"Pretty Close to a Must-Have:" Balancing Usability Desire and Security Concern in Biometric Adoption

Flynn Wolf
UMBC
flynn.wolf@umbc.edu

Ravi Kuber
UMBC
rkuber@umbc.edu

Adam J. Aviv
United States Naval Academy
aviv@usna.edu

ABSTRACT

We report on a qualitative inquiry among security-expert and non-expert mobile device users about the adoption of biometric authentication using semi-structured interviews (n=38, 19/19 expert/non-expert). Security experts more readily adopted biometrics than non-experts but also harbored greater distrust towards its use for sensitive transactions, feared biometric signature compromise, and in some cases distrusted newer facial recognition methods. Both groups harbored misconceptions, such as misunderstanding of the functional role of biometrics in authentication, and were about equally likely to have stopped using biometrics due to usability. Implications include the need for tailored training for security-informed advocates, better design for device sharing and co-registration, and consideration for usability needs in work environments. Refinement of these features would remove perceived obstacles to ubiquitous computing among the growing population of mobile technology users sensitized to security risk.

CCS CONCEPTS

• **Security and privacy** → **Authentication**; • **Human-centered computing** → *Empirical studies in HCI*;

KEYWORDS

Authentication, Biometric adoption, Mobile device, Security expertise

1 INTRODUCTION

Biometric authentication has the potential to increase the usability of mobile devices. Frequent screen unlocking and application authorization is accomplished with a quick glance or touch rather than recalling and entering long/complex passcodes [19]. Despite the benefits, adoption can be uneven due to usability issues [9, 29] and user misunderstanding or security concern [14].

From a security-conscious perspective, allowing a new technology to record and store a permanent signature of one's self and use it to control access to sensitive data transactions might cause deep concern. Research has documented biometric adoption [2, 25], experts' sophisticated mental models of network security that are distinct from those of everyday users [1, 4, 5, 26, 30, 33], and the influence that usability [12, 15, 16] and similar models of security have on outlook and behavior [8, 12, 14, 16, 27]. However, these studies have not specifically addressed the overlap of biometric adoption and expert understanding of the underlying technologies and threats involved with mobile connectivity, which we have investigated in this study.

We addressed this knowledge gap through a qualitative study comparing biometric adoption for a group of security expert and non-expert users (n=38, 19/19 expert/non-expert). Based upon criteria from prior research, we defined security awareness for the expert cohort as one year of full-time exposure to network security issues through work or academic research. Using semi-structured interviews, we found key differences and commonalities between these groups, which can inform design trade-offs between usability and security, as well as how security adoption of mobile technologies more generally can affect a broad array of systems.

We were further motivated to examine adoption of biometric unlocking because fingerprint recognition has gained significant consumer acceptance, but is also a relatively new offering by major technology providers (iOS TouchID is the most common example in our cohort, and is 5 years old at the time of this study). As a result, many security conscious users will have recent memory of how they struck their own bargain between convenience and any doubts about its use. As facial and voice-based authentication also gain acceptance by mobile device users, our aim is to compare the security bargains made with those of fingerprints.

We present six main findings that comparatively describe the outlook of two important populations of mobile users and highlight how perspectives on adoption have evolved over time. We also examine how factors including work requirements and device sharing have impacted users' behavior. Our findings include:

- Both experts and non-experts harbored misunderstanding about biometric implementation, such as its primary vs. secondary role.

,

- Both groups were subject to usability problems that led to abandoning biometric use.
- Experts were more influenced by work/bring-your-own-device (BYOD) authentication requirements than non-experts.
- Experts demonstrated more concern about securing their mobile devices.
- Experts were more likely to try biometrics immediately once available, were slightly more likely to view consumer biometric security as a good idea in principle, and were more likely to recommend the features than not.
- Non-experts were more trusting of biometric authorization for financial applications.

Finally, we derive from these findings three insights, described in Section 5, that can improve the design considerations for relevant authentication methods. Specifically, we discuss alleviating experts' concern and misunderstanding through *tailored education for security-informed advocates*. Similarly, we examine the device sharing and work-related obstacles to satisfactory biometric adoption that call for better *design for co-registration* and *usability consideration for work environments*.

2 RELATED WORK

Rise of Biometrics. Biometric authentication, including recognition of a user's fingerprint, face, or voice, addresses the need for increased usability with security of mobile devices, with estimates suggesting all mobile devices will be biometrically-enabled by 2020 [21]. Other biometric methods include continuous authentication (e.g. keystroke dynamics over a period of time) [20]. Research indicates user acceptance, including security and usability, is a major concern in biometric adoption [25]. Recognizing this, manufacturers have published descriptions of underlying technical protections such as the Apple Secure Enclave to assure users [28].

Attitudes Towards and Adoption of Biometrics. Biometric adoption has been studied from a number of perspectives. Lab-based studies have compared users' task performance and perception of different unlocking methods between operating systems, finding complex interaction between biometric method and users' task accuracy and acceptance [2, 29].

Lab and focus group studies have also surveyed user opinion directly on biometric issues such as acceptance of continuous authentication [7] and securing sensitive transactions [17]. Additional facets of biometric adoption examined by researchers include capturing user motivation in specific geographic regions [25], and the impact of romantic relationship status on password and account sharing [22].

The underlying technical integration of biometric unlocking has also been studied, in terms of potential attack points and countermeasures [20], and the security of API implementation [3].

Perceptions of Individuals with Security Expertise. Most directly related to this study, research has also examined the prevalence of mobile security awareness and its influence on behaviors such as authentication adoption. These studies indicate that security-informed users are a significant population with needs worthy of investigation. For example, researchers have examined differences and similarities in security expert and non-expert mental models of the information technology, and how these views may influence behavior. Kang et al. found advanced mental models of Internet processes in IT experts imparted more awareness of privacy risks, but did not translate into more secure behavior versus non-experts [16]. Similarly, Friedman et al. surveyed Internet users from rural, suburban, and high-tech sectors about web security, and found generally poor comprehension of security features [12]. Stobert and Biddle used thematic analysis of semi-structured interviews to describe academic and industrial security experts' (n=15) password management. These users were found to vary between laxness and caution based on perceived risk towards their sensitive accounts [27].

