2-2015

Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption

Rasekhar BHAGAVATULA
Carnegie Mellon University

Blase UR
Carnegie Mellon University

Kevin IACOVINO
Carnegie Mellon University

Su Mon KYWE
Singapore Management University, monkywe.su.2011@phdis.smu.edu.sg

Lorrie Faith CRANOR
Carnegie Mellon University

See next page for additional authors

DOI: https://doi.org/10.14722/usec.2015.23003

Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption

Chandrasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe†, Lorrie Faith Cranor, Marios Savvides
Carnegie Mellon University, †Singapore Management University
{cbhagava, bur, kiacovin, lorrie, marioss}@andrew.cmu.edu, †monkywe.su.2011@smu.edu.sg

***Abstract*—While biometrics have long been promoted as the future of authentication, the recent introduction of Android face unlock and iPhone fingerprint unlock are among the first large-scale deployments of biometrics for consumers. In a 10-participant, within-subjects lab study and a 198-participant online survey, we investigated the usability of these schemes, along with users' experiences, attitudes, and adoption decisions. Participants in our lab study found both face unlock and fingerprint unlock easy to use in typical scenarios. The notable exception was that face unlock was completely unusable in a dark room. Most participants preferred fingerprint unlock over face unlock or a PIN. In our survey, most fingerprint unlock users perceived it as more secure and convenient than a PIN. In contrast, face unlock users had mixed experiences, and many had stopped using it. We conclude with design recommendations for biometric authentication on smartphones.**

I. Introduction

Researchers have proposed the use of biometrics for authentication, citing advantages like users not having to carry or remember anything [1], [2]. Biometrics could thus avoid common pitfalls with passwords like forgetting them or writing them down. Despite these advantages, the wide-scale adoption of biometrics has seemed just around the corner for decades.

However, the introduction of Android 4.0's *face unlock* at the end of 2011 [3] and the iPhone 5S' Touch ID (termed *fingerprint unlock* in this paper) two years later [4] has suddenly brought biometric authentication to the masses. For many users, this is their first real interaction with a biometric security system, and we therefore investigated why they did or did not choose to adopt these biometric systems for authentication. We also wished to study the real-world usability of these systems in both controlled settings and day-to-day life. Notably, users' expectations may derive from what they have seen in movies and the media as to the reliability and usability of such systems. To explore the usability of these schemes, as well as users' perceptions and attitudes about them, we conducted a laboratory usability study and an online survey.

In a within-subjects laboratory usability study, our ten participants found Android face unlock and iPhone fingerprint unlock to be easy to use in a number of common usage scenarios. The most notable exception was that no participant successfully authenticated with face unlock in a dark room. Contrary to our expectations, fingerprint unlock was relatively robust to hands covered in moisturizer. In a comparative ranking, most participants preferred iPhone fingerprint unlock over Android face unlock or traditional PINs.

Whereas our lab study focused on usability in specific scenarios, our 198-participant online survey investigated participants' experiences using these schemes in everyday life. The survey also delved into their perception of the convenience, security, and benefits of each platform, as well as their rationale for adopting or not adopting that scheme. The majority of respondents with an iPhone 5S reported that they currently used fingerprint unlock to authenticate and had very positive perceptions of the scheme's security. While some participants reported issues using fingerprint unlock with dirty hands, participants overwhelmingly perceived fingerprint unlock as more convenient than a PIN.

In contrast, few users of compatible Android phones said they currently used face unlock, though a handful had tried and subsequently abandoned it. These participants were less enthused than their iPhone counterparts about biometric authentication. In particular, authenticating in situations with dim lighting had caused problems for a number of users.

Our results suggest that iPhone fingerprint unlock is much closer to large-scale adoption than Android face unlock, yet both systems suffer from usability flaws. Throughout the paper, we make recommendations for improving both schemes' usability. We conclude with general design recommendations and future directions for biometric authentication on smartphones.

II. Related Work

Researchers have argued that the usability of biometric systems is of paramount importance and that usability is a crucial element in users' adoption decisions [5], [6]. Despite their advantages, biometric schemes have failed to see large-scale adoption in part due to usability issues; as a result, biometrics seem to remain the "perennial technology of tomorrow" [7].

The literature on biometric authentication is vast, yet most work focuses on purely technical aspects of biometric systems. Traditional performance measures for biometric systems only measure system-level errors and not the errors caused by human interaction, providing an unrealistic perspective on usability [8]. Furthermore, it is crucial to consider the entire ecosystem in which the biometric technology is used [9].

USEC '15, 8 February 2015, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2015.23003

A handful of researchers have conducted usability studies of biometric systems. In contrast to the systems we investigate, none of the biometric systems studied by other researchers have seen large-scale adoption by average consumers. Though they studied systems distinct from the ones we investigate, we adopt a number of their methods. Notably, taking into account focus groups, lab studies, and field trials of iris verification for ATMs, researchers have found a major distinction between users' attitudes towards biometrics prior to and following use of the technology [10]. We therefore focus on post-usage attitudes in our studies. Similarly, researchers have found that system responsiveness impacts the overall experience of biometrics [11], leading us to consider perceptions of overall system performance. Furthermore, researchers have argued that the design and evaluation of biometric systems should focus on traditional HCI dimensions like efficiency and satisfaction [12].

Like us, a handful of researchers have compared biometric authentication systems. For example, Trewin et al. compared face recognition, voice recognition, and gesture authentication to passwords on mobile devices [13]. They found critical usability flaws in all biometric mechanisms. Braz and Robert also comparatively analyzed many schemes, including face, fingerprint, and iris authentication [14]. They found the usability of all mechanisms lacking. In field trials with different biometric authentication schemes, Lassmann found iris recognition to be most usable, followed by fingerprint and face recognition [15]. Other studies have focused exclusively on the usability of fingerprint biometrics, finding that younger users and male users found fingerprint authentication more usable [16]. In contrast to the specialized mechanisms these researchers studied, we focus on off-the-shelf systems that have recently become widely available to average consumers.

User perception of a biometric scheme's usability is also a major factor in adoption. In their survey of fifteen biometric authentication schemes, Jain et al. identified acceptability of a biometric system as the driving force in that system's success [17]. They noted face recognition as one of six biometrics they believe has "high" user acceptability, whereas they believe fingerprint recognition has "medium" user acceptability. In our studies, however, we found that participants preferred iPhone fingerprint unlock over Android face unlock.

A number of researchers have studied overall perceptions of biometrics, yet not the consumer systems we study. Less than a decade ago, researchers found most study participants to be unfamiliar with biometrics or to lack interest in those technologies [18]. Even survey responsents who are open to using biometric systems can be wary about security, such as the possibility of using a photograph to fool a face-recognition system [19]. In contrast to perceptions about face recognition, researchers have found study participants perceive fingerprint authentication as both highly secure and highly usable [20].

