Behaviour & Information Technology

ISSN: 0144-929X (Print) 1362-3001 (Online) Journal homepage: https://www.tandfonline.com/loi/tbit20

An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication

Flynn Wolf, Ravi Kuber & Adam J Aviv

To cite this article: Flynn Wolf, Ravi Kuber & Adam J Aviv (2018) An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication, Behaviour & Information Technology, 37:4, 320-334, DOI: 10.1080/0144929X.2018.1436591

To link to this article: https://doi.org/10.1080/0144929X.2018.1436591

Published online: 15 Feb 2018.

BEHAVIOUR & INFORMATION TECHNOLOGY, 2018
VOL. 37, NO. 4, 320–334
https://doi.org/10.1080/0144929X.2018.1436591

Taylor & Francis
Taylor & Francis Group

An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication

Flynn Wolf[a], Ravi Kuber[a] and Adam J Aviv[b]

[a]UMBC, Baltimore, MD, USA; [b]USNA, Annapolis, MD, USA

ABSTRACT

The purpose of this study is to better understand, from an explorative qualitative perspective, the motivations and practices of highly security-conscious users of mobile authentication, and their underlying mental models of those behaviours. Mobile authentication studies have largely overlooked the mindset of these users in the upper bound of security experience, who have considered their behaviour in terms of detailed knowledge of mobile authentication risk. Twenty IT professionals who self-identified as security-conscious mobile device users, many with decades of intensive security-specific experience, were interviewed for this study regarding their opinions and experiences with mobile device authentication and security. These users described usability and situational impairment issues, as well as a deep concern for their identity and data security arising from highly contextual combinations of distrust towards underlying technologies and situational risk. Derived implications for development of security methods adapted to these informed perspectives are discussed and will be the basis for follow-on research comparing these findings with everyday users.

ARTICLE HISTORY
Received 28 March 2017
Accepted 29 January 2018

KEYWORDS
Empirical study; mental models; mobile device authentication practices; security-conscious mobile device users

1. Introduction and motivation

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. Furthermore, the user's understanding of how their credentials are verified and protected from compromise is a key aspect of that trust relationship, given the broad array of financial, social, and communication tasks often entrusted to mobile technology. That highly variable understanding forms users' mental models of the underlying mechanisms of authentication, the threat of data loss and theft, the risks inherent in different types of data-driven work, and mobile communication functionality. Advanced models of these aspects of authentication held by security-conscious users may be a significant influence in how security is chosen and applied on mobile platforms such as smartphones, tablets, or wearables as part of their personal and professional activities.

Many authentication studies effectively summarise available 'everyday' populations that may, however, be skewed towards knowledge of IT and comfort with mobile consumer services (Adams and Sasse 1999; De Luca, von Zezschwitz, and Hussman 2009; Harbach et al. 2014; Beautement et al. 2016; Fagan and Khan 2016; Forget et al. 2016; Mare, Baker, and Gummeson 2016), but not necessarily include the experiences of security-focused participants with important aspects of their personal mobile authentication outlook. These aspects include knowledge of mobile IT vulnerabilities, consequences of authentication compromise, and understanding of the technical architectures that support authentication on mobile platforms. These are all likely to be involved in managing a complex series of personal transaction types across multiple networks, services, and devices. Generally, usability needs for authentication have been found to either differ between experts and non-experts in a domain like mobile computing (Whitten and Tygar 1999; Asgharpour, Liu, and Camp 2007; Bravo-Lillo et al. 2010; Schaub, Deyhle, and Weber 2012; von Zezschwitz, Dunphy, and de Luca 2013), or to be inadequate for both populations (Friedman et al. 2002; Ion, Reeder, and Consolvo 2015; Kang et al. 2015). A Consumer Reports survey of 1656 everyday smartphone users found that 64% did not use device authentication at all (Consumer Reports Magazine 2013). We cannot simply infer insights for how authentication may better serve the needs of everyday users from the behaviour of threat-conscientious users influenced by detailed knowledge of these worries. However, this picture of the mental models from a highly security-informed cohort may be both valuable in its own right,

CONTACT Ravi Kuber rkuber@umbc.edu

regardless of transferability to everyday users, as well as suggestive of how to improve design in this domain for an increasing population of more security-aware users.

1.1. Contribution

The intent of this inquiry is to elicit perspectives on mobile authentication and security, specifically from an under-researched cohort of security-conscious participants who have engaged in a deliberate balancing act between usability and security in accessing networked personal data. It is directly motivated by the limited focus to date on the specific challenges and needs of security-conscious mobile users by the research community overall, and particularly to capture these perspectives using a qualitative methodology. The themes derived from these informed users' mental models firstly describe the outlook of an important population of mobile users, and secondly offer insight that should improve the design considerations for relevant authentication methods. The increasing public profile of cybersecurity issues, combined with broadening public acceptance of mobile applications using sensitive personal data (i.e. for communication and banking), may very well provoke broader awareness and demand for greater customisable control of mobile authentication. Certainly, both within the findings of this study, and in broad public concern over data security, the integrity of these processes is a subject of concern. For example, a recent survey found that the percentage of 18–26-year-olds in the United States who recalled reviewing news of a cyberattack in 2016 had almost doubled in one year from 34% to 64%. In the United States, 53% reported that cybersecurity policy mattered in choosing political candidates. Worldwide, the percentage of young adults having received some formal cyber security training increased over the same period from 16% for men to 59%, and increased 40% for women to 51% (Raytheon and National Cyber Security Alliance 2016). Alternatively, semi-autonomous methods that limit user interaction, such as continuous authentication, may propagate (instead verifying a user signature based on historical sensor data and location data, as highlighted by Micallef et al. 2015). In either scenario, insight derived from the mobile authentication experiences of security informed users, like those of this cohort, could help identify needed improvements for the broader, non-expert market of mobile devices and applications, and an increasing population of more security-aware users. A recent industry survey projected as many as 2 million unfilled cybersecurity jobs by 2019 (Intel Security and the Center for Strategic and International Studies 2016), and the United States Bureau of Labor Statistics projects 18% growth in information security jobs from 2014 to 2024, compared to 12% for IT generally and 7% for all types of employment (Bureau of Labor Statistics, U.S. Department of Labor 2015).

The study described in this paper was initiated with a broad set of research questions for users with perspectives on mobile authentication issues including: (a) how risk is defined and managed (Section 4.1), (b) how usability drawbacks-associated advanced security approaches are dealt with (Section 4.2), (c) how such users see their habits interacting with mobile software and hardware (Section 4.3), and (d) what types of challenges security-conscious users face (Section 4.4). To ensure the novelty of this research, these questions focused upon motivations for the security consciousness these participants described, as well as how more recent authentication mechanisms, such as biometric device unlocking, were being incorporated into their behaviour. In response, users offered rich description of their authentication experiences and motivations. Based on those responses, two challenges to mobile authentication are defined. Firstly, participants identified authentication as part of a larger effort to control access to their data, which was hampered by doubt in two forms. Firstly, doubt regarding the underlying mobile technology, and secondly, towards the intentions of major mobile technology providers that supply devices and software. While some of these findings align well with existing qualitative security studies in related domains (described in Section 4.5), we believe documenting them specifically with regard to mobile authentication, with this method and qualified cohort, offers a novel and useful perspective. The participants' challenges are the basis for several design implications for authentication (described in Section 4.6), such as how authentication might better adapt to relevant users' task-related data sensitivity and circumstantial usability and security needs.

