfy their desire to more fully protect their user credentials. Avoiding features such as password manager sites, single sign-on, and browser password-caching (P17), or use of location services (P14) were reported, as well as generally trying to

"*compartmentalize*" (P16) by not tying mobile accounts to services. Similarly, in pursuit of "*security through obscurity*" (P16), participants frequently described limiting or avoiding use of social media and location-based features.

4.3 Password strategies

How security information workers' threat models might change was described both directly and indirectly. For example, several participants described how their methods for creating passwords had changed over time (n=7). One participant (P17) related that "*back in the Nineties*" he would have been comfortable using dictionary words as passwords, but had felt compelled over time by reports of more pervasive and sophisticated threats to progressively strengthen his strategies, making terms longer and more alphanumerically complex. Similar to observations made by Adams and Sasse [1] in their study of password behavior, this participant volunteered that he kept physical cheat sheets of passwords. He was well aware that this cheat sheet coping behavior violated common security advice, but deemed it necessary to maintain the large volume of passwords he required.

4.4 Challenges to Mobile Authentication

Security conscious users described numerous concerns regarding their mobile authentication which were rooted in their own behaviors, such as how they managed untrusted network connections or authored strong passcodes (such as choice in their length, character types, and recall cues). However, seventeen participants also related at length their worries over how underlying weaknesses in the security of the device or network architectures which might undermine their authentication. These weaknesses were often deemed beyond the control of their own choices or behavior, and led participants to limit their usage of mobile technology rather than trust authentication. Further, participants often expressed distrust of major hardware and software makers to support trusted authentication via mobile technologies.

4.4.1 Concern with Underlying Device and Network Architecture Beyond Authentication

A clear point of consensus between seventeen participants, based upon varying aspects of their individual models of authentication's role in security, was concern for the underlying architectures of their mobile devices. This finding reconciles with existing research on the functional focus of expert mental models of security [6]. This concern was exacerbated in several cases by common situational impairments and physical threats, such as worry over shoulder surfing attacks.

4.4.2 Distrust of Major Software and Hardware Companies

Eleven participants also shared pointed doubts about the motivations of commercial mobile software and hardware makers involved in authentication and security, such as Apple and Google, to fully protect their customers' credentials and data. This resulted in a reluctance to authenticate using mobile devices in order to undertake tasks while on-the-go. However, another participant (P15) felt that rather than major mobile technology companies deliberately weakening user control of personal information for profit, widespread authentication failures and data loss were more simply attributable to shortsighted reluctance in many industries to make costly security investments a business priority, and substantive improvement in mobile data security was deemed unlikely.

4.5 Implications for Mobile Authentication

Participants described a number of aspects of their device security and authentication which they would like to see improved (Section 4.4.1). Participant 7 indicated that when he was in what he considered to be a more threatening environment, such as a public space with insecure wireless networks, he chose to elevate the number of notifications provided by monitoring software he installed on his mobile device. Similarly, he stated that his wish for improved mobile authentication would include being able to quickly toggle from a convenient low security mode, such as a biometric method, to a more rigorous high security mode, such as a password, when he felt security threats were increasing.

These observations carry several implications for authentication developers. Firstly, and most basically, all security conscious users interviewed saw threats to their mobile-based identity and data authentication as a real problem that strongly influenced their decision making and everyday behavior. In this regard, they may foreshadow greater concern in consumers of mobile services as a whole, whether affected directly by identity theft or not, towards managing their authentication more carefully. This may be portrayed in either informed buying choices motivated by concern for the security of operating systems (Section 4.4.2), or choices in selecting and using applications (Sections 4.1, 4.3, and 4.4.1). Secondly, as discussed in Section 4.1, risks to mobile authentication, as articulated by the participants, were seen as a frequently changing product of multiple risk factors, such as device hardware, user behavior, sensitive data involvement, and situational circumstances. Participant 8, for instance, reflected this in choosing to be more careful with his online banking habits, stating, "*My security conscience kicks in depending on the type of information* [being used on his Android mobile device]. *I usually try more to protect my economic side*."