User perception also impacts adoption [21]. Notably, reasearchers have found the acceptance of a fingerprint authentication system to change based on context (personal versus purchasing) [22]. Subtle issues in deployment, like the height of face scanners and the hygiene of fingerprint scanners, also have a major impact on perception and therefore adoption [23].

Although we are the first to investigate the biometric systems for unlocking iPhone and Android smartphones, two recent studies have investigated smartphone unlock behaviors using traditional authentication mechanisms. One group of researchers found that users spend a lot of time unnecessarily unlocking their phone and that many users fail to perceive any threat to the data on their phone [24]. The other group also found a strong correlation between locking behaviors and a user's perception of the risks, albeit a perception the authors believe underestimates actual dangers [25]. While smartphone users' perceptions of risk and attitudes towards locking their phone are implicit in our own study, we instead focus on the iPhone and Android biometric unlock mechanisms, which have not previously been studied.

III. Lab Usability Study

The first phase of our investigation was a within-subjects usability study of smartphone authentication mechanisms. In our lab, each participant used PINs, Android face unlock, and iPhone fingerprint unlock in five typical usage scenarios. While participants had great difficulty authenticating in a dark room using face unlock, most participants authenticated easily using fingerprint unlock with freshly moisturized hands, which we had expected to be challenging. We note a number of subtle usability issues with the schemes we tested.

A. Methodology

In April 2014 we conducted a within-subjects usability study of four unlock mechanisms: Android face unlock, iPhone fingerprint unlock, Android PIN unlock, and iPhone PIN unlock. We chose these schemes because they represent the biometric authentication mechanisms most widely supported on each platform at the time of research. When we began our study, no major Android model had a dedicated fingerprint sensor like the iPhone 5S. While Samsung later introduced a model with a dedicated fingerprint sensor [26] and though some third-party apps use the Android camera to simulate a fingerprint sensor, Android still does not widely support fingerprint authentication at the time of press. Similarly, while some third-party apps can unlock the iPhone through face recognition, Apple does not natively support this scheme at the time of press. We chose to use PINs as a baseline for comparison due to the ubiquity of PIN-based authentication.

Each participant came to our lab and used phones we provided to set up each unlock mechanism and then use the mechanism under five typical usage scenarios. The study took about one hour to complete. We compensated participants $10.

1) Study Structure: The study comprised a survey of demographics and opinions, a series of interactive tasks, and an interview. We began with a survey that collected the participants' demographics and prior experiences with smartphones and biometric systems. We also queried participants' perception of biometrics by asking them to rate their agreement with various statements about biometrics on a 5-point Likert scale. We were interested in these attitudes because users' initial perceptions may impact their willingness to try biometric authentication.

Participants then authenticated using a PIN code and the predominant biometric scheme on each platform. In particular, they used fingerprint unlock on an iPhone 5s, face unlock on a Samsung Galaxy S4, and PIN unlock on each phone. We provided participants with both phones and, to reduce

bias, assigned the PIN "1234." Participants first configured each scheme. Since we wanted to know how usable each of these schemes was perceived to be, we asked participants to rank the difficulty of each scenario on a 5-point Likert scale from "very easy" to "very difficult." We iterated through the four authentication schemes in random order to account for learning effects. We also asked the participant to describe any inconveniences they encountered configuring these schemes.

Each participant then authenticated using each scheme in five different scenarios: sitting, sitting in a dark room, walking, walking while carrying a bag in one hand, and sitting after applying moisturizer to their hands. We chose Aveeno Active Naturals Skin Relief Moisturizing Lotion because most participants in a pilot study noted this as their preferred moisturizer. We chose these five scenarios as representative of potential usability issues identified in prior work [13], [14], [16] and our own experiences. The sitting scenario was our baseline. We chose the dark room because people often use phones in the dark (e.g., outside at night or before going to sleep), yet the accuracy of face recognition suffers in the dark [13]. Similarly, walking with a bag is a common scenario for smartphone users, yet may cause authentication difficulties. We used the moisturizer scenario to see if moisture or sweat would cause usability issues for the fingerprint sensor. We had participants wipe off the mosturizer using wet tissues to avoid affecting any subsequent scenarios.

After each scenario, participants rated the difficulty of unlocking the phone with that scheme. We also recorded the number of failures to log in. After completing all five scenarios for a given scheme, we asked about any inconveniences encountered. Finally, we interviewed participants about their experiences and asked them to rank the four authentication schemes in order of preference. We asked followup questions about the rationale behind their ranking and their overall perceptions of the usability of each scheme.

2) Recruitment: We recruited participants via both an ad on Craigslist and flyers placed around the CMU campus and adjacent neighborhoods. Because we were interested in the usability of biometric authentication on smartphones, we screened for people who currently own either an iPhone or Android smartphone. Because we were interested in the usability of biometric authentication for a general population, we decided not to screen for prior use of biometric authentication.

3) Limitations: Our conclusions are limited due to the small sample size. However, by virtue of the within-subjects design, each participant tried each authentication scheme, enabling comparison. Nonetheless, the results of this study are most useful for identifying, rather than quantifying, potential usability issues. Our observations in this exploratory study informed our subsequent online survey. Each study participant performed each task only once. While this approach allowed us to observe first impressions, we were unable to observe learning effects or habituation.

B. Results

Ten people, eight male and two female, took part in our lab study. Our participants were relatively young; only two participants were over 30 years old. Four participants were regular iPhone users and six were regular Android users. Four participants were familiar with biometric authentication; two of them had previously used Android face unlock, while two others had previously used iPhone fingerprint unlock.

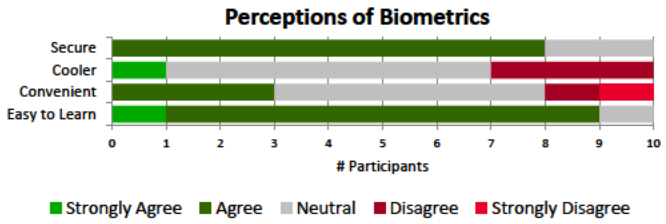

Fig. 1: Participants' responses to statements that biometric authentication systems on mobile phones "are very *secure*," "makes me look *cooler*," "are *convenient* to use every day," and are "*easy to learn.*"

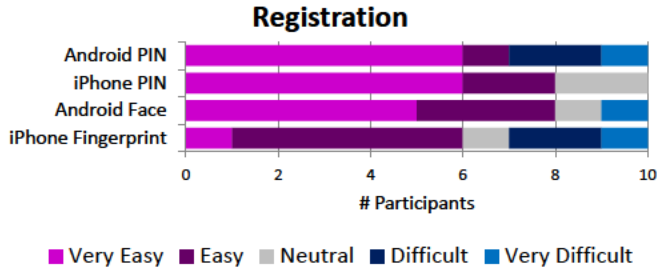

Fig. 2: Results of Likert-scale questions on the difficulty of the registration process.