2. Related work

2.1. Mental models and IT security

Mental models, such as those held by security-conscious users regarding the use of their mobile devices, were made a central concept to human factors research by Donald Norman. They are an important framework for describing user behaviour in complex domains such as mobile security (Norman 2013). Several studies have explored how users of IT conceptualise its functionality and vulnerabilities (e.g. Friedman et al. 2002; Asgharpour, Liu, and Camp 2007; Karatzouni et al. 2007; Bravo-Lillo et al. 2010; Lin et al. 2012; Ion, Reeder, and Consolvo 2015; Kang et al. 2015; Ur et al. 2016). Volkamer and

Renaud identified the potential value in aligning users' mental models of security-enhanced systems with key interaction points, but noted the difficulties in discovering and describing those security models (2013). Similarly, Asgharpour, Liu, and Camp evaluated expert and naïve mental models of computer security from a risk communication viewpoint, and concluded that those models differed distinctly with expertise, and that security models in the form of common metaphors (e.g. 'viruses,' 'zombies,' or 'keys') did not reconcile well with understanding in either group (2007). Bravo-Lillo et al. defined 'expert' users as having taken a graduate-level security course or worked for at least a year in the field, differed from novices in how they interpreted the context of a set of common security warnings, and how they chose to respond, based upon their more detailed expert models of risk (2010). Similarly, Ion et al. also compared security expert (minimum five years of experience) and non-expert computer users, via online surveys, finding divergence in both practice and opinion regarding many basic security practices. Experts favoured methods such as software updating, two-factor authentication, and password managers, which were disliked by non-experts in favour of using antivirus software and making frequent password changes (Ion, Reeder, and Consolvo 2015). In comparison, Rader et al. surveyed 301 stories about home computer security, focusing on non-expert full-time students. These users found anecdotal security stories, often heard and retold among family and friends, to have persuasive influence on their security practices (Rader, Wash, and Brooks 2012). Rader and Wash later elaborated on this, examining differences in security information from three sources, news articles, peer stories, and web-based security guidance articles. The sources differed in focus when describing threat scenarios. For example, peer stories focused on malicious actors, guidance articles on the details of attack methods, and news articles on consequences for users (Rader and Wash 2015).

Researchers have also examined the ways in which mental models of the Internet differ between expert and non-expert users. Examples include Kang et al., who estimated motivations for security-conscious behaviour, and compared their basis in the mental models in IT-expert and non-expert users. Processing advanced mental models of Internet processes, such as making an online purchase, was found to impart more awareness of privacy risks from government, hackers, or ISPs, but did not translate into more secure habits (Kang et al. 2015). Similarly, Friedman et al. 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 poor at both interpreting security features and articulating accurate models of security technologies (Friedman et al. 2002). Ur et al. reached similar conclusions about typical user perceptions of password strength, concluding that many weaknesses were not well understood, and suggested improving password strength during authoring as a useful affordance (2016). Stobert and Biddle (2014, July) interviewed university non-security expert internet users ($n = 27$) on their password use, applying grounded theory to create a model capturing a gap between user behaviour and tool support. A subsequent study (2015) more specifically used thematic analysis of semi-structured interviews to describe academic and industrial security experts' ($n = 15$) password management. These users were found to split their approach between laxness and caution in password use, based on awareness of risk towards their more sensitive accounts (Stobert and Biddle 2015, December). Ferreira et al. also surveyed university Android users, finding poor understanding of app security issues (2015).

To address these disparities in mobile security awareness, Egelman et al. performed a qualitative study of everyday users recruited through social media, particularly their perception of their screen locking and password use, and the sensitivity of data on their mobile devices. In contrast to other findings described here, security feature adoption was found to be rationally correlated to risk perception. However, users were found to underestimate the data sensitivity of their devices, and 29% did not use device authentication at all. An online survey of 2518 smartphone users found similar results, with 58% using PIN or pattern authentication (Egelman et al. 2014). 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 (Adams and Sasse 1999). In contrast, Renaud, Volkamer, and Renkema-Padmos (2014) 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.

2.2. Expert and non-expert risk perception of networked and mobile computing

Looking at everyday users, Imgraben et al. surveyed university smartphone users ($n = 250$), finding limited awareness of mobile-specific security risks, and occasional unknowing actions that actually compounded

risk (e.g. jailbreaking their devices, then loading unverified applications) (Imgraben, Engelbrecht, and Choo 2014). Mylonas et al. also looked at smartphone usage, and carried out short, structured interviews about mobile app usage with smartphone users recruited in public (n = 458), and categorised participants by their security savviness (having had university information security courses or industrial security certifications). While security experience had a slight impact on caution in app usage, users with and without that perspective were found to have unsafe behaviours such as ignoring privacy controls and prompts, and harbouring misconceptions about app systems. Mylonas et al. point out that in recommendation-based app ecosystems, this type of user behaviour can have harmful effects on other users (2013, August). A number of studies discuss potentially regionally based differences in perception and behaviour towards network and mobile security risk. Diesner, Kumaraguru, and Carley et al. used map analysis techniques to visualise relationships between key constructs present in the transcripts of 29 interviews with Indians, regarding their opinions on security and privacy, finding associations between terms for comparison (2005, May). Brooks used similar mapping analysis to explore the content of expert security courses. Key subordinate themes related to expert security risk management were identified and concept mapped. The concept of threat was found to have high centrality, while important constructs for vulnerability were absent (Brooks 2011). Looking further at non-expert mental models, Wash described eight folk models of hackers and viruses gathered from 33 qualitative interviews conducted in three mid-western cities. These models, gathered from non-security expert home computer users, were found to have potential effects in how those participants might misapply network security advice (Wash 2010, July). Blythe and Camp later explored how these eight models functioned as agent models for simulations of non-expert security behaviour. Adoption of simulated security-conscious behaviours by agents, such as virus scanning or updating software, was found to basically align with responses of people reporting the same models (Blythe and Camp 2012, May).

Looking more specifically at user security behaviour within the context of hierarchical organisations, Safa et al. used structural equation modelling within a theoretical framework to assess the relationship between security-conscious behaviour and organisational policy by information security experts (those with extensive experience) and IT professionals, based on a questionnaire (n = 212), finding that personal experience and knowledge positively influenced behaviour more than external control (2015). Posey et al. also used a theoretical view of the relationship between organisational security professionals and insider IT users on security measure adoption, using semi-structured interviews and thematic coding (n = 33). The authors identify differences between security experts' probabilistic analytic view of risk, versus users emotional and intuitive experiential view. Users were found to be aware of network computing risk from their actions in terms organisational resentment and financial vulnerability imposed on their employer. However, they were less susceptible to fear appeals to better personal security habits than to appeals to shared responsibility with their peers (Posey et al. 2014).