Research has described several effects that security knowledge may impart. Das et al. surveyed the influence of demographics and security behavioral intention (SBI) on news sharing after major security-related events. High SBI correlated with consuming security news online and willingness to share news generally, and specifically with colleagues and significant others. The authors were surprised to report a correlation between low SBI and willingness to share security and privacy news when the participant noticed others behaving insecurely [8].

Huh et al. also found that prior security awareness played a role in adoption of mobile features. An online survey of 349 mobile tap-and-pay users and deliberate non-users found usability to be the paramount consideration. However, deliberate non-users of the feature cited security as their main deterrent. In that group, there was often misunderstanding of how credit card information was stored on the mobile phone and shared during transactions. A correlation was also found between security knowledge and adoption of the tap-to-pay feature [14]. Relative *non-expertise* with security management has also been studied in terms of understanding of security issues [31, 32], along with sources that influence non-expert security decision making [23, 24].

Biometric adoption has been studied, but not with a comparative approach towards those with security training. These expert related studies indicate that security-informed mental models may be expected to differentiate some mobile user choices, but experts and everyday users may both be subject to misunderstanding and not adhere to rigorous security

practices. We have examined this cohort alongside everyday users and describe a number of contrasting themes in their adoption practices.

3 METHOD

Objectives. We conducted a study comparing attitudes and experiences with adoption of biometric unlocking by security experts and non-expert users. We asked participants to describe and reflect on their own adoption of biometrics on personal or work-issued devices, their opinions of biometric usability and security during the adoption process, and if any of those views have changed since adoption (or instances of deciding to defer adoption).

Study Design and Procedure. To gather detailed responses to questions regarding a fairly broad range of topics, we decided to use semi-structured questioning. A set of research questions was used to generate a 41-question interview instrument that was used with all participants, addressing basic participant demographics, mobile usage, and experiences and opinions on biometric authentication. Other topics included exposure to biometrics, BYOD and work-related authentication requirements, and possible concern towards spoofing or compromise of one's biometric signature. Questions were generated iteratively through a set of pilot interviews. A list of questions are in the Supplementary Materials.

All interviews were conducted by phone or audio Skype, lasting on average 32 minutes. All participants were read an IRB notification describing the study and the handling procedures for their data, and their consent was recorded. Interviews were conducted, notated, and transcribed.

Participant Demographics and Sampling. In total, 38 participants were recruited, 19 security experts and 19 non-experts (detailed in Table 1). Experts were recruited through personal networking among security researchers and developers to locate biometrics users, and through attendances at venues where experts would be present (e.g. security related conferences). Non-experts were recruited through a range of mailing lists. Individuals were carefully screened to ensure that they met criteria defined for each category.

To fit under the category of 'expert', a review of comparable research standards for security expertise was conducted to identify an effective definition [1, 4, 12, 15, 16, 27]. We adopted a standard of one year of professional or research exposure to network security issues, which was intended to identify those with sensitizing exposure to privacy and network security concerns. While this standard was not intended to qualify full domain expertise, our expert cohort averaged 16.9 years of related experience. Two experts had near-minimum duration experience, but were both highly engaged over at least 2 years in either biometric software development or network security. Experience with usage of biometrics on a mobile device (current or previously) was also a requirement for the study for both experts and non-experts. Non-experts included individuals with little or no security experience who were current or prior users of biometric unlocking on mobile devices.

		Expert			*Non-Expert*			*Total*
		M	F	Total	M	F	Total	
Age	<21	0	0	0	2	1	3	3
	22-34	2	1	3	5	4	9	12
	35-44	3	1	4	3	1	4	8
	45-54	2	1	3	0	0	0	3
	55-64	4	0	4	1	1	2	6
	>65	4	1	5	1	0	1	6
BAM use	<1 yrs	2	1	3	0	1	1	4
	1 to 2 yrs	4	1	5	2	2	4	9
	>2 yrs	8	1	9	7	3	10	19
Mobile OS	iOS	6	3	9	6	3	9	18
	Android	7	0	7	1	3	4	11
	Windows	4	0	4	0	3	3	7
	Total	15	4	19	12	7	19	38

Table 1: Participant demographics.

The expert group consisted of 15 men and 4 women, with an average age of 50.7 years, an average of 16.9 years of network security experience, and an average of 3.4 years of direct experience with biometric authentication. The non-expert group consisted of 12 males and 7 females, with an average age of 33.6 years and average of 2.5 years of direct experience using biometric authentication (as described with additional detail of biometric experience and mobile device use in Table 2). The size of these two groups were similar to those of related qualitative security research [6, 10, 34].

Analysis of Transcripts. Inductive thematic analysis was performed using four reviewers to identify themes from participant responses. Initial open coding was conducted with notes and audio from each interview to sensitize to any themes or observations, followed by axial coding. The codes were combined and deconflicted to produce a set of 76 mutually exclusive, descriptive themes. These were then further iterated and clarified. A subset of the interview transcripts (12.5%) were reviewed by a fourth coder, and good inter-rater reliability was found (Cohen's Kappa coefficient (κ) = 0.72). A subset of codes are shown in Table 3.

Themes that emerged towards the end of the interview process were re-addressed with a subset of expert participants in short follow-up interviews. These included questions about using biometrics on work-related versus personal devices, passcode sharing and biometric co-registration, and differences in concern regarding compromise of behavioral versus biometric signature data. Sampling was concluded when coding saturation became apparent and no new axial codes emerged from interviews.