1) Preconceived Perceptions of Biometrics: Before beginning the usability portion of our study, the majority of our participants already perceived biometric authentication on mobile phones as secure and easy to learn, though they were more skeptical about its convenience and "coolness." Figure 1 summarizes participants' perceptions. Nine of the ten participants agreed or strongly agreed that biometric authentication is easy to learn, while eight participants agreed with the statement that biometric authentication is secure. The potential convenience of biometric authentication was less obvious to participants; only three of the ten participants agreed that biometric authentication is convenient. These results are particularly interesting since they are at odds with the perception Android tries to convey to users. For example, when a user enables face unlock, Android warns the user that face unlock is actually less secure than other authentication schemes and should be used for convenience, not security.

2) Initial Setup (Registration): Participants found the process of initial setup (registration) relatively easy across all authentication schemes, as shown in Figure 2.

Six participants found registering a PIN code "very easy" on both Android and iPhone. The Android PIN registration process appeared slightly more difficult, however. Three participants rated Android PIN as difficult or very difficult, while no participant rated iPhone PIN below "neutral." This difficulty seems to be caused by Android requiring users navigate through a series of menus before selecting PIN authentication or any other scheme. The iPhone requires fewer clicks.

Many participants also found registration fairly easy for the biometric schemes. Eight participants rated registration as easy or very easy for Android face unlock, while six participants rated iPhone fingerprint unlock as easy or very easy. Though participants did not find either process particularly difficult, participants found the Android face registration process easier than iPhone fingerprint registration. Only one participant felt iPhone fingerprint registration was very easy, whereas five participants felt Android face registration was very easy. When asked to clarify this distinction, seven of the ten participants complained that the iPhone fingerprint registration lacked clear instructions, particularly in contrast to the other schemes. For example, P3 explained, "The image they were showing me didn't make sense to me, so I was like I'm not sure which way I'm supposed to be like turning my finger. So that was kind of difficult." Furthermore, during the second phase of registration, the user is asked to grip the phone differently to capture more of the fingerprint area. Unfortunately, many participants did not understand how far they needed to move their finger. Clearer instructions, perhaps with a video or animation, might help.

Unlike iPhone fingerprint registration, Android face registration did not experience any widespread usability problems. That said, a few participants said it takes too long or is awkward to hold the phone during registration. Some complained about positioning the image of their face within a circle on the screen, which required holding the phone at arm's length in just the right position. P7 explained, "I have to place the phone [so that my face is] in the circle mentioned. I mean it should probably detect my face anyway."

Notably, none of the participants took advantage of the option to improve face recognition, which appears following registration. This option enrolls examples of the face in different situations to ensure that the user's face is recognized in multiple scenarios. Participants' tendency to skip this optional process might have caused some of the scheme's inaccuracy under different scenarios, as we detail later in this section. By making this step obvious or perhaps mandatory, face unlock may become more robust and thereby gain greater acceptance.

3) Unlocking The Phone: In the five usage scenarios we investigated, the comparative usability of the authentication schemes differed. For our baseline of the participant sitting in a chair, nearly every participant found each of the schemes to be easy to use (Figure 3). One participant, however, had difficulty with face unlock when he did not point the phone's camera at his face. Instead, he left the phone on the table and assumed it would unlock. After pointing the camera at his face, he still experienced difficulty due to a timeout in the authentication process. Finally, on the third attempt, he authenticated. This difficulty may be caused by a difference between the appearance of the phone's screen during registration and during authentication. At no point is a user told what the screen should look like. This difficulty could be mitigated by presenting unlocking instructions following registration.

Trying to authenticate while seated in the dark was highly problematic for Android face unlock, but not for the other schemes. While authenticating in the dark is a known issue for face recognition [13], users often need to authenticate in the dark. Unfortunately, not a single participant in our study was able to authenticate using face unlock in the dark. As a result, everybody rated it as either "difficult" or "very difficult,"

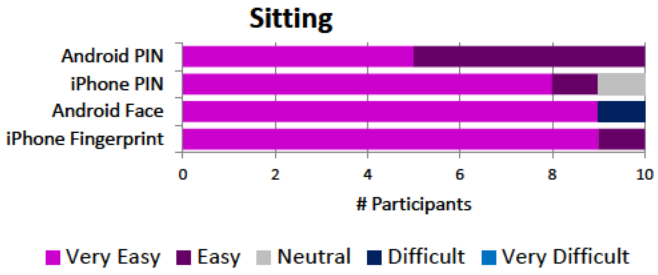

Fig. 3: Participants' perceptions of the ease of authentication while seated, which was our baseline scenario.

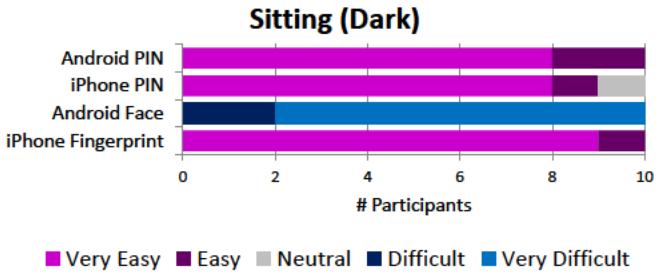

Fig. 4: Participants' perceptions of the ease of authentication while seated in a dark room.

as shown in Figure 4. In contrast, nine of the ten participants rated authentication in the dark as "easy" or "very easy" for the three other authentication schemes. One possible solution to face unlock's usability issues in the dark is for the phone to detect when it is too dark to recognize a face and to switch automatically to a backup authentication scheme. Android face unlock requires users have configured a backup authentication scheme anyway, so this dynamic adjustment would not add additional registration overhead.

Contrary to our expectations, participants did not find unlocking to be difficult for any authentication scheme in either of the walking scenarios. As shown in Figure 5 and Figure 6, eight or more participants found unlocking "easy" or "very easy" in both walking scenarios for each authentication scheme. The iPhone fingerprint unlock, however, was more commonly rated "easy," as opposed to "very easy." Participants explained that in order to use your fingerprint, you have to hold the phone on the bottom. Doing so was a little more awkward while walking, especially doing so using one hand. As P2 explained, "Spatially, my finger was wider, so I had to think about where I was putting it."