In contrast, Camp surveyed research on the difficulty in transferring that knowledge of security risk. Mental models of risk in medical, physical, criminal, military, or market metaphorical forms are limited in their ability to educate users and produce rational behavioural approaches, such as adopting risk-proportional privacy measures online (Camp 2009). Brase et al. also found that users, when offered a network security scenario presented in terms of common domain metaphors (crime, disease, and physical security), demonstrated similar Bayesian reasoning and responses. This suggested that the design of security warnings and interventions should focus on communicating actual risk and reward issues, rather than use metaphors which are not likely to be predictive of user reactions (Brase, Vasserman, and Hsu 2017). Chin et al. used structured interviews and surveys (n = 60) to review average smartphone users' perception of risk in their mobile device usage. Mobile devices were deemed more risky than other networked computing, and users consequently reported more caution about financial and privacy-sensitive applications. However, the concern was directed mostly at physical loss or damage of the device, with some worry over making mistakes with interfaces. Concern with underlying technical vulnerability was attributable to common misconceptions about network connectivity (Chin et al. 2012, July).

2.3. Threats of observational attacks

Shoulder surfing is frequently cited as a motivating factor for more secure forms of usable interaction in studies dealing with mobile authentication. Worries relating to third parties viewing and recreating passcodes have resulted in researchers investigating this area. Studies have aimed to characterise the real-world prevalence of shoulder surfing (Harbach et al. 2014), which was found to be rarely perceived by mobile users. Studies have also tested novel interaction schemes that might deter observer attacks, such as gesture recognition and tactile cues for distraction gestures (De Luca, von Zezschwitz, and Hussman 2009; De Luca et al. 2012;

Hang, De Luca, and Hussmann 2015). Also, the interaction of usability and security in the passcode entry phase of authentication has been identified as a key relationship and studied (Yee 2002; Aviv and Fichter 2014; Wiese and Roth 2015; Mare, Baker, and Gummeson 2016), including lab-based comparisons of shoulder surfing susceptibility between different types of virtual keyboards (Schaub, Deyhle, and Weber 2012), field studies of grid and PIN passcode entry (von Zezschwitz, Dunphy, and de Luca 2013), as well as cognitive walkthrough studies of encryption software usability (Whitten and Tygar 1999; Warshaw, Taft, and Woodruff 2016). More broadly, research has examined password management habits (Schaub, Deyhle, and Weber 2012; Stobert and Biddle 2014; Melicher et al. 2016, July, Ur et al. 2016; Wash et al. 2016).

While prior mobile authentication-related research offers critical insight into the relationship between security and usability, a need has been identified for further investigation specifically examining the mental models and behaviours of security-conscious mobile IT users. By better understanding the needs of security-conscious users (i.e. those at the upper bound of awareness regarding the integrity of their authentication behaviours), systems can be designed to better support their needs, and all users encountering the need to balance the conveniences of mobile computing with protecting their data. We conducted an explorative qualitative study into this line of inquiry.

3. Methodology

Data collection for this study was conducted using semi-structured interviews and direct observation (detailed in Section 3.2). Transcripts of these interviews were then reviewed with inductive thematic analysis to discern prevalent themes in the discussions (described in Section 3.3). These methods were chosen to afford more flexible, in-depth questioning of participants regarding a very broad subject matter that was deemed likely to elicit detailed and heterogeneous answers.

3.1. Participant sampling

To address security-conscious perspectives on mobile authentication, our study drew upon a sample of industry, government, and academic practitioners. These included highly experienced government and military information security professionals and cyber security educators. We also recruited from researchers and presenters at the 2015 Annual Computer Security Applications Conference (ACSAC). For this study, 'security conscious' includes those who have learnt about mobile security in those professional and academic venues, and then modified or reconsidered their own authentication behaviour. A more specific definition of an 'expert user' is limited by several issues. Many of the participants had individual histories that crossed between professional domains. With this disparate and blended range of backgrounds, defining expertise with a simple comparison of rank or years of experience was deemed insufficient for qualifying the authority of participant responses. Furthermore, four highly technically literate participants volunteered that they were essentially *self-taught* within the field, suggesting that years or level of formal education would also be an incomplete qualifier for expertise. As such, an inclusive definition of 'security conscious' was used in defining the type of participants solicited for participation. Comparable definitions for security expert or security-conscious technology users are described in Section 2.1, such as Bravo-Lillo et al. (those having taken a graduate-level security course or having one year's work experience in the field) (2010), and Ion et al. (a minimum of five years' work experience) (Ion, Reeder, and Consolvo 2015). All but one of the cohort for this study (a security-focused undergraduate university student) would comply with all of these definitions, and the majority far exceed the minimums, several having decades-long careers in penetration testing and network security. In part, this may reflect recruitment in geographic proximity to the Baltimore-Washington area, which has a large and long-standing IT and cybersecurity industrial focus.

Given this study's attention to security-conscious users (versus users with an average sense of mobile technology security issues), sampling participants with relevant experience was a priority. A key sampling approach to address this challenge was 'snowballing' from one participant to their colleagues by direct referral. Participants were also recruited from professional information security associations, speakers at campus information security student group events, ads placed on campus IT security groups, and through direct solicitation and introductions facilitated through the Los Angeles Information Systems Security Association (ISSA) chapter at ACSAC 2015. These participants included highly experienced government and industry security developers and researchers. Twenty participants were interviewed, primarily between the ages of 35 and 44 years, including 3 females (Table 1). All self-identified as being security-conscious mobile device users.

3.2. Semi-Structured interviews

Semi-structured interviews were chosen as the primary data collection method in this study to afford open-

Table 1. Participant demographics.

Participant	Age	Sex	Experience
1	35–44	F	Career government information security (IS), academic IT researcher
2	>65	M	Career government IS officer, industry IS developer, IT educator
3	45–54	M	Security developer, academic IT security educator
4	35–44	M	Career government IS officer, academic IS researcher
5	<21	F	IT security student
6	35–44	M	Government network security researcher, academic IS researcher
7	35–44	M	Academic cybersecurity educator, IS developer
8	35–44	M	Industry mobile security researcher, university IS educator, industry IS developer
9	22–34	M	Academic IS researcher
10	45–54	M	Government IT security researcher
11	45–54	M	Government IT security researcher
12	22–34	M	Academic IT security researcher, government information security officer
13	35–44	M	Industry chief technology officer (CTO) and mobile IS researcher
14	>65	M	Military and government IS developer, academic IS educator, industry IS researcher and developer
15	55–64	M	Government and industry researcher and developer
16	22–34	M	Government IS researcher, academic IS student
17	45–54	M	Government IS developer, academic IS educator and researcher
18	22–34	F	Government IS researcher
19	>65	M	Government and industry IS researcher and developer
20	45–54	M	Mobile security app developer, academic IT security researcher

ended discussion on a defined set of questions, which we felt better suited the subject matter than other related qualitative methods, such as surveys and either informal or highly structured interviews (Merriam and Tisdell 2015). This in-depth questioning was assumed to be important to fairly assessing complex and variable authentication behaviours and their underlying mental models of risk and technical functionality. An interview question instrument was piloted, and then iterated over the course of the interview process to improve the efficacy of knowledge elicitation, based on responses and initial themes. For example, several questions that addressed prior experiences that influenced authentication behaviour and outlook were reordered in the question instrument to reduce redundancy and support exploratory questioning. Member check questions were also added as themes emerged, to bolster the internal validity of conclusions regarding complex opinions. Questioning included information about participants' basic demographics (age and gender) and mobile authentication usage; the types of mobile devices owned (including 'dumb' phones, smartphones, tablets, laptops, fitness wearables, and gaming devices), choice of authentication methods (including PINs, passwords, biometric signatures such as face or fingerprint recognition, and Android grid patterns), and use of other types of mobile security software. Questions also focused on authentication attitudes and goals, confidence in their own security habits, experience and concern and with different types of threats, rationales for habits differing between places and devices, and perceived downsides to security-conscious behaviour. Follow-up questions were used frequently in all interviews conducted for this study. These were essential to clarifying meanings and motivations behind answers with otherwise confounding characteristics (Merriam and Tisdell 2015). Analysis memos were recorded regularly while conducting interviews, to note ideas for improving the efficacy of the interview instrument and any emergent codes (Merriam and Tisdell 2015). As themes were identified, member check questions were also added to support cross-interview thematic comparison.

