Pre-print from: Wolf, F., Kuber, R. & Aviv. A.J., 2018: How Do We Talk Ourselves Into These Things? Challenges with Adoption of Biometric Authentication for Expert and Non-Expert Users. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18, Montreal, Canada, LBW502

How Do We Talk Ourselves Into These Things? Challenges with Adoption of Biometric Authentication for Expert and Non-Expert Users

Flynn Wolf, Ravi Kuber and Adam J. Aviv
UMBC and USNA
{ flynn.wolf, rkuber } @umbc.edu, aviv@usna.edu

Abstract
Biometric authentication offers promise for mobile security, but its adoption can be controversial, both from a usability and security perspective. We describe a preliminary study, comparing recollections of biometric adoption by computer security experts and non-experts collected in semi-structured interviews. Initial decisions and thought processes around biometric adoption were recalled, as well as changes in those views over time. These findings should serve to better inform security education across differing levels of technical experience. Preliminary findings indicate that both user groups were influenced by similar sources of information; however, expert users differed in having more professional requirements affecting choices (e.g., BYOD). Furthermore, experts often added biometric authentication methods opportunistically during device updates, despite describing higher security concern and caution. Non-experts struggled with the setting up fingerprint biometrics, leading to poor adoption. Further interviews are still being conducted.

Author Keywords
Biometrics; Empirical study; Mobile authentication; Mobile security;

Introduction

Biometric authentication on mobile devices promises users a great deal. It ostensibly relieves them of recalling complex passcodes by replacing touchscreen interaction with simple, easy measurement of a unique personal feature. This seems like unequivocal progress; users avoid troublesome and error-laden memorization and data entry tasks and can instead unlock devices and services with a quick gesture or glance into a camera. Further, it removes human frailty from the authentication processes, such as choosing weak passcodes.

However, those with in-depth exposure to security technology issues are likely to have second and third thoughts about the promises of biometrics. Real concerns abound: uncertain rates for false positives may allow unauthorized access, the existence of numerous low-tech methods of biometric spoofing, and legal precedent that is unfavorable in compelling users to provide biometrics to unlock devices [11]. Like other security measures, informed users may dwell upon these disconcerting issues, but may react unpredictably in adoption and recommendation of biometric authentication [8]. Despite this, biometric methods, such as fingerprint and facial recognition, are proliferating on mobile devices in many contexts, including unlocking but also within other device applications, such as for authorizing financial

transactions with banking apps.

To understand user context in biometric authentication adoption, we conducted a preliminary study comparing security experts and non-expert users (expertise defined in Methodology). We asked participants to describe their views of biometric adoption, opinions of biometric usability and security during the adoption processing, and if any of those views have changed since adoption (or non-adoption). Essentially, we are trying to hammer down on the questions: how do we talk ourselves into these things, and do different groups do so using different information and understanding?

Existing research suggests that imparting a clear understanding of new security features, with the intent of shaping improved security hygiene, should be challenging for both experts and non-experts alike [2, 4, 7]. The goal of this research direction is to provide a detailed picture of adoption of new biometric authentication features across a range of security expertise which can serve to inform better security education and policy making. For example, several experts and non-experts alike reported in preliminary results that they were dissatisfied with the reliability and setup of their biometric unlocking features, attributable to incomplete instruction and explanation. A clearer comparative understanding of why this process is troubling for users will inform improved design.

We have an initial set of research questions, based upon thematic coding of a pilot study of eight participants, comprised of four experts and four non-experts:

- **RQ1:** Do workplace technology requirements affect experts/non-experts choices regarding biometric adoption, and does this effect differ?
- **RQ2:** Comparatively, how do experts and non-experts learn about and qualify the trustworthiness of new technologies, particularly biometric methods?
- **RQ3:** Do experts and non-experts differ in seeing biometric features as motivation for timing and selection of new mobile devices, or is it a lower/non-priority?
- **RQ4:** Does direct experience with biometrics change expert/non-experts' informed perspective on the security or usability of these features?

With additional data collection and analysis, we intend to further comparatively describe the relationship between security expertise and these facets of biometric authentication adoption, and use those findings to inform better designs for presenting biometric authentication to users from varying technical backgrounds.

Related Work

Considerable research has been conducted investigating how users, at various levels of expertise, build their own understanding of a how technology appears to work and how best to use it. Particularly, the "chain of causation" between users' mental models of network security concepts and their behavior has been explored. Wash [13] described eight folk models of hackers and viruses gathered from 33 qualitative interviews conducted in three mid-western American cities with non-security expert home

computer users. Stories about those topics impacted participants and led to misapplication network security advice. Rader et al. [10] also used a survey of 301 non-expert undergraduate technology students to explore sharing of home security stories, and how narratives individually shaped similar folk models.