We chose the final scenario, authenticating after applying moisturizer to the hands, to reflect what might happen when a user is sweaty: distorted fingerprint readings causing a drop in performance. Contrary to our expectations, most participants did not experience problems authenticating with fingerprint unlock. As shown in Figure 7, only two participants encountered difficulty. One participant applied a large amount of moisturizer to their finger without spreading it around at all, occluding the finger. We believe this behavior to be atypical. However, all participants preferred using face unlock after applying moisturizer since they did not have to touch the screen, leaving it clean. This result exposes face unlock's advantage of not requiring contact with the screen when the

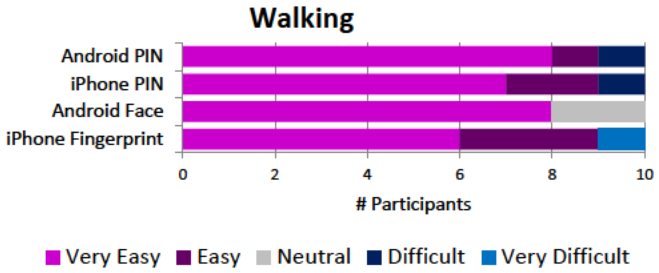

Fig. 5: Participants' perceptions of the ease of authentication while walking.

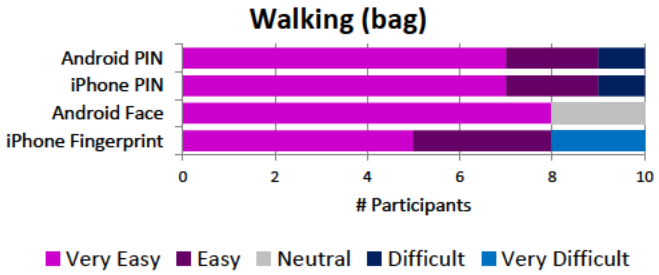

Fig. 6: Participants' perceptions of the ease of authentication while walking and holding a bag in one hand.

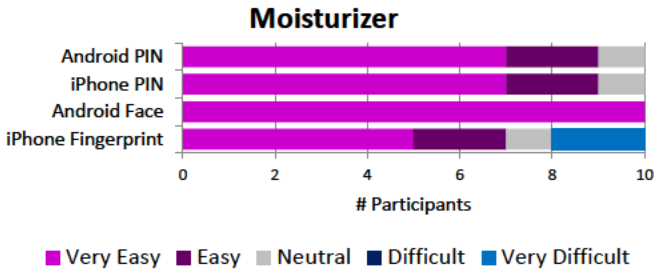

Fig. 7: Participants' perceptions of the ease of authentication while seated after having applied moisturizer to their hands.

user has sweaty, dirty, or greasy hands. Of course, what the user can subsequently do on their phone without touching the screen is another matter.

4) Ranking of Authentication Schemes: At the conclusion of the usability tests, we asked participants to rank the schemes. Participants generally preferred the two iPhone schemes, fingerprint unlock and PIN. As shown in Figure 8, six of the ten participants ranked iPhone fingerprint unlock as their favorite, while eight of the ten participants ranked the iPhone PIN scheme as either their first or second choice. Participants frequently credited the smaller iPhone as being easier to use than the Samsung Galaxy we tested. Furthermore, they noted that the iPhone PIN authentication does not require the user to hit "enter" after inputting the PIN.

While six participants ranked fingerprint unlock as their favorite, reaction was quite polarized; the remaining four participants said it was their *least* favorite. Participants who disliked fingerprint unlock cited the confusing and time-consuming registration process as their primary gripe. By clarifying registration instructions and shortening the enroll-

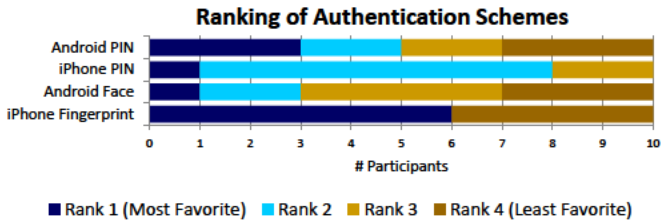

Fig. 8: Participants' ranking of the authentication schemes.

ment process, fingerprint authentication may gain greater acceptance. However, the impact of shortening the enrollment process on system accuracy is a major concern.

Participants mostly disliked Android face unlock. Seven participants ranked it either last or second to last among the four schemes. These participants said holding the phone in front of them was awkward, particularly if they were to use it in public. Often, in order to get enough lighting and an appropriately sized face in the frame, they would have to hold the phone out in front of them. Some stated this would be inconvenient if there were lots of people around, and it would also look too much like they were taking a selfie. They did not want this inconvenience to occur every time they needed to unlock their phone. Participants stated that this would make them look uncool and draw too much attention to themselves. Furthermore, they did not like having to hold the phone at arm's length to make sure the face was inside the required area. In contrast, Android PIN authentication was almost evenly distributed in participants' rankings, likely indicating that participants did not feel strongly about it.

IV. Online Survey

While our laboratory study revealed usability issues with both biometric authentication schemes we investigated, we did not gain a sense of usability in the wild, nor what factors influence users' adoption (or non-adoption) decisions. To that end, we conducted an online survey in September 2014 focused on impressions of, experiences with, and adoption decisions related to Android face unlock and iPhone fingerprint unlock.

To probe actual experiences and adoption decisions among potential users, we screened for participants who owned a phone model that supported either Android face unlock or iPhone fingerprint unlock. Following the Technology Acceptance Model (TAM), first put forth by Davis [27], our survey focused mostly on the perceived usefulness and ease of use of the systems. Since we were focusing on authentication schemes, we defined the usefulness of the system as how secure the scheme is, or how well it protects the phone from being used by others. The ease of use of the system encompasses scenarios in which the system worked well for the users, as well as their general perceptions of how convenient the system was to use. These two factors have been shown to be correlated with user acceptance of a system [27], which is why we chose to focus on them.

We found that few Android survey participants, each of whom used a device that supported face unlock, had adopted face unlock. A slight majority of current face unlock users felt

it to be more convenient and more secure than a PIN, whereas former face unlock users had very mixed opinions about the scheme's security and convenience. A number of face unlock users noted issues with using it in the dark.

In contrast, the majority of our iPhone 5S survey participants currently used fingerprint unlock, overwhelmingly perceiving it as more secure and more convenient than a PIN. Whereas few participants in our lab study had difficulty using fingprint unlock even after applying moisturizer, many survey participants reported issues authenticating with dirty or greasy hands. Alarmingly, a sizable fraction of fingerprint unlock users noted the convenience of the scheme for authenticating while driving an automobile.