3.3. Analysis methods

Using inductive thematic analysis (Braun and Clarke 2013), we adopted open coding and a sequential approach to the data analysis of the interviews. During the interviews, analysis memo, and transcription phases, initial codes were established. Deconflicting and combining the codes derived from the transcripts, memos, and notes led to mutually exclusive descriptive themes, which were also iterated by our two reviewers. The final thematic observations are described in the findings.

Interview data were first reviewed as handwritten notes recorded during the interview, to sensitise to any themes or observations that were apparent at the time of the conversation. In many cases, observations were gathered as analysis memos, with the intent of summarising an internal record of the research process, rationales for changes, and to compel continual reflection on emerging themes. Following those steps, interviews were then transcribed. Two researchers independently evaluated a subset of responses to derive a relevant coding taxonomy. 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. The large initial set of research questions, although

relevant to the broad task of qualitative discovery, introduced many responses that did not pertain to motivations or behaviours related directly to authentication. As stated in Merriam and Tisdell, an overly long list of open codes can be suggestive of analysis too rooted in 'concrete description,' rather than descriptive abstraction that may more easily be communicated to an audience (Merriam and Tisdell 2015). Considering this, a shorter, more abstract set of codes was deemed appropriate. These open codes were then compared for a combinative set of axial codes which would coalesce the common themes between participants (Merriam and Tisdell 2015). A second researcher independently coded 15% of all the interviews. This analysis showed a good inter-coder agreement between the two researchers (Cohen's Kappa coefficient (κ) = 0.74), Table 2.

4. Discussion

Themes arising from the analysis include risk management, drawbacks to secure behaviour, and password strategies. These are described below. A subset of preliminary findings are briefly described in (Wolf, Kuber, and Aviv 2016), but are discussed in greater detail in this paper. Other findings which were not covered have also been added.

4.1. Highly contextualised risk management (n = 19)

While all participants regularly authenticated to gain entry to their mobile devices to access applications and data, 19 described assessing risks taking into account the device hardware being used (also discussed in 4.4.1), involvement of sensitive data, and the situation or environment that the interactions would be made in, prior to utilising the device. If risk was thought to outweigh the reward, participants were only too aware of the negative consequences, which were described in detail. Most participants highlighted a balance they try to establish between adherence to strict security procedures when authenticating, which impose penalties in time and convenience, and the need to permit network accesses to perform work (including responses coded for limiting concern about low value data exposure, evaluating risk/benefit trade-offs, and maintaining ongoing models of data security threats). This negotiation of priorities was often carried out in context of a well-articulated mental model of vulnerability in mobile authentication, with participants ($n = 10$) stating that ultimately, against determined adversaries, 'no device is secure' and that 'everything can be hacked (P19).' ' … I never believe there's total security anywhere,' stated Participant 7 (an academic cybersecurity researcher with extensive industry and government information security experience), ' … so I'll never say my security practices are perfect.' The balance was itself often poised by participants upon a mental model of the threat to their data security. These threat models were described in detail, and with abundant context, including 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 professionals, such as keyloggers from email-attached malware, compromised applications downloaded from app stores, spoofed cell towers and password manager sites, and intrusion into in-car systems or public wireless connections (Code: modified authentication method due to situational context, κ: 0.92). Additionally, the severity

Table 2. Sample codes and excerpts.

Code	Cohen's kappa (κ)
Avoids single point of failure	1.00
'The idea of a single sign on, where you go to places and sign on with your Facebook or Google Plus credentials: that scares me. I don't like having that single point of failure, or vulnerability, so to speak.' (P07)	
'Don't use password managers. Never felt a strong enough need to do it, and I've looked around at them and they're nice, but I look at password manager as a single point of failure.' (P07)	
Has modified authentication method due to situational context	0.92
'I'm much more conscious of where I access my home banking, whether its home or the network of my organization at my work. I tend not to do it outside unless I'm really forced. On public networks … For sure, I never do it when I'm traveling, like through airports. You can have dodgy wifi hotspot around.' (P08)	
Not expecting authentication improvements	0.84
'I think it's going to be a case of everybody fend for themselves, so stay the same or get worse. So the government has demonstrated with its ham-fisted response to the OPM breach that they don't have the best most efficient, most knowledgeable way of dealing with cyber security concerns, and there were too many special interests competing for limited dollars and resources to make any broad stroke improvements meaningful.' (P07)	
'I don't see any changes actually. What I've seen people talking about is that privacy more and more is going to disappear. We as consumer and user are going to be … We are willing to start to provide more and more information out in order to get a good deal.' (P08)	
Desire quick change in authentication method	1.00
'So the device has a lot of sensors so there are smarter ways of identifying the user, so if my phone can talk with my laptop. They easily could understand that it's still me interacting with the device, and that I've entered the password five minutes ago, and never left the device. Then there is no reason to ask me again. Maybe if there was some way of streamlining all this and getting some information from the environment.' (P08)	
Distrust/doubt in major mobile providers	0.84
'And for certain types of environments I will not see too many changes. So for Google I don't think they will change the operating systems or the way the security model is implemented at the moment.' (P08)	

of these threats was modulated for participants by their knowledge of the types of potentially sensitive data access required to carry out tasks on their mobile devices, and how dire the potential consequences of compromise of that data could be. Participant 20, an application development security researcher, stated 'I just thought, well, I only have a half dozen, a handful of web services where I actually care if somebody breaks in, and the other two hundred, three hundred, there's not much damage they can actually do if they do break in.' This participant explained his decision to forego more stringent security on most accounts, due to onerous usability penalties, also stating

> So, I think to some extent the perfect solution is paying a bit much, for the benefits that you get,' and, 'there's a limit to the value beyond a certain point of my improving my authentication strategy. Yes, it makes certain sorts of attacks less likely, but so what? It's got lost in the noise compared with all the other possible attacks.