Participant #	Expertise	Expert Domain	Netsec. Experience (Yrs.)	Age	Gender	Current Biometric OS/Device	Biometric Use
1	Expert	Gov & Industry	40	70	M	iPhone & Win10 laptop	2 yrs (face) & 1 yr (finger)
2	Expert	Gov & research	2	25	M	Android Oxygen (phone) & Win10 laptop	2 yrs (phone) & 5 yrs (laptop)
3	Non-expert			21	M	iPhone	3 yrs
4	Expert	Gov & Research	21	45	F	iPhone & iPad)	3 yrs (phone) & 1.5 yrs (iPad)
5	Expert	Industry	12	42	M	Win10 laptop	4 mos
6	Non-expert			42	F	iPhone)	2 yrs
7	Non-expert			33	F	iPhone 6)	1 yr
8	Non-expert			22	M	iPhone 5)	4yrs
9	Non-expert			34	M	iPhone 10 (FaceID) & iPad)	2-3 yrs (TID) & 3-4 yrs (FID)
10	Non-expert			21	F	iPhone 5s & iPad	3 yrs (iPad) & 6 mos (phone)
11	Non-expert			22	F	iPhone 6	3 yrs
12	Non-expert			26	M	Pixel 2 XL (Android)	2-3 mos (Pixel) and 3 yrs (old Nexus 6P)
13	Non-expert			21	M	iPhone 7	2 yrs
14	Expert	Gov & Industry	20	70	M	Samsung Edge 7 (Android)	1.5 yrs
15	Expert	Gov & Industry	30	70	M	iPhone 6c & Lenovo Win10 Laptop	5 yrs
16	Expert	Gov & Industry	25	66	M	Android Samsung S8 (Android)	10 mos
17	Non-expert			23	F	iPhone 6	10 mos (incl. 7 mos. previous device)
18	Expert	Gov & Industry	27	64	M	iPhone 7	1 yr
19	Expert	Gov & Industry	30	56	M	iPhone 6	2 yrs
20	Expert	Gov & Industry	20	52	M	Galaxy 8S (Android)	1 yr (incl. previous Galaxy 7)
21	Expert	Industry	2	39	F	iPhone 6	6 mos
22	Non-expert			24	M	Samsung S6 Edge (Android)	3 yrs
23	Non-expert			27	M	iPhone 6s & Win (Surface & old Toshiba)	7 yrs
24	Expert	Academia	3	29	M	iPhone 6	2 yrs
25	Expert	Academia & Industry	4	54	M	Android Samsung S6, iPad Pro, & prev. laptop	2 yrs
26	Expert	Academia	17	38	M	iPhone 6S	2 yrs
27	Non-expert			29	F	Android Google Pixel, iPad Pro	1.5 yr
28	Expert	Industry & Academia	20	42	M	Android Google Pixel 2	3 yrs
29	Non-expert			27	M	None (prev. Win10 laptop & Android S6)	1 yr
30	Expert	Academia	20	59	M	Android Motorola	1 yr
31	Expert	Gov & Industry	20	65	F	iPhone & iPad)	1 yr (on/off)
32	Non-expert			58	F	Android Samsung Galaxy	3 mos.
33	Expert	Industry	5	54	M	iPhone 6S & iPad Pro)	>20 yrs.
34	Non-expert			56	M	Android Samsung Galaxy Edge	1.5 yrs.
35	Expert	Academia	3	23	F	iPhone	2 yrs.
36	Non-expert			66	M	iPhone X & Win laptop	3 yrs.
37	Non-expert			43	M	iPhone & iPad	2 yrs.
38	Non-expert			38	M	iPhone 5S & Win laptop	4.5 yrs.

Table 2: Details of participant experience.

4 ANALYSIS

We address six major findings and 10 sub-findings drawn from themes derived from expert and non-expert participant responses of our expert and non-expert participants (summarized in Table 6). As shown in Table 4, users generally favored fingerprint recognition, either iOS (22 total users, 10 experts), Android (13 total users, 7 experts), or Windows (7 total users, 5 experts). Facial recognition use was still relatively scarce, and its use was divided between Apple FaceID and older Windows facial recognition. Several expert users also had past experience using or developing advanced biometric security controls, including body weight, iris scanning, and hand size measures.

At a high level, we found that experts held an expected higher degree of concern towards data compromise than non-experts. This concern shaped both their willingness to try out new authentication methods and concurrently their distrust towards using mobile platforms for sensitive transactions. However, we also found significant misunderstanding in both groups about how biometric authentication is implemented. Both groups feared compromise of their biometric signatures, and experts, in particular, tended to project their prior knowledge of other network vulnerabilities onto this fear.

Misunderstanding of primacy of biometric unlocking

While biometrics may function in mobile operating systems as a secondary method of authentication to back up other what-you-know passcodes, half of both non-expert and expert users misunderstood the biometric method to instead be the primary means of unlocking their mobile device. This view was also evenly split between the two groups (held by 9 experts and 9 non-experts). *This view was held at a higher rate than any other code.*

Device sharing and co-registration

A number of participants (n=8, 4 experts) discussed how both biometrics and passcodes fit into their approach to physically sharing access to their mobile devices with others. For example, several non-experts reported cross-registering fingerprints with partners on their phones to speed up routine tasks and for potential emergencies. However, all expert participants reporting this type of device sharing with their spouses, partners, or children (n=4) preferred only sharing conventional PIN passcodes, despite using biometric unlocking for themselves. One non-expert (p37) reported deliberately not sharing any passcodes or biometric co-registering because he did not want his children accessing his devices ("I don't want them buying stuff"), and to avoid having to reset the authentication if a trusted relationship ended. Another non-expert (p38) felt that iOS FaceID was more secure for sharing, on the assumption that faces seemed more unique, despite acknowledging not knowing the "rhyme or reason ...behind the science," but like other participants chose biometric co-registration for convenience rather than security.

Participants who only shared PINs with others, versus biometric co-registration, described their preference as simply

convenience rather than reluctance to co-register because of social or security concern. For example, an expert participant (p25, an academic security researcher and application developer) described telling his PIN to his children while driving so they could control music in the car without distracting him. *However, it is possible that co-registration is not a familiar option, given that other expert participants described simply being unaware that multiple fingers could actually be registered.*

Participants who had tried and discarded biometric authentication still shared passcodes, even if they did not use PINs. A non-expert university professor, p32, had stopped using Android fingerprint recognition stating, "I really hate it, a lot" because of frequent false negatives, but still shared grid pattern shapes that could be described verbally with her husband. The instances of misunderstanding towards biometric co-registration and the likelihood of interaction with other usability and security concerns found here indicate a need for more effective *design for device co-registration*, discussed in Section 5. Device sharing and co-registration occurred within a number of relationship types (e.g. with both children, spouses, or romantic partners) and among a wide range of ages that suggests very limited potential for age effects.