A. Methodology

We recruited owners of a phone supporting biometric authentication. In particular, owners of Android phones running version 4.0+ of the operating system and owners of the iPhone 5S were eligible. We restricted our survey to owners of those phones because we were only interested in the impressions and adoption decisions of users whose phones already support biometric authentication. We chose to include users of these phones who had never used biometric authentication because we were curious why they had chosen not to adopt these schemes. As with our laboratory study, at the time of our research and the time of press, Android did not widely support fingerprint unlock and the iPhone did not natively support face unlock. As a result, we asked iPhone owners only about fingerprint unlock and Android users only about face unlock.

Following the online consent process, we asked about demographics and general phone unlock behaviors, building upon questions from prior work on phone unlocking [24], [25]. We also gauged participants' familiarity with biometric authentication features on their smartphone. Based on the participant's familiarity with these features, as well as their status as a current user, former user, or non-user, the remaining survey questions followed a branching approach tailoring questions to their prior experiences. To discourage biased responses designed to game the survey, this branching generated approximately the same number of questions regardless of the branching. To provide a baseline understanding of biometric authentication, we showed all participants a brief description of their phone's biometric authentication system regardless of the participant's stated familiarity with biometric authentication.

We asked current users of biometric authentication why they used it, what advantages and disadvantages they had noticed compared to other schemes, and what issues, if any, they had encountered. For iPhone fingerprint unlock, we asked if they had run into issues while seated, while walking, or in any other situation. For Android face unlock, we asked if they had encountered any issues at night, indoors, or in any other situation. If the participant had previously used biometric authentication, yet had stopped, we asked the same questions in the past tense, along with questions about why they had stopped using the scheme. We asked participants who said they had never used their phone's biometric authentication scheme why they had not, what they perceived to be advantageous and disadvantageous about the scheme, and what, if anything, might make them choose to use such a scheme.

If the participant had ever used the biometric authentication scheme on their phone, we asked participants to respond to a series of statements on 5-point Likert scales. These questions gauged whether biometric authentication took more or less time, resulted in more or fewer errors, were more or less convenient, and seemed more or less secure than their current or previous authentication scheme. We also asked them to elaborate on specific scenarios in which they found the biometric scheme to be more or less convenient, as well as listing any scenarios in which they had seen someone fool the biometric authentication scheme.

We compensated participants $1.00 for the survey, which took an average of 9 minutes to complete. We excluded participants who failed to verify ownership of an appropriate phone, as described below.

1) Recruitment: We recruited on Amazon's Mechanical Turk (MTurk) crowdsourcing service for a survey on smartphone usage. We restricted the survey to MTurkers age 18+ and located in the U.S. who had completed at least 50 tasks with an approval rating of 95%+. We stated that the survey was open only to current users of Android 4.0+ or the iPhone 5S, the models that support face unlock and fingerprint unlock.

To ascertain that we only surveyed users whose current phones support biometric authentication, we included a question to verify the participant's ownership of an appropriate phone. For the iPhone 5S, we asked participants to type exactly what is written as the two options for Touch ID in "Settings → General → Touch ID & Passcode -> Touch ID on your iPhone 5S." We asked Android participants to enter the third unlocking scheme listed in "Settings → My Device → Lock Screen → Screen Lock along with the security level listed underneath." Unlike the iPhone, which had only one set of correct answers, we accepted as valid any answer that contained "face unlock" or "face and voice." The precise wording varied based on the Android phone model and service provider.

We initially recruited 100 participants for the Android survey and another 100 participants for the iPhone survey. As we discuss in the results, few of the Android respondents had ever used face unlock. Therefore, we reopened the survey, but instead advertised it prominently as only for current or former users of "Android face unlock."

2) Analysis: Our survey was not a controlled experiment, so we do not perform any statistical comparisons. Instead, we report the frequencies of participants' perceptions, attitudes, and adoption decisions. While some survey questions were multiple choice, we included 28 open-ended questions across the different branches of the survey to delve into participants' attitudes. To analyze open-ended responses, members of the research team read through all responses and iteratively developed a codebook on a per-question basis. The number of codes per question varied, but ranged from two to fourteen. Two coders independently applied these codes. Across all questions on both surveys, their percentage agreement was 87.4%. The coders discussed disagreements and came to consensus; we report these consensus codes.

From the Likert-scale data, we report perceptions of security and convenience for each of the biometric authentication schemes versus baseline PIN authentication. Since we wanted to see what issues may drive adoption decisions by the general

public, it is important to investigate the perceptions of those who have used these systems in the past.

B. Findings of the Android Face Unlock Survey

We initially collected data from 100 participants, yet only a single person reported currently using face unlock. An additional 15 participants had previously used face unlock. As discussed in the methodology, we reposted a survey restricted to current and former users of face unlock to enable parallel analyses of current users, former users, and non-users. Another 63 participants responded to our second survey.

Out of the 163 total respondents, we analyze data only from the 109 participants who passed the validation question. These 109 participants included 47 women, 61 men, and one person who did not specify. Our participants included 12 people with a post-graduate degree, 33 who held a bachelor's degree, 14 who had an associate's degree, 36 additional participants with some college education, and 14 participants without college education. Of our participants, 3% were under 20 years old, 54% were 20–29, 33% were 30–39, and the remaining 10% were age 40 or above.

1) Current Users of Android Face Unlock: Of the 109 participants, 17 (16%) currently use face unlock. Participants commonly said they use face unlock for increased convenience and security over other authentication schemes; all but one current user indicated one or both of these reasons. As P-A91 explained, face unlock "is fast and convenient when I can't focus on typing in a PIN." Similarly, P-A113 uses face unlock "because it ensures ONLY I can unlock it unless someone knows my pin code as well- which hopefully no one does."

As shown in Figure 9, two-thirds of current face unlock users considered face unlock to be more secure than using a PIN. This result is particularly notable for its dissonance with reality, supported by Android's notification when a user enables face unlock that it is *less* secure than other methods. By design, face unlock is only as secure as the backup authentication scheme (e.g., PIN) that Android requires face unlock users to have enabled. The required backup authentication scheme can always be used in place of face unlock. Although the current implementation of face unlock objectively cannot be more secure than a PIN, most of our participants seemed to perceive face unlock in the abstract as inherently more secure. Participant P-A113, quoted above, even mentions that if an attacker knows only their PIN, the attacker can gain access to the phone even if face unlock is set up. Regardless, P-A113 believes face unlock to be more secure than using a PIN. Of course, the vulnerability of face recognition schemes to photographs of a valid user are well known [19], yet so is the tendency of users to pick predictable PINs [28].