To manage their own mobile authentication risk based upon the type of data being exposed, some security conscious users wanted more granular insight and control of processes on their devices. For example, Participant 3 demonstrated using a network analysis application on his tablet to characterize the dozens of open wireless connections in his surroundings, and to observe the connections made by other apps he had installed. He explained that being able to see this extra information motivated additional cautious behaviors, such as using strong authentication, controlling individual service permissions given to applications, and his refusal to load many common mobile applications that he felt would risk his credentials. Participant 13, a CTO for a security systems integration company, predicted a similar response to authentication challenges in the future for himself and other security conscious users. He felt these users would "*dig in their heels*" to be the "*back of the pack*" in adopting new technology that might undermine their ability to control their own devices and the information they collect, so as to "*dilute*" the "*correlatable ability between platforms*." As an implication, security conscious users in this regard might well be suggestive of users who may want more ability to configure "under the hood" of their device processes, such as what specifically the device tells the user about changes in the use of their persona-based services or stored authenticated data. This desire may be a challenge to "walled garden" approaches that would instead restrict user control.

Additionally, as discussed in Section 4.2, a number of participants described their interest in context-sensitive authentication, which would allow them to either manually toggle to a higher level of security (with an assumed penalty of less convenience) when in riskier circumstances, and to have some of this process automated. In the case of automation, participants described mobile devices potentially using behavioral or network analysis to establish when the device was in a safe place, and then switch automatically to less rigorous but more convenient authentication methods to avoid interrupting the user. For designers of mobile services, and especially for new authentication methods, consideration would need to be given to the usability impact of modal shifts [12] based upon the user's activity and circumstances (such as situational impairments or network connections).

5. CONCLUSION AND FUTURE WORK

The participants interviewed in this study described many tradeoffs in their mobile authentication behavior between ease of use and the desire to protect their important data, and elaborated on the frustrations this introduces. Additional insights drawn from these perspectives suggest mobile authentication researchers and developers consider passcode methods that more fully reflect and adapt to the situations and activities of users with informed models of data security risk.

Further qualitative research of this topic would endeavor to more fully characterize answers to how security conscious users develop and maintain their models of this risk, overcome situational impairments to authentication, and extrapolate how these experiences could be transferred to other users of mobile technology.

6. ACKNOWLEDGEMENTS

This work was supported by the Office of Naval Research (N00014-15-1-2776).

7. REFERENCES

1. Adams, A., & Sasse, M. A. (1999). "Users are not the enemy," *Communications of the ACM*, *42*(12), 40-46.
2. Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2010). "Bridging the gap in computer security warnings: A mental model approach," *IEEE Security & Privacy*, (2), 18-26.
3. Corbin, J., & Strauss, A. (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage Publications.
4. Ferreira, D., Kostakos, V., Beresford, A. R., Lindqvist, J., & Dey, A. K. (2015). "Securacy: an empirical investigation of Android applications' network usage, privacy and security," In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, Article 11.
5. Friedman, B., Hurley, D., Howe, D. C., Felten, E., & Nissenbaum, H. (2002). "Users' conceptions of web security: a comparative study," In *CHI'02 extended abstracts on Human factors in computing systems*, 746-747.
6. Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "'My Data Just Goes Everywhere:' User mental models of the internet and implications for privacy and security," In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, 39-52.
7. Karatzouni, S., Furnell, S. M., Clarke, N. L., & Botha, R. A. (2007). "Perceptions of user authentication on mobile devices," In *Proceedings of the ISOneWorld Conference,* 11-13.
8. Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012). "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing," In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 501-510.
9. Merriam, S. B. (2015). *Qualitative research: A guide to design and implementation* (4th Ed.). John Wiley & Sons.
10. Norman, D. A. (2013). *The design of everyday things: Revised and expanded edition*. Basic Books.
11. Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). "Why doesn't Jane protect her privacy?," In *Privacy Enhancing Technologies*, 244-262. Springer International Publishing.
12. Sklar, A. E., & Sarter, N. B. (1999). "Good vibrations: Tactile feedback in support of attention allocation and human-automation coordination in event-driven domains," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *41*(4), 543-552.
13. Ur, B., Bees, J., Segreti, S., Bauer, L., Christin, N., Cranor, L., & Deepak, A. (2016). "Do users' perceptions of password security match reality?," In *Proceedings of the 2016 ACM Conference on Computer-Human Interaction*, 3748-3760.
14. Volkamer, M., & Renaud, K. (2013). "Mental models–general introduction and review of their application to human-centred security," In *Number Theory and Cryptography*, 255-280. Springer Berlin Heidelberg.