One participant (P17), a career industry and government information assurance practitioner, referred to a 'risk spectrum,' alluding to the range of data security issues that could apply to a mobile user. This spectrum included being inadvertently 'swept up' in large data breaches related to a vendor or service provider, without making obvious security missteps, to operating in risky shared network environments like hotels or airports where insecure practices could be exploited, to the extreme of being specifically targeted by resourceful criminal or nation state adversaries with advanced technical capability. The level of threat to any individual user was understood to reflect the 'value proposition' their data presented to these various types of hostile actors. This awareness of data context is clearly not likely to be exclusive to security professionals. Information systems specialists, for example, would likely maintain similarly detailed and stateful mental models of their systems usage. However, the additional step of comparing that model of work-driven system and data dependencies with further consideration (occasionally termed *paranoia* by participants) of the types of vulnerabilities and frequency of compromise may be the result of security-focused experience. For example, Participant 7 was specifically concerned with any devices that combined network access and sensitive data storage. He stated, 'The phone doesn't have all my entire life on it. I don't store sensitive files on my phone, but the laptop is tied into other secure storage mediums.' This overlapping series of mental models, constructing understanding of how a task and its associated personal data might relate to security threats, forms the basis of a design implication, discussed later (Section 4.6), that suggests considering authentication as a layered process informed by the same view of contextual risk. How this model might be interpreted was often situationally based. For example, Participant 17 described 'lowering the attack surface' of his smartphone and laptop at security and hacker-related professional conferences, by shutting off network services and not leaving devices unattended (even in a lockable room safe), because of the perceived elevated risk of more aggressive targeting for malicious compromise.

4.2. Perceived drawbacks noted to security-conscious mobile device authentication behaviours (n = 20)

Participants reported numerous frustrations with their personal authentication experiences (including responses coded for using higher authentication rigour on mobile devices with sensitive data, and controlling sensitive data allowed on mobile devices). These adverse consequences related to overlapping aspects of their mental models of situational risk and the usability of their mobile devices. For example, Participant 14, a government information security developer, explained that he had researched the strength of the biometric device lock he used on his smartphone, and was only comfortable with the method if he also fully encrypted the drive, in case the authentication could be spoofed. This encryption, however, made rebooting the device much slower. Participants also disliked the usability impacts imposed by frequently entering long, complex passcodes, as well as the penalties associated with limiting the number of authentication tries allowed before locking an account (P17). These frustrations, with the burdens imposed by frequent complicated authentication schemes, on the one hand, and the potential consequences of data compromise, on the other, were the basis for several design implications, discussed later (Section 4.6).

Participants described strictly limiting storage of personal data on their mobile devices. They also avoided entirely many common mobile activities to satisfy their desire to more fully protect their user credentials. Avoiding conveniences such as password manager sites, single sign-on, and browser password-caching (P17), or the use of location services (P14) were reported, as well as generally trying to *compartmentalise* (P16) by not tying mobile accounts to services (Code: Avoids single point of failure, κ:1.00). Similarly, in pursuit of 'security through obscurity' (P16), participants frequently described limiting or avoiding use of social media. The motivations for this included not publically exposing personal information, hiding references to their geographic location, and not allowing mobile applications that harvested user data. One participant (P16), a government security researcher, noted regretfully that not

using his real name as a username in social media would prevent making some social connections with old classmates, but felt that was a necessary cost of limiting his security exposure. While perfectly security-conscious users might avoid mobile services entirely – 'bury gold and live off the grid' (P17), accepting some risk was also frequently acknowledged.

4.3. Imperfect password strategies (n = 8)

Several studies have documented difficulty in getting even sophisticated IT users to adopt secure authentication habits, particularly password management (Wash 2010; Schaub, Deyhle, and Weber 2012; Imgraben, Engelbrecht, and Choo 2014; Renaud, Volkamer, and Renkema-Padmos 2014; Micallef et al. 2015; Fagan and Khan 2016; Forget et al. 2016; Melicher et al. 2016; Ur et al. 2016, July). However, in this study, when asked if possible to recall an instance of new information influencing a change in their authentication behaviour, several participants ($n = 8$) volunteered that they had tried to strengthen their password authoring approach over time. 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. To make these more variable passwords memorable, he had arrived at using passphrases he could easily recall, sometimes up to 30 characters in length. Recalling and entering these phrases, however, was complicated and made frustrating by stringent security rules for password age, length, and character type requirements. Although the participant had not described externalising the data (i.e. writing down passwords) to support accurate entry, the cognitive demands were noted to pose strong challenges to the user.

Another participant (P15) described a similar change over time, also driven by knowledge of data security risks, and the need to recall numerous passwords which he did not want to cache in mobile device applications that he deemed insecure. This led to using simple geometric or arithmetic algorithms that he could mentally generate based upon an easily recalled alphanumeric seed. Participant 20 acknowledged deliberately using an imperfect approach that deviated from expert advice he had sought out, stating 'So I rejected that piece of advice from our experts, to use something like one password but don't have it talking to the Internet at all. That clearly is secure, but it's also not usable.' He also described choosing to ignore regular passcode updates to accounts deemed less important. Passcodes to these accounts were changed if they were shared to circumvent work sharing obstacles. He stated,

> I have to admit, except for my work one [account], [passcode updates are made] not at all. The only reason I have shifted them around is if I've told it to someone else, which is usually because of some unfortunate thing in the way they manage sharing forces me to do that. So, in general, I have never made a habit of changing my less-used passwords.

Similar to observations made by Adams and Sasse (1999) and Forget et al. (2016) in their studies of password behaviour, several of these participants volunteered that they kept physical cheat sheets of some of their passwords, in addition to their complex coping strategies for recalling strong mobile passwords. Both were well aware that this cheat sheet behaviour violated common security advice, but deemed it necessary to maintain the large volume of passwords they required.

4.4. Challenges to mobile authentication

Security-conscious users described numerous concerns regarding their mobile authentication which were rooted in their own behaviours, such as how they managed untrusted network connections or authored strong passcodes (such as choice in their length, character types, and recall cues). However, 17 participants also related at length their worries over how underlying weaknesses in the security of the device or network architectures might undermine the protection their authentication approaches were intended to provide. These weaknesses were often deemed beyond the control of their own choices or behaviour, and led participants to strictly limit their usage of mobile technology rather than trust authentication. For example, Participant 2, a career information security manager, split his work between two laptops, one 'trash' device never touching sensitive data but permitted to connect with many networks, and another with work data that never touched untrusted networks. The same participant related that several professional information security colleagues would regularly reinstall operating systems, or *dispose entirely* of their networked devices every six months out of concern for zero-day vulnerabilities, if they maintained a public persona that might make them a target of sophisticated hacking attempts. Other participants described similar 'air gap' methods to protecting data such as tax records. Participant 7 also expressed this risk evaluation challenge when considering the constant trade-off between new mobile device functionality and securing his private information, stating, 'That's great but what are we sacrificing, or what are we exposing ourselves to?' Furthermore, participants often expressed

distrust of major hardware and software makers to support trusted authentication via mobile technologies.