Current face unlock users also lauded the scheme's convenience, as shown in Figure 10. Nearly two-thirds of current users stated that face unlock was more convenient than a PIN. In free-response answers, users noted the convenience of face unlock when the user's hands are occupied or when they want to unlock their phone quickly. Echoing the findings of our lab study, the most common situation where face unlock was less convenient was in dimly lit rooms. Participants reported that, in low light settings, face unlock fails very often, causing frustration. Indeed, 65% of current users cite the reliability

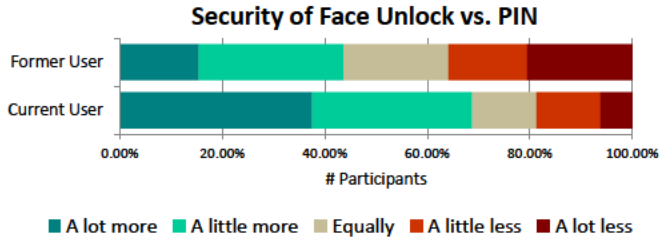

Fig. 9: Current and former face unlock users' perceptions of face unlock's security compared to traditional PINs. While the majority of current users found face unlock *a little* or *a lot more* secure than a PIN, former users had mixed opinions.

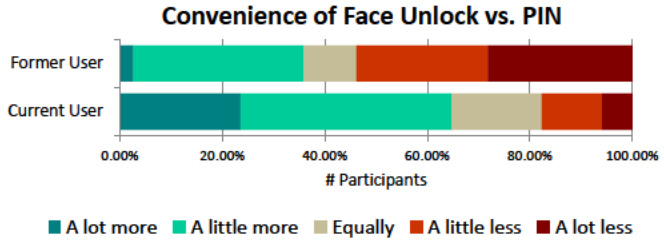

Fig. 10: Current and former face unlock users' perceptions of face unlock's convenience compared to traditional PINs. While the majority of current users found face unlock *a little* or *a lot more* convenient than a PIN, the majority of former users found face unlock *less* convenient than a PIN.

of face unlock as its main disadvantage. Despite this stated disadvantage, these users have continued to use face unlock.

2) Former Users of Android Face Unlock: Of the 109 valid participants, 40 participants (37%) had previously used face unlock, yet had stopped doing so by the time of the survey. The majority of these former users (25, 63%) said they had tried face unlock out of curiosity, not necessarily for security or convenience. For example, P-A112 said, "It seemed like a fun new thing to try out. So I did try it out." This result seems to indicate that the novelty of face unlock was enough to encourage people to try it, yet it was not sufficiently compelling to continue using.

Why is it, then, that these participants did not use face unlock? The most commonly cited reasons for discontinuing use were that face unlock was unreliable (18 participants, 45%) and that it was inconvenient to use, as discussed below. Eight participants specifically noted adapting to difficult lighting conditions as face unlock's main reliability issue. As P-A132 explained, "I stopped using it because at times I would be in a place where there isn't much light, so my phone couldn't recognize me. In the end, it became a hassle." This sentiment exemplifies the common complaint that face unlock was a hassle or inconvenient.

As shown in Figure 9 and Figure 10, former face unlock users were split about whether face unlock is more or less secure than using a PIN. Most former users, however, found it to be less convenient than a PIN. Overwhelmingly, these former users listed low-light situations (20 participants, 50%)

as a major downside of face unlock, particularly compared to their replacement authentication scheme. Six participants (15%) stated that face unlock was inconvenient when they were in a hurry, while another six participants (15%) said face unlock was less convenient in all situations. This result seems to indicate that after some use, many people encounter situations where face unlock is inconvenient, dissauding them from continuing to use it.

3) People Who Have Never Used Face Unlock: We were curious why the remaining 52 participants (48%) had never used face unlock despite having a phone that supports that form of biometric authentication. Three main reasons dominated. Most commonly, participants said they had never heard of face unlock (15 participants, 29%). Despite never trying face unlock, thirteen others (25%) expected face unlock would be too much of a hassle to use. These participants expressed particular concern about how long it would take to unlock the phone. Another twelve participants (23%) expressed concern about the security of face unlock on Android phones.

When asked what would compel them to use face unlock, participants commonly cited curiosity (19 participants, 37%), echoing the most common reason former users had initially tried face unlock. Some participants said that they would try face unlock after completing the survey because they were now better informed about it. For example, P-A105 said, "Reading about the feature has compelled me to try face unlock when I'm done with this survey. So I guess you could say this survey compelled me!" However, 12 participants (23%) said nothing would compel them to try face unlock.

When asked what they expect to be the biggest disadvantage of using face unlock, even participants who had never used it before commonly cited face unlock's expected high failure rate. A total of 15 participants (29%) listed reliability as the biggest disadvantage, while 10 participants (19%) each listed lighting conditions and the length of time needed to unlock the phone. This result suggests that people generally can predict situations in which face unlock would not work. It is possible that because they can predict these situations, they are particularly reluctant to try face unlock without guarantees of its reliability. As P-A132 wrote, face unlock "could possibly take a while to unlock your phone, if you had to have correct lighting or align your face correctly. If you had to unlock in a hurry or in the dark, it might be a disadvantage."

C. Findings of the iPhone Fingerprint Unlock Survey

A total of 101 MTurkers responded to our iPhone 5S survey. Of these 101, 89 passed the validation question. These 89 valid participants included 35 women and 54 men. There were 12 participants with a post-graduate degree, 47 who held a bachelor's degree, 5 with an associate's degree, 18 who had some college education but no degree, 4 high school graduates, and 3 participants with some high school education. The age distribution was similar to the Android survey; 4% of our participants were under 20 years old, 55% were 20–29, 33% were 30–39, and the remaining 9% were at least 40 years old.

1) Current Users of iPhone Fingerprint Unlock: Whereas only a fraction of respondents to our Android 4.0+ survey had ever used face unlock, the majority of respondents to our iPhone 5S survey were current users of fingerprint unlock.

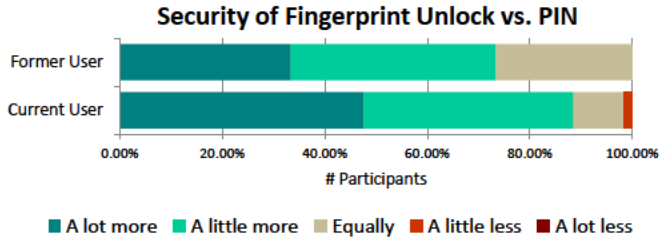

Fig. 11: Current and former fingerprint unlock users' perceptions of fingerprint unlock's security compared to traditional PINs. The majority of current and former users felt fingerprint unlock *a little* or *a lot more* secure than a PIN.