Experts more influenced by BYOD requirements

A majority of those reporting that work-related requirements influencing their authentication choices were experts (6 of 8). We acknowledge that this may also reflect the higher average age of the expert cohort (50 years old, versus 33 for non-experts), which could place them further along in technology-related careers that might contribute to this effect, rather than it being solely a product of their network security exposure. The average age of participants reporting this code was 46.6 years old. Of those experts, several were required to add authentication through contract or employment conditions. One expert (p04, a government security researcher) explained her caution towards authentication choices for work related devices, stating "I'm very cognizant at work that if I make a poor security decision it doesn't just affect me, it can affect the whole organization. So, I'm probably just more vigilant... just because of the potential consequences... If there was a big breach and I was responsible for it that would be really bad."

Experts also dominated commentary made about recent changes to one's authentication approach (n=13, 10 experts). The mentioned changes included both usability-driven actions (e.g. p01, a cybersecurity consultant, who stopped using buggy Windows face recognition on his laptop) and security-driven actions (e.g. p02, a military cybersecurity developer, adding two-factor authentication to an account). However, in several cases biometric adoption imposed by work requirements was reluctant. For example, an expert (p05, a security company CTO) was actually very skeptical of how biometric authentication was implemented for his Windows work devices ("the entire integration needs to be done differently"), but was required to apply them, stating "I try to be secure, but I had to use them [biometrics] for work." These findings suggest a need for *usability consideration for work environments*, discussed further in Section 5.

Software automation of authentication. A subset of expert users was asked specifically about their willingness to allow continuous authentication to use behavioral data to control unlocking, and about their willingness to use third party software to automatically configure their security settings in this way. The latter issue would involve a product such as Samsung Knox [18] continually reconfiguring a device's security settings based on risk measures such as location and user behavior.

One expert (p04) summarized the prevailing outlook, stating that she liked the idea of software assistance with security, but lacked requisite trust in autonomous change of security settings. She stated, "I would prefer [third party continuous authentication software] make a best guess, then give me a choice... Even though I'm a computer science person I don't really trust automation 100%." Participants were asked to compare their level of concern between potential compromise of their behavioral data and their biometric data (as used in either case for authentication). Another expert (p05) surmised that attempting to withhold behavioral data from continuous authentication for privacy reasons was already not realistic, stating, "The cat's already out of the bag."

Biometrics as added protection for sensitive local storage. Others felt the need to apply biometrics to improve the physical security of their devices (laptops, primarily) when those devices were used to locally store sensitive data in order to avoid cloud storage (p01 and p15, both industry and government information security consultants with 20 years of experience). Another (p25, a university security researcher) was frustrated that their university employer dictated minimum authentication standards for devices accessing work email, because "I know things about the devices they [the employer] don't." Similarly, another expert (p30, an academic security researcher) was uncomfortable using biometrics alone for unlocking a work device, unless it also had allowed an alphanumeric password for disk encryption.

Biometric Adoption

Experts are more likely to be early adopters of biometrics. We examined participants' descriptions of the interval between acquiring a biometric-capable mobile device and setting up the feature (n=14, 11 experts). This is of interest assuming

Code	κ	n	Sample Quote
BAM considered primary rather than secondary unlocking method	.86	19, 8 experts	"I would never use biometric alone as the primary on anything, without backup, on anything holding secure information." (p05)
Would not use BAM on a work/high security device	1.00	7, 5 experts	"If I think about it deeply I don't like it. I start to think about ridiculous murder mystery things that wouldn't happen." (p29)
Would recommend BAM use to others	.95	22, 12 experts	"I'd say go for it... [but use] flagship products." (p23)
Work requirements influence personal device choices	.69	8, 6 experts	"I try to be secure, but I had to use them [BAM] for work." (p05)
Did not try BAM immediately when available	.84	11, 5 experts	"'[friend recommended] that I let everyone throw everything at it first." (p27)
When first heard of it, consumer BAM sounded like a good idea	.80	11, 8 experts	"I thought its about time to allow biometrics." (p14)

Table 3: Example codes

that users may have security-informed motivations for either using immediately or avoiding a new authentication method. A preponderance of the experts interviewed reported at least trying out the biometric unlocking feature immediately when it was first available. Given the even split between using Android and iOS devices for experts, this effect was likely a response to several aspects of the expert cohort. Firstly, the expert cohort had a greater rate of direct familiarity with biometrics (21% had prior direct experience with biometrics outside of unlocking a personal mobile device, through purposes such as using or developing building access controls). Secondly, it might be assumed that experts, as a result of their general training and experience with security, would be more likely to know the usability and security difficulties associated with recalling strong what-you-know passcodes and want a better what-you-are biometric alternative.

Experts view biometrics positively post-adoption. We found that experts were almost evenly divided on whether they initially thought biometric authentication would be a positive or negative feature to offer consumers, although a majority of all participants favoring the idea were experts (n=13, 8 experts). Prolonged exposure (primarily fingerprint recognition, see Table 4) appears to have put experts at ease. "It's pretty close to a must-have [feature]," stated one (p30), "it's just so doggone convenient." When asked whether they now, having used biometric unlocking, have or would recommend it to others, experts were more favorable than not. It is also possible that the higher rate of immediate use of biometrics in experts is attributable to their slightly higher age and the commensurate exposure to technology that could support exploring and trying out new features (the average age of participants reporting this code was 43.9 years old). One expert (p04) stated, "I definitely went to the TouchID as a preferred authorization method and that was just because of my own experience and knowledge of how passwords can become co-opted very easily. That influenced me, once I had that available on my iPhone to just immediately enable that feature... That's based on my work experience and what I can see and the problems I see people having."