4.4.1. Concern with vulnerable mobile devices and network technology (n = 18)

Eighteen participants concurred, based upon varying aspects of their individual model of authentication's role in security, that they were concerned for the underlying technical architectures of their mobile devices (including responses coded for having responded to new threat information by changing authentication methods and passcodes, and maintaining tight control over wireless connections). This finding reconciles with existing research on the functional focus of expert mental models of security (Imgraben, Engelbrecht, and Choo 2014; Ion, Reeder, and Consolvo 2015). This concern was exacerbated in several cases by common situational impairments and physical threats, such as worry over shoulder surfing attacks. For example, Participant 3, a university instructor with industry and teaching experience with network security, had experienced losing a password to shoulder surfing, and recalled seeing others' vulnerability when riding on trains, stating, 'many times you can have a not-so-bad view of their mobile device, the reflection.' However, the participant expressed greater worry regarding allowing his laptop browser to store his passwords, because of his detailed doubts about the underlying software's connectivity. 'There is a lot of stuff connected to the browser. The browser is really a complicated piece of equipment and my trust level is not as high … ' he stated, and, ' … complicated systems are more likely to contain unnoticed vulnerabilities, and with the browser there are many, many components.' Furthermore, this distrust extended to the use of software-based password managers, to the extent of avoiding available commercial solutions and instead writing his own code to generate 512-bit hash passwords, to have a trusted source. The participant stated that this approach was, firstly, trustworthy in the sense that he felt he knew enough about computer science and cryptography to rely more on software he developed himself than obtained elsewhere, and, secondly, both secure and usable in its ability to regenerate memorable pass phrases.

Participant 20 also modified the frequency with which he changed passwords, based on the potential for the device with account passwords to be exposed through regular use, stating,

> It's because I have quite a number of devices that know my work password. My Samsung, my phone, my iPad, etcetera, etcetera. And that kind of proliferation of knowledge is itself a security issue. So, if I change my password fairly regularly I can ensure only the devices I'm using that regularly actually have access to my accounts.

Similarly, Participant 8, a mobile security researcher, was concerned over the vulnerability underlying the Android operating system in his smartphone, stating,

> No, it's the whole stack … [as the basis for security flaws in the Android architecture] … the kernel itself [the underlying Linux kernel upon which Android runs], but Google has simplified the security model compared to the Linux model. It's kind of concerning.

While the participant was still willing to authenticate entry to the device to perform necessary tasks, he was uneasy about the potential impact of these security flaws. Participant 7 also expressed greater concern for the authentication security of his laptop than his other mobile devices. Not because of its value or the authentication methods it supported, but instead because it was configured to connect to more networked accounts than his other devices. Participant 2 found this concern to be compounded by typical situational impairment issues. He found it disconcerting to have the phone locked while driving, but also felt use an in-car hands-free Bluetooth was highly insecure ('eleven,' on a hypothetical risk scale of 1–10) because of a perceived lack of security in its network architecture.

4.4.2. Distrust of major software and hardware companies' commitment to authentication (n = 11)

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 (including responses coded for distrust of technology providers, κ: 0.84). This resulted in a reluctance to authenticate using mobile devices to undertake tasks while on-the-go. Participant 3, alluding to his frustration with the practices of anti-virus protection providers, 'I don't have trust in those companies … so I figured, if that's how they want to play, then why bother?' Participant 8 closely echoed this sentiment, regarding security flaws in the Android mobile operating system he used, stating,

> … so it's insecure by design almost. And I think this openness is OK for Google. If we look at the threats we can see, its concerning, relating to privacy. It's quite easy to leak data from this device, but I think, for Google, this is the name of the game, right?

Participant 4 also shared this concern regarding how authenticated data from his Garmin wearable exercise watch might be stored. He placed trust in the device's authentication, based on detailed knowledge of how

the device carried out its low power Bluetooth connection and device verification with his laptop, but was dubious of the security of that personal information once it was cloud-stored.

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 instead attributable to short-sighted reluctance in many industries to make costly security investment a business priority. Publicised data breaches might make companies and customers 'wake up for a week,' (P17) but substantive improvement in mobile data security was deemed unlikely (Code: Not expecting authentication improvements, κ: 0.84). Another participant (P20) differed, seeing potential mobile authentication schemes based on personal behavioural and computing signatures as 'slightly scary,' but also so promising in their potential to reduce usability burdens as to merit trust in major technology providers.

4.5. Comparison of findings with prior research

Researchers have examined numerous technology-related issues faced by informed users. Examples include Kang et al. (2015), Ion, Reeder, and Consolvo (2015), and Bravo-Lillo et al. (2010) who found that these groups of users, who were likely to have commensurately more informed models of security and privacy risks, did not directly demonstrate that knowledge in their adoption of secure behaviours. Stobert and Biddle's thematic analysis of security experts' password approaches also found that informed users made a personal assessment of risk which determined how strictly they maintained security for their accounts. This would align with the security-conscious risk evaluation behaviours we relate (Section 4.1), but we also captured the underlying doubt about the intentions of technology providers (Section 4.4.2) motivating that caution (Stobert and Biddle 2015, December). Forget et al. (2016) also noted that engagement with security, in the form of proactive maintenance and information seeking behaviours, did not necessarily translate to more secure computing states. Our findings described in this paper, with a cohort that is both technical and specifically security conscious, have some similarity. Like Kang et al., these security-conscious mobile users varied in their approaches to securing their devices. However, that variation did not stem from a lack of regard for vulnerabilities and risk in this domain. Some simply opted not to use mobile devices at all for tasks that required data they deemed too sensitive to place at risk. Whether engaged in this purposeful avoidance of mobile authentication risk, or highly active in controlling it, these users were carefully considering the contextual and situational risk parameters they were willing to accept.

Additionally, several participants were consistently mindful enough of their secure authentication habits that they could describe when they accepted breaking their own rules. Motivations as disparate as being 'on the couch and wanting a pizza' (P16) or needing to send a bill payment (P7) were cited as reasons for accepting more risk. However, like the richly contextual decisions made by security experts in Bravo-Lillo et al., these deviations from typical authentication behaviour were described as thoughtful actions that involved evaluations of a familiar low-risk environment or task urgency. Forget et al. suggested that actions taken by users motivated to maintain their home computing security might incidentally introduce unsafe states, and that engagement also did not predict either security knowledge or concern with protecting personal computers (2016). Furthermore, Kang et al. suggested developing policy and technology that would not rely on users' engagement with security, given that the relationship appeared unreliable. Trewin et al. also found that non-security-conscious users, including doctors, online banking customers, and IT workers, were not mindful of risks beyond the scope of shoulder surfing and accessing malicious content, compared to a cohort of computer security experts. A lack of awareness of numerous potential types of network-based attacks risks was found in non-experts. This suggested a need for tailored notification, and for software applications to adjust tolerance for security non-compliance based upon the sensitivity of involved data (Trewin et al. 2016).

Existing research has also explored novel authentication smartphone methods which monitor user behaviours in the background, developing a profile which is used as a risk threshold for automatically adjusting device locking (De Luca et al. 2012; Micallef et al. 2015). These studies have largely dealt with better supporting everyday users, who have been found to resist adopting security practices with usability penalties. We suggest extending this view, by acknowledging that highly security-informed users presented highly variable responses to everyday scenarios, based on their richly modelled contextual and situational understanding. We suggest supporting that type of awareness, with authentication methods intuitively adjusting their rigour and usability to those contexts and situation.