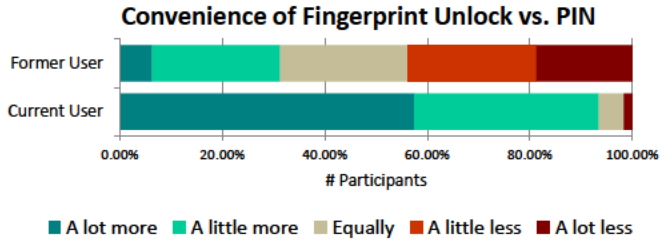

Fig. 12: Current and former fingerprint unlock users' perceptions of fingerprint unlock's convenience compared to traditional PINs. While nearly all current users found finger unlock *a little* or *a lot more* convenient than a PIN, less than one-third of former users concurred.

A total of 61 of the 89 valid participants (69%) currently use fingerprint unlock as their iPhone authentication scheme. Forty-two of these current users (69%) stated that they use fingerprint unlock out of convenience, while 25 of them (41%) cited security reasons. The convenience of fingerprint unlock appears to come both from it being either quicker or easier than other authentication methods. As P-I142 states, "It's really quick and saves me from having to type my Apple ID password when I am lazy."

As with Android face unlock, we observed a disconnect between participants' perceptions of security and actual security. As shown in Figure 11, most current fingerprint unlock users felt fingerprint unlock to be more secure than a PIN. For example, P-I162 wrote that fingerprint unlock "is harder to break through than a numeric code." Notably, however, the iPhone requires a PIN be set up as a backup to fingerprint authentication. Therefore, it suffers from the same vulnerability as Android face unlock that an attacker who guesses the PIN circumvents fingerprint authentication.

In contrast to our lab usability study, where the application of moisturizer did not have a large effect on the accuracy of the iPhone fingerprint reader, 34 of our survey participants (56%) reported incidents of unreliability as fingerprint unlock's biggest disadvantage. Commonly, participants cited water from the rain, sweat, and grease as causes of unreliability. As P-I147 explained, fingerprint unlock "doesn't always work. Sometimes my fingers will be greasy or the phone will be dirty and it won't recognize my fingerprint."

Nevertheless, over 90% of current fingerprint unlock users found fingerprint unlock to be a lot or a little more convenient than a PIN, as shown in Figure 12. In fact, 40 of the 61 current users (66%) cited fingerprint unlock's convenience as the scheme's single biggest advantage. Given that these responses all came from current users of fingerprint unlock, the scheme's overall convenience seems to outweigh the situations in which the sensor does not read the finger correctly.

When asked to relate a scenario in which fingerprint unlock was more convenient than alternative authentication schemes, 12 current users (20%) specifically mentioned using fingerprint unlock while driving. This convenience could be a potential safety hazard; if fingerprint unlock makes using a phone too convenient, people may be tempted to use their phone more while driving. That said, most of these participants mentioned liking that fingerprint unlock distracts them less than other authentication schemes while driving. For instance, P-I79 calls out the advantages of fingerprint unlock "when driving, so I don't need to look down on my phone." While it may be a positive that drivers do not need to take their eyes off the road to unlock their phone, it is not clear whether they are able to use their phones subsequently without looking at them.

D. Former Users of iPhone Fingerprint Unlock

Sixteen participants (18%) had tried fingerprint unlock, yet decided not to continue using it. Although our Android and iPhone samples are distinct and therefore cannot be used to reach any definitive conclusions beyond observations, iPhone fingerprint unlock appears to have a much higher retention rate than Android face unlock. Eleven of these 16 participants (69%) stated that they had originally tried fingerprint unlock out of curiosity because it was a new Apple feature.

As with face unlock, the most common reason given for discontinuing use was that fingerprint unlock performed unreliably (7 participants, 44%). We did not observe a consensus toward any other reason for abandoning fingerprint unlock. We hypothesize that some users merely tired of it. For example, P-I24 stated, "I just tested it and just do not think about it," while P-I115 stated, "Because I started being at home all day and didn't need [authentication]."

Surprisingly, as shown in Figure 11, every former user of fingerprint unlock felt that fingerprint unlock was at least as secure as a PIN. However, these former users had far more mixed opinions about convenience, as shown in Figure 12. Many former users thought the best thing about fingerprint unlock was that they did not have to remember anything, which is true of all biometrics. Unfortunately echoing current users, the most common scenario for which former users noted fingerprint unlock's convenience was its use while driving (5 participants, 31%).

E. People Who Have Never Used Fingerprint Unlock

The remaining 12 participants (13%) had never used fingerprint unlock. We did not observe a strong consensus as to why. Some participants were just not interested in configuring the mechanism. However, a few participants stated that they actively did not trust Apple with their biometric data. For example, P-I49 wrote, "Although Apple states that the fingerprint resides on the device and not uploaded into the cloud, I do not trust it. I do not want to inadvertently share my biometric data with the rest of the world."

Unexpectedly, eight of these non-users (67%) said they felt fingerprint unlock's greatest advantage was security. This contrasts sharply with the opinion of current and former users, who far more commonly cited convenience as fingerprint unlock's primary benefit. We hypothesize these non-users are not fully aware of fingerprint unlock's convenience. Some non-users, however, identified expectations of a high failure rate as the primary reason for not using fingerprint unlock.

V. Conclusions and Design Recommendations

In both our lab usability study and online survey, we found a mix of successes and failures in one of the first large-scale deployments of biometric authentication for average users. Convenience and usability were key factors in positive adoption decisions, yet further improvements in usability could go a long way in encouraging non-users to reconsider the pros and cons of biometric authentication for their use cases. Our online survey confirmed our intuition that a number of prospective users have tried biometric authentication on their new phones out of curiosity.

Whereas few participants in our online survey used Android face unlock, iPhone fingerprint unlock seemed to enjoy wide adoption. This difference in adoption may stem from fingerprint unlock being perceived as faster, cooler, and more accurate. Both mechanisms fail in specific scenarios, wet fingers and dark rooms, respectively, yet fingerprint unlock seemed to have been adopted at a much higher rate. We hypothesize that these usability failures are not quite comparable, however, because people will want to use their phone in a dark area more often than when they have wet fingers. For any biometric scheme, it is crucial that developers account for the scenarios in which people often use their phone, and usage in dimly lit or dark areas is common. While we did not specifically ask about scenarios like using the phone in the rain, vibrations from travel in a vehicle, or interference from other people, no participants in either study brought up these scenarios as issues in the free-response portion of the studies.