Non-experts delay adoption of biometrics. A slightly higher rate of non-experts also reported having deliberately waited to try out their biometric unlocking features, compared to the rate of reported initial avoidance in experts. In the case of experts this reluctance could be attributable to a generally more polarized opinion on security matters. Non-experts' may have a relative lack of technological experience (in part due to their lower average age) that produces caution or indifference towards new and unfamiliar security features. The average age of participants reporting this code was 41.7 years old. One non-expert (p27) felt it best to wait to try the fingerprint unlocking features on both his Android phone and iOS tablet out of a non-specific sense of security caution to "let everyone throw everything at it first." Another (p07) initially felt that the TouchID feature on her iPhone was an unnecessary "stupid rich person's feature." She eventually tried the feature after a year, to "keep in touch, in the same boat with technology," but still wondered, "is it really safe?" and would its use might "make my brain lazy."

Expert caution with securing data biometrically

At the same time that experts demonstrated more eagerness to try out biometric unlocking, they also distrusted it to secure their most sensitive data. While only a portion of the total cohort reported avoiding biometrics entirely for securing a highly sensitive device, that view was primarily held by experts (n=7, 5 experts). Similarly, concern over sale or leakage of one's biometric signature was a view only reported by experts (n=6 experts), often stating variations on "you can't grow a new thumb (p15, a government and industry security developer). An expert (p04) stated, "I don't know that people think about [trusting a device to store their fingerprint data], but if it's a foreign government... I might be a little more concerned. There's some acceptability issues, depending on who has access to your info." "The fact that biometrics can be forced out of you, against your will... I shy away from those," another expert (p05) stated, adding "I would never use a biometric method alone as the primary, without backup, on anything holding secure information... if

a fingerprint is the only thing between you and the keys to the kingdom, that's a bad design." Further, the user's trust was limited by knowledge of who was providing the device and services, saying, "Two companies I don't place my trust in are Apple and Google."

Experts much more reluctant to biometrically authorize financial applications. In addition to these views, using biometrics to authorize financial applications (including bank apps and payment apps such as PayPal or Venmo) was much less prevalent in experts. Many participants used biometrics to authorize these types of financial applications, but non-experts outpaced experts in allowing this. Interestingly, only one non-expert (p09) explicitly pointed out that biometric unlocking of his banking application allowed him to use a longer complex passcode for better security because he did not have to remember it or write it down. Demonstrating this added level of concern with financial transactions on a mobile platform, expert p05 stated, "After having my wife's phone stolen and the credit card info extracted, I, you know, wipe down any device I'd ever used for any type of transaction... Basically reinstall the OS. Wipe it down. Remove any transaction history, and when that's not possible I use increasing layers of disk encryption to protect the files that are stored." Participants were also asked if security had factored in when choosing their current mobile devices. Participants in general were almost twice as likely to have voiced affirmative responses (n=17, 12 experts) as negative responses (n=9, 3 experts), but experts specifically were four times as likely to cite concern with security features.

Biometric adoption interacting with experts' distrust towards mobile platforms. These findings of both greater expert curiosity and concern towards authentication suggest that experts view biometrics with a sort of 'accept but restrict' approach, in which quick adoption based on prior familiarity or principles of secure computing are balanced with doubt towards the trustworthiness of mobile platforms in general. Indicative of this, when asked which was more secure, of their laptop (n=11, 5 experts) or smartphone (n=4, 1 expert), more experts trusted the desktop operating systems over mobile. There is "less idea of what's going on in the background" of his Motorola Android phone, versus a PC, one expert (p30) related. Some experts also expressed preferences in mobile platform based on configurability for security. For example, p05 stated "I would pick one [Android] over the other because I believe I understand how to secure its attack surfaces more efficiently."

Experts and non-experts both aware of biometric spoofing. However, while experts offered detailed descriptions of threat models of data leaks or hacking that amplified their distrust, awareness of risks to biometrics was not exclusive to that cohort at all. In response to late-added question specifically about biometric-spoofing stories, an almost equal number of non-experts and experts (n=7, 3 experts) could recall examples. Experts could place these stories in context (for example, p30 stating, "we're in an arms race with gummy bears [used to spoof fingerprints]"), but macabre news reports of amputated fingers being used in criminal heists (p29, non-expert) and YouTube videos of fake heads unlocking phones (p27, non-expert) appeared to have also made a mark with non-experts. More specifically, an equal number (n=4, 2 experts) of expert and non-expert participants also stated in almost exactly similar terms that they did not feel like they were a "high value target" that would warrant elaborate biometric-spoofing. One expert, (p28) stated, "I generally don't hang around those types of people [who might be targeted with elaborate spoofing techniques]. They build rockets."

Apprehension towards facial recognition. The number of current facial recognition users was low compared to fingerprint recognition. Participants mentioned two factors contributing to this. Apple FaceID was only recently released at the time of this inquiry, and some curious iOS users were not ready to upgrade to a compatible device. Other laptop-based facial recognition users had stopped use because of frequent false negatives. Participants who were current or prior users of other forms of biometric unlocking (n=7, 5 experts) expressed that they were already resolved to not immediately adopt facial recognition. A non-expert (p27) felt the approach was "unnecessarily personal," and might be exploitable if Facebook's algorithms for facial recognition were also hacked. One expert (p26, an academic security researcher) echoed a common sentiment that new technologies were generally untrustworthy, and he felt it "would be better to wait to see how things play out."

Given this lack of recent and direct experience with facial recognition, it evoked doubt and concern about its security that fingerprint recognition had largely overcome in the same users. *The acceptance of one biometric method did not readily transfer to another, even on the same device.* Experts who had overcome their doubts and become fingerprint recognition users still expressed similar concerns about facial recognition. Participant 05, a recent user of fingerprint recognition, saw facial recognition as "still not controllable." Another expert (p35) thought it "strange for social norms," easier to fake, and potentially discriminatory. Even participants who had accepted facial recognition expressed doubt. A non-expert (p09) was dubious of the feature "doing lots of crazy stuff," and found the prospect of his facial signature being compromised "terrifying."

Context on fear of biometric signature compromise. It is worth observing that major concerns that security conscious

users commonly expressed about face and fingerprint recognition, namely that it could leak or be stolen off the device (rendering their face or fingerprint forever unusable), are not very likely. For example, Apple's TouchID feature (the most common biometric method among participants) is stated to only collect the scan of the user's finger in a format that is not reconstructable as a fingerprint scan. The imagery is also not tagged with that user's identity, not uploaded anywhere off the device, and is only stored and encrypted locally. A secure boot chain, system software authorization processes, and unique session keys also control how an Apple device's processor and Secure Enclave exchange information about the fingerprint scan, lessening the likelihood that malware could easily spoof a component to obtain sensitive biometric information [28]. Despite these safeguards, concern with biometric signature compromise transferred to experts' approach to setting up device access. For example, several experts (p15 and p30) deliberately limited the number of fingers they would register, either to have a reserve fingerprint if all others were compromised by a data leak or to reduce the perceived possibility of false positives. This fear of signature data leaks was acute for some experts. One expert (p30) explained, "I just assume it's going to get out at some point [his biometric signature]... I do think I will regret it. Hopefully not soon. Maybe it will only be iOS users." These overlapping instances of expert distrust and misunderstanding towards features including biometric registration, mobile financial transactions, and facial recognition and their impact on adoption and expert advocacy suggest a need for *tailored education for security-informed users*, discussed in Section 5.

Impact of 2015 San Bernardino shooting story on both experts and non-experts. News accounts of law enforcement efforts to unlock an iPhone belonging to a suspect in the 2015 San Bernardino shooting made a similar impression to that of biometric spoofing. Respondents (n=4, 1 expert) mentioned this as positively impacting their sense of security with their own device, since law enforcement appeared initially to be unable to unlock the phone. Of these participants, three of the four were non-experts. Other news stories drew mention as influences on authentication behavior, including compromise of biometric signatures in the Indian Aadhaar database and the 2013 Snowden leaks (p24, expert).

Expert and non-expert biometric usability issues

Participants described trying out but then abandoning some type of biometric unlocking (n=16, 9 experts), mostly attributed to usability problems and nearly evenly distributed between experts and everyday users (n=12, 7 experts). Many instances involved unreliable biometrics on older Windows laptops. One expert (p02) explained his frustration with the fingerprint reader on his Windows laptop, stating, "Nobody is getting in there with a fingerprint, including me usually."

Other users stopped using biometrics because they simply felt that PIN entry was quicker (n=2). However, several experts described security concerns that caused them to stop using a biometric unlocking method. One expert (p24) was alarmed enough by reported leaks of his phone's operating system code to stop using fingerprint recognition, while another (p05) disabled his laptop fingerprint reader after learning details of implementation in the operating system that he considered untrustworthy. One non-expert (p03) felt TouchID was too unreliable for regular unlocking and switched back to PIN use, but liked its added security enough to still use for authorizing purchases in applications.

Participants (n=17, 6 experts) also described other types of biometric usability problems. Again, many had struggles particularly with older laptop biometric unlocking. The most commonly described problem was relatively simple: wet or oily fingers not being read well (n=12, 4 experts). However, participants explained other theories for unlocking problems, including speculation that winter weather changes skin to make it unrecognizable, or that the phone itself might work less reliably when cold. Others guessed that the phone could only read fingerprints accurately at certain angles (n=2, 1 expert). Frustrated laptop facial recognition users, including experts, speculated that non-facial factors such as hairstyle or background lighting caused interference. A non-expert facial recognition user (p37) felt the feature very reliably identified him with different beard lengths, but failed if he switched from his regular sunglasses to his golf sunglasses.

Changing perceptions over time

Users noted a number of ways that their authentication approach had changed over time (n=13, 10 experts), but this type of observation was most commonly shared by experts. Their adjustments intended to add more security or try new methods with better usability and the same level of security. These security-enhancing actions included adding two-factor account authentication (p02), adding boot encryption to devices before travel (p04), and changing duplicate passwords (p15). One expert (p24) and non-expert (p37) also noted changes made after biometric adoption. p24 was comfortable enough with the security of fingerprint recognition on his phone to reduce his PIN from 6 to 4 digits for quicker entry and easier recall. Similarly, p37 shortened his screen lock time to make it less vulnerable if snatched, but felt that facial recognition unlocking was fast and reliable enough that more frequent unlocking produced by the change would not impose a time penalty.

Motivation for these changes, primarily made by experts, was keeping pace with hazards to secure mobile computing. Participants were asked about their preferred sources

Biometric method	Experts	Non-ex.	Total
Apple TouchID	10	12	22
Apple FaceID		1	1
Android fingerprint	7	5	13
Windows fingerprint	5	7	13
Windows facial	1		1

Table 4: Frequency of biometric authentication methods, by participant experience

Source	*n*	Source	*n*
Technology news sites	15, 8 experts	Social media	3, 2 experts
Trusted manufacturers	11, 7 experts	In-store tryout	2 non-experts
Academic sources	6 experts	Direct exposure	2 experts
Professional security organizations	6 experts	Hacker groups	1 non-expert
Friends	5 non-experts	Aesthetics of device	1 non-expert

Table 5: Participants' sources of information for making technology choices

of trustworthy security information, which were likely the same sources motivating their perception of risk and authentication changes. These sources are shown in Table 5. There were a number of differences between experts and non-experts. As stated previously, there are demographic differences between the groups, which might also affect were users want to get news and information, but the users were prompted to describe specifically the trustworthy sources they use for researching mobile technology choices. Both groups favored in similar proportions tech-specific web news sites (n=13, 8 experts, e.g. CNET Tech Radar, Ars Technica, WIRED). Two sources were exclusive to experts. Academic research (p26 called this "the tube I'm swimming in") was cited only by experts (n=6), as were publications of professional security organizations (n=5 experts, e.g. SANS Institute, FBI Infragard, Mandiant reports). Non-experts exclusively chose to ask (non-security trained) friends (n=5 non-experts).