4.6. Implications for mobile authentication

Participants described several 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 untrusted 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 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 behaviour**. Again, we do not assert that this foreshadows changes in behaviour or attitude towards authentication management among the broad base of consumers of mobile services. Instead, we note the scepticism found towards long-term improvement in mobile security (Section 4.4.2), which may influence adherence to secure practices and demand for security controls in this cohort. This may be portrayed in either informed buying choices, based on concern for the security of operating systems (Section 4.4.2), or choices in selecting and using applications (Sections 4.2, 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 behaviour, 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 exposure, 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 characterise 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 his desire to use strong authentication and to control the individual service permissions given to applications, as well as 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 that 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. As stated previously (Section 1.1), the transferability of this finding to everyday users is an important consideration. While studies of security experts have found differing outlook and behaviour from everyday users, it appears that this informed demographic itself is growing, and that greater concern for mobile computing risks may be spreading to everyday users.

Additionally, as discussed in Section 4.2 and in (Wolf, Kuber, and Aviv 2016), several 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 (i.e. changes in situation, context, and environment), or to have this process automated. In the case of automation, participants described mobile devices potentially using behavioural 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. Interestingly, this contradicts a general aversion to location-based services. Several participants related turning off GPS-based services when not in use, and avoiding social media location features entirely. Similarly, several participants also described their existing layered approaches to authentication, in which use of sensitive services or data on their mobile devices required entering additional passcodes, besides the device locking method. In this case, the context sensitivity would be to the type of access being requested by the user, rather than the environmental circumstances, but the participants again wanted to apply adaptive authentication methods.

For designers of mobile services, and especially for new authentication methods, these informed perspectives suggest that authentication may better be thought of as a series of responsive controls, layered throughout services, and responsive to auditing needs derived from the type of work being performed on a device, rather than a single method just for unlocking it. Developers would

need to consider the usability impact of modal shifts based upon the user's activity and circumstances (such as situational impairments or network connections). These findings offer valuable insight into how security-conscious users address their mobile computing, and how those needs may diverge from everyday users.

5. Conclusion and future work

Many difficult trade-offs were described by the participants interviewed in this study regarding their mobile authentication behaviour, between ease of use and the desire to protect their important data. This group of security-conscious users elaborated on the frustrations this introduced. Although some of these observations date to 2015, and the security implications of underlying technology (such as operating systems and prevalence of biometric unlocking methods) have shifted, the insights drawn from these perspectives suggest for mobile authentication researchers and developers that passcode methods should more fully reflect and adapt to the situations and activities of users with informed models of data security risk. As previous research has suggested (Asgharpour, Liu, and Camp 2007; Camp 2009; Bravo-Lillo et al. 2010; Ion, Reeder, and Consolvo 2015), our findings indicate that security-conscious users want enhanced mobile security features (i.e. warning and control dialogs) that are detailed and accurate enough to develop and inform their models of mobile data security. We also contribute a picture of how these users are likely to modify their expectations of these types of feature, based upon their interpretation of situational risk. This risk appears as a function of their assessment of the data sensitivity of their current mobile work, and the threats of compromise posed by their current network environment. Further qualitative research of this topic will more fully characterise 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. Specifically, we are undertaking a follow-on study which will compare our findings on the mental models and adoption of authentication methods of these security-conscious users with everyday users with a less defined sense of mobile computing risk. Existing research into mental models has made positive use of diagramming as a tool for extracting and comparing mental models. This method was deemed outside the scope of the collection and analysis portions of this explorative study, but may be applied in follow-on studies utilising the themes established here, directed at participants with those varying levels of security exposure. Our intent is to better define and understand differences between these groups to characterise how design recommendations regarding security can address wider audiences.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by Office of Naval Research.

References

Adams, A., and M. A. Sasse. 1999. "Users are not the Enemy." *Communications of the ACM* 42 (12): 40–46. doi:10.1145/322796.322806.

Asgharpour, F., D. Liu, and L. J. Camp. 2007. "Mental Models of Security Risks." In *Financial Cryptography and Data Security*, Scarborough, Trinidad and Tobago, edited by S. Dietrich and R. Dhamija, 367–377. Berlin: Springer.

Aviv, A. J., and D. Fichter. 2014. "Understanding Visual Perceptions of Usability and Security of Android's Graphical Password Pattern." Proceedings of the 30th Annual Computer Security Applications Conference, 286–295. ACM, December. doi:10.1145/2664243.2664253.

Beautement, A., I. Becker, S. Parkin, K. Krol, and M. A. Sasse. 2016. "Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours." Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO.

Blythe, J., and L. J. Camp. 2012. "Implementing Mental Models." IEEE Symposium on Security and Privacy Workshops (SPW), San Francisco, CA, USA, 86–90. IEEE, May.

Brase, G. L., E. Y. Vasserman, and W. Hsu. 2017. "Do Different Mental Models Influence Cybersecurity Behavior? Evaluations via Statistical Reasoning Performance." *Frontiers in Psychology* 8. doi:10.3389/fpsyg.2017.01929.

Braun, V., and V. Clarke. 2013. *Successful Qualitative Research: A Practical Guide for Beginners*. London: Sage.

Bravo-Lillo, C., L. F. Cranor, J. Downs, and S. Komanduri. 2010. "Bridging the Gap in Computer Security Warnings: a Mental Model Approach." *IEEE Security & Privacy* 2: 18–26. doi:10.1109/MSP.2010.198.

Brooks, D. J. 2011. "Security Risk Management: A Psychometric map of Expert Knowledge Structure." *Risk Management* 13 (1–2): 17–41.

Bureau of Labor Statistics, U.S. Department of Labor. 2015. *Occupational Outlook Handbook*. 2016-17 ed. Information Security Analysts Job Outlook. Accessed 6 December 2016. http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6.

Camp, L. J. 2009. "Mental Models of Privacy and Security." *IEEE Technology and Society Magazine* 28 (3).

Chin, E., A. P. Felt, V. Sekar, and D. Wagner. 2012. "Measuring User Confidence in Smartphone Security and Privacy." Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, DC. ACM, July.

Consumer Reports Magazine. 2013. "Keep Your Phone Safe: How to Protect Yourself from Wireless Threats." Accessed 7 December 2016. http://consumerreports.org/privacy0613.

De Luca, A., A. Hang, F. Brudy, C. Lindner, and H. Hussmann. 2012. "Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 987–996. ACM. doi:10.1145/2207676.2208544.

De Luca, A., E. von Zezschwitz, and H. Hussman. 2009. "Vibrapass: Secure Authentication Based on Shared Lies." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 913–916. ACM. doi:10.1145/1518701.1518840.

Diesner, J., P. Kumaraguru, and K. M. Carley. 2005. "Mental Models of Data Privacy and Security Extracted from Interviews with Indians." 55th Annual Conference of the International Communication Association (ICA), New York, NY, May.

Egelman, S., S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. 2014. "Are You Ready to Lock?" Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 750–761. ACM. doi:10.1145/2660267.2660273.

Fagan, M., and M. M. H. Khan. 2016. "Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice." Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).

Ferreira, D., V. Kostakos, A. Beresford, J. Lindqvist, and A. K. Dey. 2015. "Securacy: An Empirical Investigation of Android Applications' Network Usage, Privacy and Security." Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, 11. ACM. doi:10.1145/2766498.2766506.

Forget, A., S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang. 2016. "Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes." Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO.

Friedman, B., D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum. 2002. "Users' Conceptions of Web Security: A Comparative Study." CHI"02 Extended Abstracts on Human Factors in Computing Systems, 746–747. ACM. doi:10.1145/506443.506577.