Usability issues were a major driver of users' adoption decisions. To spur adoption, Android face unlock in particular could benefit from fixing its major usability flaw: unlocking in low-light environments. While a radical refactoring of Android's approach to face unlock might automatically illuminate the user's face in the dark, perhaps even using infared light to minimize interrupting the user, we have two simpler recommendations for improving face unlock. First, the 'improve face recognition' option should be more obvious to users. This option, intended to increase the reliability of the face unlock scheme, could conceivably help in low-light scenarios, but only if users take advantage of it during registration. Second, the smartphone should detect automatically whether face recognition has enough light to work. If it does not, the phone should switch to the secondary authentication scheme without requiring the user to attempt face recognition first. Doing so may alleviate some of users' frustration since they will not have to wait for biometric authentication to fail before falling back to the secondary mechanism.

The iPhone fingerprint unlock could also benefit from usability improvements, albeit in a more minor way. Even though many survey participants said the fingerprint unlock did not work when their fingers were wet, this shortcoming did not cause many of them to stop using fingerprint unlock. However, given some of the troubles observed in setting the system up, we think the registration step could be improved. We recommend a better explanation, perhaps through a video, of what the participant should do and how long they should press their finger down. Such instructions could remove some of the ambiguity in the registration process.

Another notable takeaway from our studies was users' perhaps overly optimistic perceptions of the security of biometric authentication. In particular, despite assertions from the smartphone operating systems that users should consider enabling biometric authentication for convenience at the cost of reduced security, participants generally considered biometric authentication to be more secure than PIN codes. Objectively, current implementations of biometric authentication cannot be more secure than a PIN because a PIN can always be used as a fallback mechanism. It is likely that participants considered only the biometric authentication mechanism itself, and not any fallback authentication method, when judging security. However, unless biometric authentication were to become far more robust, a fallback mechanism is necessary.

Furthermore, even though biometric systems can be fooled with molds of fingerprints or photographs of a user [19], few participants in our study were aware of these risks. It is possible that users assume that something high tech is inherently more secure. More conspicuous notice of the security properties of biometric authentication might disabuse users of their misperceptions of security. Progress could also be made in the opposite direction. Negative perceptions of the security of biometric data itself impacted a handful of participants' impressions of iPhone fingerprint unlock. In particular, worries that biometric data would be sent to the cloud, rather than constrained to the device itself, was a barrier to adoption for some participants. While we did not observe evidence among our participants of privacy concerns about face-recognition data, one could imagine similar misgivings for face unlock.

The current availability of biometric authentication on smartphones may signal that the day in which biometric authentication is widely adopted is near. However, without further attention to usability quirks and user perceptions of these systems, barriers to adoption remain.

VI. Acknowledgments

This research was supported in part by NSF grant DGE-0903659, by a gift from Microsoft Research, and with Government support under and awarded by DoD, Air Force Office of Scientific Research, National Defense Science and Engineering Graduate (NDSEG) Fellowship, 32 CFR 168a.

References

[1] V. Matyáš and Z. Říha, "Biometric authentication — security and usability," *Advanced Communications and Multimedia Security*, vol. 100, pp. 227–239, 2002.

[2] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes," in *Proc. IEEE S&P*, 2012.

[3] Google, "Introducing android 4.0," http://www.android.com/about/ice-cream-sandwich/, accessed October 2014.

[4] Apple, "Using Touch ID on the iPhone," http://support.apple.com/kb/ht5883, accessed November 2014.

[5] M. F. Theofanos, R. J. Micheals, and B. C. Stanton, "Biometrics systems include users," *IEEE Systems Journal*, vol. 3, no. 4, 2009.

[6] M. A. Sasse, "Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems," *IEEE Security and Privacy*, vol. 5, no. 3, pp. 78–81, May 2007.

[7] S. Furnell and N. Clarke, "Biometrics: no silver bullets," *Computer Fraud & Security*, August 2005.

[8] E. P. Kukula, M. J. Sutton, and S. J. Elliott, "The human-biometric-sensor interaction evaluation method: Biometric performance and usability measurements," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 784–791, 2010.

[9] A. S. Patrick, "Usability and acceptability of biometric security systems," in *NATO Workshop on Enhancing Information Systems Security Through Biometrics*, 2004.

[10] L. Coventry, A. De Angeli, and G. Johnson, "Usability and biometric verification at the ATM interface," in *Proc. CHI*, 2003.

[11] G. Kwang, R. H. C. Yap, T. Sim, and R. Ramnath, "An usability study of continuous biometrics authentication," in *Proc. ICB*, 2009.

[12] D. T. Toledano, R. Fernández Pozo, Álvaro Hernández Trapote, and L. Hernández Gómez, "Usability evaluation of multi-modal biometric verification systems," *Interacting with Computers*, vol. 18, no. 5, pp. 1101–1122, 2006.

[13] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David, "Biometric authentication on a mobile device: A study of user effort, error and task disruption," in *Proc. ACSAC*, 2012.

[14] C. Braz and J.-M. Robert, "Security and usability: The case of the user authentication methods," in *Proc. IHM*, 2006.

[15] G. Lassmann, "Some results on robustness, security and usability of biometric systems," in *Proc. ICME*, 2002.

[16] M. Theofanos, B. Stanton, R. Micheals, and S. Orandi, "Biometric systematic uncertainty and the user," in *Proc. BTAS*, 2007.

[17] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, 2004.

[18] A. P. Pons and P. Polak, "Understanding user perspectives on biometric technology," *CACM*, vol. 51, no. 9, September 2008.

[19] S. Furnell and K. Evangelatos, "Public awareness and perceptions of biometrics," *Computer Fraud & Security*, January 2007.

[20] H. Sieger, N. Kirschnick, and S. Moller, "Poster: Towards a user behavior model in computer security," in *Proc. SOUPS*, 2010.

[21] R. Tassabehji and M. Kamala, "Improving e-banking security with biometrics: Modelling user attitudes and acceptance," in *Proc. NTMS*, 2009.

[22] R. R. Heckle, A. S. Patrick, and A. Ozok, "Perception and acceptance of fingerprint biometric technology," in *Proc. SOUPS*, 2007.

[23] C. Maple and P. Norrington, "The usability and practicality of biometric authentication in the workplace," in *Proc. ARES*, 2006.

[24] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in *Proc. SOUPS*, 2014.

[25] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are you ready to lock? Understanding user motivations for smartphone locking behaviors," in *Proc. CCS*, 2014.

[26] C. Gunther, "How to use the Galaxy S5 fingerprint scanner," http://www.gottabemobile.com/2014/07/14/how-to-use-the-galaxy-s5-fingerprint-scanner/, July 2014.

[27] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q.*, vol. 13, no. 3, pp. 319–340, Sep. 1989. [Online]. Available: http://dx.doi.org/10.2307/249008

[28] J. Bonneau, S. Preibusch, and R. Anderson, "A birthday present every eleven wallets? The security of customer-chosen banking PINs," in *Proc. FC*, 2012.