5 DISCUSSION AND IMPLICATIONS

Tailored education for security-informed advocates. Experts clearly expressed more concern about mobile security, e.g., feared their biometric data being leaked (n=6, all experts), and concurrently showed enthusiasm for adoption of biometrics, e.g., experts were more likely to try biometrics immediately rather than wait (n=14, 11 experts). Given these observations, experts appear very motivated to improve security using biometrics, but more dubious about the integrity of mobile platforms, compared to everyday users. This distrust was acute towards mobile financial applications (13 users, only 3 experts). Researchers have described similar instances in which users' misunderstanding and lack of security knowledge was a disincentive to adoption of systems such as mobile tap-and-pay [14] and two-factor authentication [15]. Methods of invoking greater trust in biometric security for sensitive transactions would offer promise by explaining underlying protections in mobile operating systems and applications (obviously assuming they are correctly applied). In particular, research into the work of cybersecurity advocates suggests that their technical knowledge combines with a service orientation to provide direction and influence towards better practices by peers. Given this, tailored guidance describing biometric features that could overcome some of the misunderstandings we have documented should improve security adoption and outreach more broadly as better-informed expert users function as effective advocates [13].

Without such guidance, all users appear willing to form incomplete models of security from alternative sources. Non-expert and expert users are both aware of topical issues with mobile authentication and spoofing attacks. News stories such as the FBI attempting to unlock the San Bernardino shooters' iPhones (n=4, 2 experts) and online news articles about biometric spoofing (n=7, 3 experts) were both mentioned by similar rates of experts and non-experts and impacted the understanding of biometrics in both groups. Experts also spoke to concerns that seemed to re-purpose their existing knowledge of conventional network security concerns (e.g., malware keylogging or exfiltrating data) by projecting it onto the architecture of their mobile devices, which could be addressed by tailored education. Notably, there were several venues both expert and non-experts chose for trustworthy technology information (e.g. online technology news sites), or that were exclusively chosen by experts (e.g. academic studies on security and publications of professional security organizations) (see Table 5). This picture of where different types of users go with their security questions suggests promising venues for appropriately educating users.

Designing for device co-registration. Given how many activities are entrusted to mobile devices, it is unsurprising that both experts and non-experts shared devices with family and friends. Several factors were found to shape biometric co-registration, such as not understanding that it was possible (p32, non-expert) and impromptu nature of device sharing with family members (p25, expert). In both cases these obstacles prevented co-registration. Deep and unfamiliar device setting menus did not support users otherwise cognizant of biometrics from discovering and implementing co-registration they might have favored. Biometric setup dialogs could assist with this by more clearly indicating how related features work and presenting associated risks and benefits.

Usability consideration for work environments. Participants described a number of issues with authenticating on devices

Experts	Both	Non-Experts
• More influenced by work and BYOD requirements than non-experts • More likely to have used BAM immediately when available than non-experts • Change authentication approach more frequently than non-experts • Device choices more influenced by security concern compared to non-experts	• Frequently mistake biometric unlocking as the primary rather than secondary method • Equally likely to have stopped using biometric unlocking because of usability problems • Security concern motivated by fear of physical loss/theft • Similar proportions initially thought consumer biometrics were a bad idea	• Less concerned than experts about compromise of their biometric signatures • Less afraid than experts of using biometric unlocking on mobile payment/banking apps • Less likely than experts to have initially thought consumer biometrics were a good idea

Table 6: Overview of findings, by participant experience

supplied by an employer or co-employed for personal activities and work (a "blurry line," as p32 put it). In these instances, the users wanted to meet work-imposed obligations, but also add security features that were both secure and usable for frequent routine unlocking. In several cases (p01 and p05, both experts) the usability of older Windows-based work-required biometric features was frustrating and inadequate, and use was discontinued. However, those users' perceptions later changed with exposure to different biometric methods.

BYOD difficulties and concern were exacerbated by authenticating while traveling (e.g. experts p04 and p24), which often imposed exposure to observation in public spaces and untrustworthy wireless connections. Similarly, work requirements for authentication might be deemed inflexible for not acknowledging devices that never left secure spaces (e.g. expert p25). From these responses, we would suggest that BYOD policies should account for public and private usage to avoid complicating authentication and security configuration headaches that may ultimately only frustrate and demotivate users.

6 LIMITATIONS

We have discussed several potential limitations of this study in our Methods and Analysis sections. Although we attempted to balance for age and gender, challenges were experienced in recruiting female security experts. Our non-expert cohort was 37% female (n=19, 7 females), and expert cohort was 22% female (n=19, 4 females). However, a 2016 industry survey actually indicates a lower rate of 11% female representation among comparable cybersecurity professionals [11]. Nonetheless, while our sample size meets or exceeds that of similar security-related qualitative research [6, 10, 34], the expert cohort is older and more male. We have addressed instances where this might have an effect within our analysis, including discussion of expert BYOD requirements, device sharing and co-registration, and experts' views of biometrics before and after adoption. Further investigation using more fully balanced demographic samples may be necessary to establish generalizable results.

7 CONCLUSION

We have offered here a comparative picture of expert and non-expert adoption of biometric authentication methods (primarily fingerprint recognition), with a detailed explanation of what motivated differences between the two user groups. For most of these users, this was a relatively recent adoption process, and the experts involved offered a picture of the bargain they struck between their long-standing awareness of network computing risk and their desire for better mobile computing usability. At the same time, we were able to gather and compare initial perspectives of these users, already accommodated to fingerprint registration, towards facial recognition as it is being made more broadly available on consumer devices. Based upon these findings (summarized in Table 6), we have also presented the implications for effective biometric authentication posed by the issues raised by the participants. Several distinct points of misunderstanding and mistrust regarding biometric authentication were made clear, and we offer insight on how these implications can be addressed. Improvement along these lines can be expected to also ease users' acceptance of biometric-controlled application use.

8 ACKNOWLEDGMENTS

The authors wish to thank Jeff Romanowski (UMBC) for his help with data gathering. This work was supported by the Office of Naval Research (N00014-15-1-2776).

REFERENCES

[1] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. 2007. Mental Models of Security Risks. In *Financial Cryptography and Data Security*, Sven Dietrich and Rachna Dhamija (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 367–377.

[2] Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. In *Procedings of the Workshop on Usable Security (USEC)*.

[3] Antonio Bianchi, Yanick Fratantonio, Aravind Machiry, Christopher Kruegel, Giovanni Vigna, Simon Pak Ho Chung, and Wenke Lee. 2018. Broken Fingers: On the Usage of the Fingerprint API in Android. In *Proceedings of the Network and Distributed System Security Symposium, NDSS*.

[4] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2011. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy* 9, 2 (2011), 18–26.

[5] Jean Camp, Farzaneh Asgharpour, and Debin Liu. 2007. Experimental evaluations of expert and non-expert computer users' mental models of security risks. *Proceedings of WEIS 2007* (2007).

[6] Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, and Konstantin Beznosov. 2015. On the Impact of Touch ID on iPhone Passcodes..

In *SOUPS*. 257–276.

[7] Heather Crawford and Karen Renaud. 2014. Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management* 1, 1 (2014), 7.

[8] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 1, 12 pages. https://doi.org/10.1145/3173574.3173575

[9] Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1411–1414. https://doi.org/10.1145/2702123.2702141

[10] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. 2006. Decision Strategies and Susceptibility to Phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06)*. ACM, New York, NY, USA, 79–90. https://doi.org/10.1145/1143120.1143131

[11] The Center for Cyber Safety, Risk Management Education, Executive Women's Forum on Information Security, Frost Privacy, and Sullivan. 2017. The 2017 Global Information Security Workforce Study: Women in Cybersecurity. Retrieved July 05, 2018 from https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

[12] Batya Friedman, David Hurley, Daniel C. Howe, Edward Felten, and Helen Nissenbaum. 2002. Users' Conceptions of Web Security: A Comparative Study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems (CHI EA '02)*. ACM, New York, NY, USA, 746–747. https://doi.org/10.1145/506443.506577

[13] Julie M. Haney and Wayne G. Lutters. 2018. "It's Scary…It's Confusing…It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 411–425. https://www.usenix.org/conference/soups2018/presentation/haney-perceptions

[14] Jun Ho Huh, Saurabh Verma, Swathi Sri V Rayala, Rakesh B Bobba, Konstantin Beznosov, and Hyoungshick Kim. 2017. I Don't Use Apple Pay Because It's Less Secure...: Perception of Security and Usability in Mobile Tap-and-Pay. In *Workshop on Usable Security (USEC)*. 15–41.

[15] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices.. In *SOUPS*, Vol. 15. 1–20.

[16] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. My data just goes everywhere:âĂİ user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association Berkeley, CA, 39–52.

[17] Sevasti Karatzouni, Steven M Furnell, Nathan L Clarke, and Reinhardt A Botha. 2007. Perceptions of user authentication on mobile devices. In *Proceedings of the ISOneWorld Conference*. 11–13.

[18] Samsung Knox. 2018. https://www.samsungknox.com/en/knox-platform/knox-security Accessed: 2018-09-18.

[19] L. M. Mayron. 2015. Biometric Authentication on Mobile Devices. *IEEE Security Privacy* 13, 3 (May-June 2015), 70–73. https://doi.org/10.1109/MSP.2015.67

[20] W. Meng, D. S. Wong, S. Furnell, and J. Zhou. 2015. Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys Tutorials* 17, 3 (thirdquarter 2015), 1268–1293. https://doi.org/10.1109/COMST.2014.2386915

[21] Rawlson O'Neil King. 2015. *Mobile Biometrics Market Analysis*. Technical Report. Biometrics Research Group, Inc. https://www.biometricupdate.com/wp-content/uploads/2015/10/287127021-Mobile-Biometrics-Market-Analysis-5.pdf

[22] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 83–102. https://www.usenix.org/conference/soups2018/presentation/park

[23] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (2015), 121–144. https://doi.org/10.1093/cybsec/tyv008

[24] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories As Informal Lessons About Security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, Article 6, 17 pages. https://doi.org/10.1145/2335356.2335364

[25] Abdullah Rashed and Nancy Alajarmeh. 2015. Towards understanding user perceptions of biometrics authentication technologies. *International Journal of Computer Science and Information Security* 13, 6 (2015), 25.

[26] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia (MUM '12)*. ACM, New York, NY, USA, Article 13, 10 pages. https://doi.org/10.1145/2406367.2406384

[27] Elizabeth Stobert and Robert Biddle. 2015. Expert password management. In *International Conference on Passwords*. Springer, 3–20.

[28] Harry Thornburg. January, 2018. iOS Security Guide: iOS 11. Retrieved May 22, 2018 from https://www.apple.com/business/docs/iOS_Security_Guide.pdf

[29] Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. 2012. Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12)*. ACM, New York, NY, USA, 159–168. https://doi.org/10.1145/2420950.2420976

[30] Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the Wild: A Field Study of the Usability of Pattern and Pin-based Authentication on Mobile Devices. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '13)*. ACM, New York, NY, USA, 261–270. https://doi.org/10.1145/2493190.2493231

[31] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, New York, NY, USA, Article 11, 16 pages. https://doi.org/10.1145/1837110.1837125

[32] Rick Wash and Emilee Rader. 2011. Influencing mental models of security: a research agenda. In *Proceedings of the 2011 New Security Paradigms Workshop (NSPW '11)*. ACM, New York, NY, USA, 57–66. https://doi.org/10.1145/2073276.2073283

[33] Alma Whitten and J Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.. In *USENIX Security Symposium*, Vol. 348.

[34] Flynn Wolf, Ravi Kuber, and Adam J Aviv. 2018. An empirical study examining the perceptions and behaviours of security-conscious users of mobile authentication. *Behaviour & Information Technology* 37, 4 (2018), 320–334.