Security stories and their models were found to often be incomplete and inaccurate, but also influential and not necessarily harmful to non-expert users practices. Topic modeling was used by Rader and Walsh [9] to examine the differences in how security information from different sources; news articles, peer stories, and web-based articles on computer security advice. The focus of these sources differed when describing threats to users via computer security scenarios. Peer stories focused on malicious actors, expert guidance on the mechanisms of attacks, and news articles on consequences. Research on mental models of security has also noted differences in how expert and non-expert technology users develop the opinions that underpin their behaviors. Examples include the study by Asgharpour et al. [2], who found experts and non-experts differed in understanding and communicating risk using computer security metaphors such viruses and zombies. Ion et al. [7] also surveyed security expert and non-experts, finding divergence in their acceptance and adherence to security practices such as two-factor authentication and frequent password changes.

Some of the challenges in establishing the linkage between user mental models and behavior have also been explored, including sometimes confounding disparity between IT security expertise and adoption of actual secure personal IT behaviors. Studies have noted the challenge in assessing underlying expert and non-expert mental models of security in areas such as online purchasing [8], as well as the potential insights of those sort offer to improved user interaction with security [12]. Looking more specifically at non-expert acceptance of mobile biometrics, DeLuca et al. found that surveyed mobile users cited usability and convenience rather than security as their prime motivation [6]. Bhagavatula et al. also found surveyed users attracted to Android and iOS fingerprint unlocking features compared to PINs, but noted lower acceptance of similar facial recognition methods [3].

Methodology

A 26-question interview instrument was prepared and iterated in eight semi-structured interviews (four experts, four non-experts). Security qualified participants were snowball recruited and by word of mouth through professional and academic associations. Non-expert users were also recruited by word of mouth within an academic setting. The questioning was designed largely around open-ended questions to encourage flexible and accurate reflection and recollection of opinions and experiences. Question iteration addressed improvements in the efficacy of individual questions and the topic order of the overall interview session.

A research memo process was employed to track themes and record rationales for any instrument changes. As cross response themes developed, 'member check' questions were added to examine

additional participants' responses to the concepts [5]. Interview responses averaged 25 minutes, and included an Institutional Review Board-approved document of consent.

The current interview instrument addresses basic demographics (Table 1), including years of security experience and personal mobile device usage (Table 2). Facets of personal usage examined include types of personal devices, operating systems, and authentication methods employed, duration of use, and opinions on usability and security. Responses have been examined with open thematic coding, clustering responses by their content.

Participants	Expertise	Age	Gender
p01	Expert (+45 years)	65+	M
p02	Expert (+3 years)	22-34	M
p03	Expert (21 years)	45-54	F
P04	Non-Expert	18-21	M
p05	Expert (10 yrs)	35-44	M
p06	Non-Expert	35-44	F
p07	Non-Expert	22-34	F
p08	Non-Expert	35-44	M

Table 1: Demographic Information

Participants	Devices
p01	Mac (FPR 1yr.), PC Laptops (FR 2yrs.), iPhone, FitBit
p02	Android Oxygen phone (FPR 1 yr.), Win 10 laptop (FPR 5 yrs.), Nintendo Switch
p03	iPhone (FPR 3yrs.), Mac laptop, iPad (FPR 1.5 yrs), FitBit
P04	iPhone (FPR 2-3 yrs.), Mac laptop, laptop, tablet
p05	Android phones, Win 7 & 10 laptops (FPR 3-4 months), Linux laptop, Amazon Fire tablet
p06	iPhone (FPR +4 yrs.), Mac & PC laptops, Amazon Kindles
p07	iPhone (FPR 1 yr.), Mac laptop
p08	iPhone (FPR 4 yrs.), PC laptop

Table 2: Personal Mobile Devices of Participants, inset: (years of biometric use) [FPR=fingerprint rec., FR= facial rec.]

We have used a one year threshold for exposure to network or cybersecurity issues, such as malware attack vectors and data loss scenarios, in professional or academic settings as basis for defining "expert" and non-expert" users. Our initial assumption was that security-informed participants would react differently to biometric security adoption than less security-informed users. One year of exposure is intended to be a reasonable threshold for sensitizing participants to security issues at an expert level, despite variation between academic fields and professional domains. Comparable standards for similar delineations in related work include those having taken a graduate level security course or having one year's work experience in the field [4], and those with a minimum of five years of work experience [7].

Years of experience with security issues amongst the expert cohort range from over forty in related government and industry positions (p01), to two years in military cybersecurity work (p02), averaging 18.25 years of relevant experience (SD=14.25). The amount of direct experience using biometrics on personal devices varied from 3-4 months to five years.

Discussion of Findings

One surprising aspect of the preliminary study is the mostly positive outlook of security experts towards biometrics. Contrary to our initial expectations, that experts would be reluctant to adopt biometrics, three of four experts reported largely positive initial views. The positive outlook is motivated by different factors for each participant. Some viewed biometrics positively for having the support of well-resourced trustworthy technology providers (p01), or practically as a more reliable and secure alternative to using multiple passcodes (p03). The single reluctant expert adopter felt that biometrics were not appropriate to data-sensitive devices because a biometric signature (fingerprint or face image) was less secure than PIN or alphanumeric passcodes against police seizure or criminal manipulation.