Hang, A., A. De Luca, and H. Hussmann. 2015. "I Know What You Did Last Week! Do you?: Dynamic Security Questions for Fallback Authentication on Smartphones." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 1383–1392. ACM. doi:10.1145/2702123.2702131.

Harbach, M., E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith. 2014. "It's a Hard Lock Life: A Field Study of Smartphone (un) Locking Behavior and Risk Perception." Symposium on Usable Privacy and Security (SOUPS 2014), 213–230.

Imgraben, J., A. Engelbrecht, and K. K. R. Choo. 2014. "Always Connected, but are Smart Mobile Users Getting More Security Savvy? A Survey of Smart Mobile Device Users." *Behaviour & Information Technology* 33 (12): 1347–1360.

Intel Security and the Center for Strategic and International Studies. 2016. "Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills." Accessed 6 December 2016. http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf.

Ion, I., R. Reeder, and S. Consolvo. 2015. "" … No One Can Hack My Mind": Comparing Expert and Non-expert Security Practices." Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 327–346.

Kang, R., L. Dabbish, N. Fruchter, and S. Kiesler. 2015. "'My Data Just Goes Everywhere:' User Mental Models of the Internet and Implications for Privacy and Security." Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 39–52.

Karatzouni, S., S. Furnell, N. Clarke, and R. A. Botha. 2007. "Perceptions of User Authentication on Mobile Devices." Proceedings of the ISOneWorld Conference, Las Vegas, USA, April 11–13.

Lin, J., S. Amini, J. Hong, N. Sadeh, J. Lindqvist, and J. Zhang. 2012. "Expectation and Purpose: Understanding Users' Mental Models of Mobile app Privacy Through Crowdsourcing." Proceedings of the 2012 ACM Conference on Ubiquitous Computing, 501–510. ACM. doi:10.1145/2370216.2370290.

Mare, S., M. Baker, and J. Gummeson. 2016. "A Study of Authentication in Daily Life." Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO.

Melicher, W., D. Kurilova, S. M. Segreti, P. Kalvani, R. Shay, B. Ur, and M. Mazurek. 2016. "Usability and Security of Text Passwords on Mobile Devices." Proceedings of the 2016 Annual ACM Conference on Human Factors in Computing Systems, CHI (Vol. 16). doi:10.1145/2858036.2858384.

Merriam, S. B., and E. J. Tisdell. 2015. *Qualitative Research: A Guide to Design and Implementation*. 4th ed. San Francisco, CA: John Wiley.

Micallef, N., M. Just, L. Baillie, M. Halvey, and H. G. Kayacik. 2015. "Why Aren't Users Using Protection? Investigating the Usability of Smartphone Locking." Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services, 284–294. doi:10.1145/2785830.2785835.

Mylonas, A., D. Gritzalis, B. Tsoumas, and T. Apostolopoulos. 2013. "A Qualitative Metrics Vector for the Awareness of Smartphone Security Users." In *International Conference on Trust, Privacy and Security in Digital Business*, edited by S. Furnell, C. Lambrinoudakis, and J. Lopez, 173–184. Berlin: Springer, August.

Norman, D. A. 2013. *The Design of Everyday Things: Revised and Expanded Edition*. New York: Basic books.

Posey, C., T. L. Roberts, P. B. Lowry, and R. T. Hightower. 2014. "Bridging the Divide: A Qualitative Comparison of Information Security Thought Patterns Between Information Security Professionals and Ordinary Organizational Insiders." *Information & Management* 51 (5): 551–567.

Rader, E., and R. Wash. 2015. "Identifying Patterns in Informal Sources of Security Information." *Journal of Cybersecurity* 1 (1): 121–144.

Rader, E., R. Wash, and B. Brooks. 2012. "Stories as Informal Lessons about Security." Proceedings of the Eighth Symposium on Usable Privacy and Security. doi:10.1145/2335356.2335364

Raytheon and National Cyber Security Alliance. 2016. "Securing Our Future: Closing the Cybersecurity Talent

Gap." Accessed 5 December 2016. http://www.raytheoncyber.com/rtnwcm/groups/corporate/documents/content/rtn_335212.pdf.

Renaud, K., M. Volkamer, and A. Renkema-Padmos. 2014. "Why Doesn't Jane Protect her Privacy?" In *Privacy Enhancing Technologies*, 244–262. Springer. doi:10.1007/978-3-319-08506-7_13.

Safa, N. S., M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan. 2015. "Information Security Conscious Care Behaviour Formation in Organizations." *Computers & Security* 53: 65–78.

Schaub, F., R. Deyhle, and M. Weber. 2012. "Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms." Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia, 13. ACM. doi:10.1145/2406367.2406384.

Stobert, E., and R. Biddle. 2014. "The Password Life Cycle: User Behaviour in Managing Passwords." Proceedings of the SOUPS, Menlo Park, CA, July.

Stobert, E., and R. Biddle. 2015. "Expert Password Management." In *International Conference on Passwords*, edited by F. Stajano, S. F. Mjølsnes, G. Jenkinson, and P. Thorsheim, 3–20. Cambridge: Springer, December.

Trewin, S., L. Koved, C. Swart, and K. Singh. 2016. "Perceptions of Risk in Mobile Transactions." Proceedings of the 2016 IEEE Symposium on Security and Privacy Workshops. (IBM T.J. Watson Research Center). doi:10.1109/SPW.2016.37.

Ur, B., J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor. 2016. "Do Users' Perceptions of Password Security Match Reality?" Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16), 3748–3760. New York: ACM. doi:10.1145/2858036.2858546.

Volkamer, M., and K. Renaud. 2013. "Mental Models – General Introduction and Review of Their Application to Human-Centred Security." In *Number Theory and Cryptography*, 255–280. Berlin: Springer. doi:10.1007/978-3-642-42001-6_18.

von Zezschwitz, E., P. Dunphy, and A. de Luca. 2013. "Patterns in the Wild: A Field Study of the Usability of Pattern and pin-Based Authentication on Mobile Devices." Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services, 261–270. ACM. doi:10.1145/2493190.2493231.

Warshaw, J., N. Taft, and A. Woodruff. 2016. "Intuitions, Analytics, and Killing Ants: Inference Literacy of High School-Educated Adults in the US." Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO.

Wash, R. 2010. "Folk Models of Home Computer Security." Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA, 11. ACM, July.

Wash, R., E. Rader, R. Berman, and Z. Wellmer. 2016. "Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites." Symposium on Usable Privacy and Security (SOUPS), Denver, CO.

Whitten, A., and J. D. Tygar. 1999. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." Usenix Security (Vol. 1999), Washington, DC.

Wiese, O., and V. Roth. 2015. "Pitfalls of Shoulder Surfing Studies." Proceedings of NDSS Workshop on Usable Security, San Diego, CA.

Wolf, F., R. Kuber, and A. J. Aviv. 2016. "Preliminary Findings from an Exploratory Qualitative Study of Security-conscious Users of Mobile Authentication." Proceedings of the Second Workshop on Security Information Workers (WSIW) (4 pages), Denver, CO.

Yee, K. Y. 2002. "User Interaction Design for Secure Systems." Internal Technical Report - UCB/CSD-02-1184. http://digitalassets.lib.berkeley.edu/techreports/ucb/text/CSD-02-1184.pdf.