With regard to the research questions, RQ1-4, we have several early findings. Per RQ1, workplace requirements, in the form of Bring-Your-Own-Device (BYOD) policies and contract IT requirements, appear to influence authentication method choices, even for personal devices. Several expert participants mentioned that they must use certain types of devices because of work requirements (e.g. PC laptops for p01 and p05, both industry security professionals with government contracting experience). Most experts stated a preference for Apple products as more secure and usable, except for p05 (CIO of a technology services company), who felt iPhones and Mac laptops were more difficult to configure, relative to Android and Windows platforms.

The sources of information that shape understanding and acceptance of biometrics (RQ2) were also surprising. The non-expert and expert cohorts largely overlapped in their preferred sources, eschewing general news outlet reporting on technology as too shallow and sensationalistic, and instead seeking specialized industry sources. Non-experts were motivated and as adept at choosing similar sources as experts. P04, a non-expert, was actually the only participant to have tried-before-buying both fingerprint and facial recognition because of a personal investment interest in technology stocks. Experts differed primarily in their access to specialized threat reporting services such as FBI Infraguard (p01 and p05). However, as existing research into security adoption would suggest, even informed users are not always reliable in their adherence to security protections. Non-experts may misinterpret a limited picture of risk or technical functionality (e.g. p06 and p07, suspecting their unreliable fingerprint recognition might be attributable to temperature or something intrinsic about only their fingers). Similarly, expert users may choose to reserve their cautionary effort for only devices or scenarios they believe to have higher data sensitivity (e.g. p01, enabling two-factor authentication with biometrics on a work laptop with sensitive Human Resources data).

Regarding RQ3, most experts and non-experts reported starting to use biometrics only when they got a new device (both laptops and smartphones), although one expert stated it was a motivating factor in the timing of purchasing a new personal phone (p03, government and academic security researcher). This is intriguing, given that this cohort spoke extensively about their concerns and informed approaches for securing their data (e.g. using disk encryption and strict network isolation, etc.). They were almost unanimously positive on biometrics, yet did not deem it adequate motivation for the timing or selection of a new device, instead using it only once it was available because of other priorities.

Once exposure to biometrics occurs, experts and non-experts reported little change in their overall opinion of the security it provides (RQ4). Instead, change in outlook on the associated methods (primarily facial and fingerprint recognition) mostly centered on usability. Specifically, the rate of false negatives with both of those methods was described by participants, including experts, as a user experience issue. Only one participant (p02) described testing his fingerprint signature with another person for the possibility of a false positive. Otherwise, usability was understood in terms of common biometric performance factors (wet fingers affecting fingerprint readers and lighting problems with facial recognition causing false negatives). For example, non-expert users p06 and p07 largely stopped using fingerprint recognition because they found it to be much less reliable than entering their 4 or 6-digit PIN. Only one expert participant differed from this outlook. P05 was generally intolerant of any biometric use on data-sensitive devices, because he was unsatisfied with the integration of the fingerprint reader on his Windows laptop. He also understood his biometric signatures to be insecure from police seizure, and was concerned he could be coerced or tricked into unlocking a device.

Future Work

The preliminary results are promising, and as the next logical step in the research, we intend to collect and analyze fifty-two more interviews, counterbalanced for security expertise, to gain a deeper insight into the ways perceptions differ by group, and how these have evolved over time. Additionally, we are considering the use of a video-based prompt that appeals to fear of data compromise, as a discussion device [1]. The intent would be to use the content as a common article between experts and non-experts, and see how immediate and longer-term reactions and opinions may change in response.

Acknowledgments

The work is supported by the Office of Naval Research.

References

1. Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. 2017. "... better to use a lock screen than to worry about saving a few seconds of time": effect of fear appeal in the context of smartphone locking behavior. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS).

2. Farzaneh Asgharpour, Debin Liu, and L Jean Camp. 2007. Mental models of security risks. In Proceedings of the International Conference on Financial Cryptography and Data Security. Springer, 367–377.
3. 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 Proceedings of the Symposium on Usable Privacy and Security (SOUPS).
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. Juliet Corbin, Anselm Strauss, and Anselm L Strauss. 2014. Basics of qualitative research. Sage.
6. 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 Conference on Human Factors in Computing Systems. 1411–1414.
7. Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... No one can hack my mind": comparing expert and non-expert security practices. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS). 327–346.
8. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My data just goes everywhere:" user mental models of the internet and implications for privacy and security. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS). 39–52.
9. Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. Journal of Cybersecurity 1, 1 (2015), 121–144.
10. Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS).
11. Elliott Thompson. 2018. Understanding the Strengths and Weaknesses of Biometrics. (2018). Retrieved Jan 15, 2018 from https://www.infosecurity-magazine. com/opinions/strengths-weaknesses-biometrics/
12. Melanie Volkamer and Karen Renaud. 2013. Mental models–general introduction and review of their application to human-centred security. In Number Theory and Cryptography. Springer, 255–280.
13. Rick Wash. 2010. Folk models of home computer security. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS).