A Study of Authentication in Daily Life

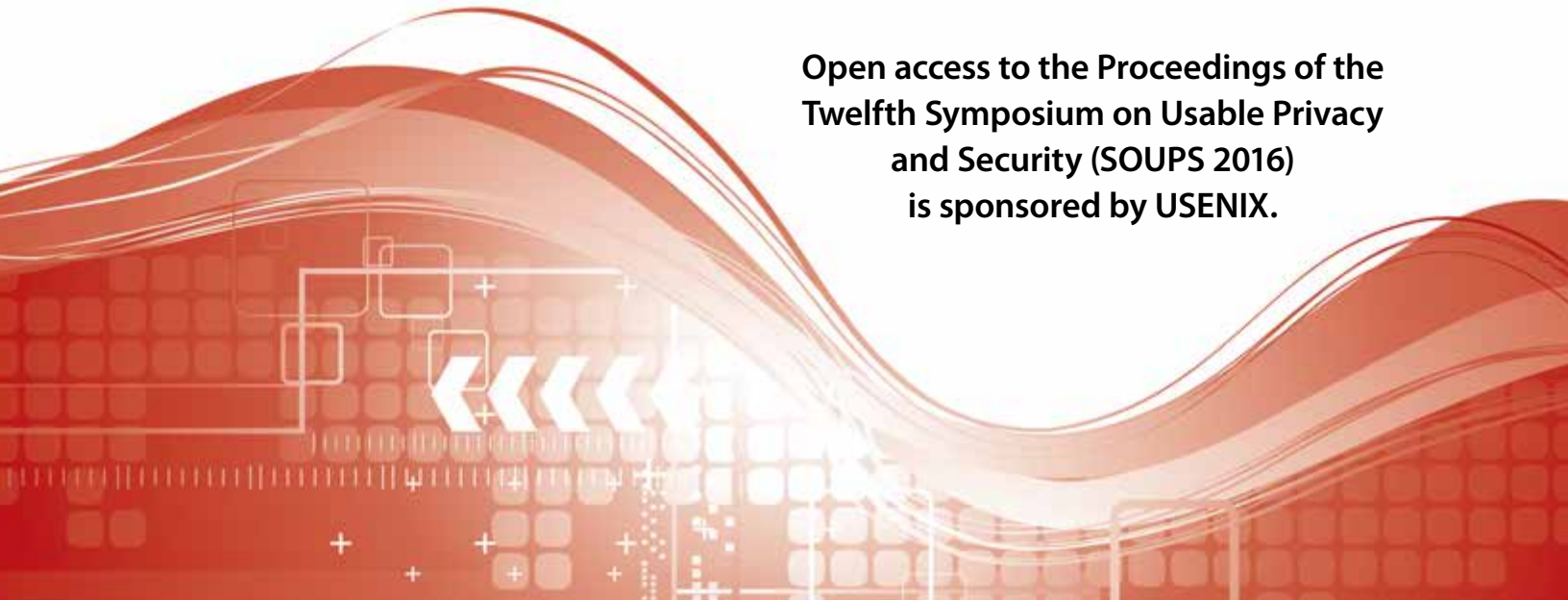
Shrirang Mare, ***Dartmouth College;*** **Mary Baker,** ***HP Labs;***
Jeremy Gummeson, ***Disney Research***

https://www.usenix.org/conference/soups2016/technical-sessions/presentation/mare

This paper is included in the Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).

June 22–24, 2016 • Denver, CO, USA

ISBN 978-1-931971-31-7



Open access to the Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) is sponsored by USENIX.

A Study of Authentication in Daily Life

Shrirang Mare
Dartmouth College

Mary Baker
HP Labs, Palo Alto

Jeremy Gummeson
Disney Research, Pittsburgh

ABSTRACT

We report on a wearable digital diary study of 26 participants that explores people's daily authentication behavior across a wide range of targets (phones, PCs, websites, doors, cars, etc.) using a wide range of authenticators (passwords, PINs, physical keys, ID badges, fingerprints, etc.). Our goal is to gain an understanding of how much of a burden different kinds of authentication place on people, so that we can evaluate what kinds of improvements would most benefit them. We found that on average 25% of our participants' authentications employed physical tokens such as car keys, which suggests that token-based authentication, in addition to password authentication, is a worthy area for improvement. We also found that our participants' authentication behavior and opinions about authentication varied greatly, so any particular solution might not please everyone. We observed a surprisingly high (3–12%) false reject rate across many types of authentication. We present the design and implementation of the study itself, since wearable digital diary studies may prove useful for others exploring similar topics of human behavior. Finally, we provide an example use of participants' logs of authentication events as simulation workloads for investigating the possible energy consumption of a "universal authentication" device.

1. INTRODUCTION

Car key, house key, corporate badge, bike key, RSA token, bus pass, credit card, driver's license, ATM card, ... Many of us carry several of these with us every day to access the doors, computers, and services we need (see Figure 1). We also use passwords, PINs, and fingerprints for devices, websites, and applications. These are all *authenticators* – ways to provide evidence that we are the right people to unlock the restricted resources in our lives. We expect people, especially those working in corporate environments, to carry these authentication tokens and remember complex passwords. This burden leads to *frustration* (when we forget our badges, keys, and passwords), *security breaches* (when we tailgate other people through secure doorways, write down our passwords, or leave our devices unlocked), and *IT expense* (when we call help desks to reset passwords or issue new authentication tokens). Password resets make up 10% to 30% of IT helpdesk calls and can cost from $50 to $150 each to resolve [34]. Even physical keys present an increasing risk, as new smartphone apps enable scanning an unattended key in a few seconds and then printing copies of it by mail order or at kiosks [11].

Figure 1: A subset of the authentication material carried by one participant, who also has to manage over 250 passwords.

Evidence and rationale suggests that password authentication can indeed be burdensome for users [5, 15], and experts provide several approaches for addressing this problem, such as using password managers [17], but how about other forms of authentication? If we aim to reduce the authentication burden for users, is it only worth considering passwords, or are physical authenticators like keys also worthy? Answers to additional questions will further help us tackle this area: How much authentication of different kinds do users actually do, and does it correspond to their own concept of the burden they face? How failure-prone are the different kinds of authentication? Do people generally agree about what kinds of authentication they like and dislike, or will it be hard to help the bulk of people in the same way?

To address these questions and gather a better understanding of the user authentication burden, we conducted a wearable digital diary user study of twenty-six people, including teenagers and adults, students, corporate employees, and others. We provided participants with a commercially avail-

This work was performed while all three authors were at HP Labs.

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado.

able wrist wearable, the MOTOACTV [24] running our own logging application, and asked participants to log all their authentication events for a week. We used the wrist wearable because there are typically so many required authentication events during a day that we wanted participants to be able to log events in the moment, rather than try to remember what they did later. We designed a "slot machine" application interface to provide the wearable with an immediately available and streamlined logging process to help reduce the amount of under-reporting to which diary studies (including ours) are susceptible [18]. We also applied this logging approach because we are interested in authentication with physical infrastructure and not just online authentication, and we could not simply instrument all of the participants' targeted resources to log authentication events automatically. The product of the study includes 4,623 hours of logged events, interviews of each participant before and after the week of logging, and comments participants entered through daily surveys on their smart phones. Our results thus include quantitative information in the form of "traces" of user authentication behavior as well as qualitative information in the form of participants' opinions. Twenty-six participants is not a large enough population to make broad claims about the general population or any particular demographic, but it allows for close observation of a diversity of authentication behavior and opinions.

Our contributions are threefold. First, we hope the design of the wearable digital diary may be interesting to others performing similar studies, even though we believe this particular study suffers from several flaws such as the small sample size of participants. Second, our results incorporate information that might help others working to reduce people's authentication overheads. We find, for instance, that authentication using physical tokens is a sufficient burden to warrant addressing. On average, 25% of a participant's authentications employ physical authenticators – tokens such as car keys that users need to carry with them – and participants offered negative opinions about physical authenticators, not just passwords. We also find that people's authentication behavior and their opinions about authentication vary greatly, so it may be hard to please everyone in the same way. For instance, some people's favorite authenticators are others' least favorite, although several participants favor quick, effortless authentication methods even if they come with significant error (false reject) rates. We see surprisingly high failure rates across many types of authentication: 5% for passwords (with an even higher rate for PCs and websites), 3% for physical keys, and 3% for fingerprints. Our third contribution consists of the authentication event logs themselves, which we will make publicly available. We provide an example of how we use the logs as workloads for simulating energy consumption of a "universal authenticator" – a device that performs many varieties of authentication on behalf of its user.

2. RELATED WORK

There is a tremendous amount of existing and ongoing work related to ours, especially in the areas of authentication, user studies, and wearables. We confine our descriptions of related work to examples of user authentication behavioral studies that we perceive to be the most relevant to ours. We note that even definitions of authentication devices differ across these studies, with some including the presentation of "things you have" such as keyfobs, and others only including tokens that display or contain information specific to a single individual, such as a badge with the owner's photograph [29].

Several studies focus on smartphones and how people choose to secure them or not, and their results vary considerably. Based on 2,000 Android users' smartphone usage Hintze et al. report that on average people unlock their phones 25 times per day [16], whereas Harbach et al. find an average of 47 unlocks per day in their 52-participant study [13]. In our study we observed unlock usage of about 33 times per day. A 2013 study by Lookout [19] of 1,003 Americans (age 18 and older) found that 56% of users surveyed did not choose to enable a security lock for their phones, and that "people care [about privacy] but exhibit risky behavior." Other studies see fewer people choosing not to lock their phones [20]. Egelman et al. report that 8 of their 28 interviewed participants (29%) and 42% of their 2,418-person online questionnaire respondents did not lock their phones [9]. Bruggen et al. observed that 35% of phones out of the 149 running their software agent did not employ any locking mechanism [32]. In our study, 4 of 26 participants (15%) did not lock their phones, and we too observed risky authentication behavior in terms of password management and sharing.

Various other non-smartphone studies and essays explore passwords and how users manage, choose, and forget them [5, 10]. A study of the password habits of half a million users over a 3-month period used a component in Windows Live Toolbar on users' machines to record password strength, usage, and frequency metrics [10]. The study found users choose weak passwords and use them across multiple sites and that 4.28% of Yahoo users forgot them during the study. We see an even higher percentage of users who forget, struggle to remember, or reset a password at least once during our study (36%). Hayashi and Hong conducted a diary study with twenty-one participants, in which participants carried diaries and recorded information about password-based authentications, but the focus of the study was authentications only on laptops and desktops [14]. A *New York Times* study explores the meaningful personal information users embed in their choice of passwords [31]. All of these studies agree with ours in concluding that users find it hard and frustrating to manage passwords according to established rules of safety. Usable security that takes into account human limitations and strengths has become increasingly important [6].

A recent study of online safety covers opinions and practices of both experts and non-experts regarding how to stay safe online [17]. It is interesting to note that the reported expert security advice on password management differs somewhat from the requirements promoted by some of the participants' companies' IT departments. In particular, at least one IT department asks employees not to trust their passwords to third-party password managers, and yet it does not provide any in-house password manager. Experts promote the use of password managers, while non-experts surveyed by the study shared the IT department's distrust of password managers.

At least two studies include consideration of authentication other than with phones and passwords. A National Institute of Standards and Technology (NIST) study involved 23 NIST employees (ages 20 and above) carrying a written diary in which they recorded a wealth of information about their authentication events for a 24-hour period [29]. This study

covers not just smartphones, passwords, or online authentication behavior but also a few other types of devices such as badges. Their participants recorded an average of 23 events a day, which is significantly lower than the 45 average of our participants. This may be because of differences in the study sample (a majority of their participants were in their fifties, whereas the median age of our participants is 29 years) or differences in the event logging mechanism (a paper diary vs. a digital wearable diary). Some other results from their study correlate well with ours, such as finding no strong relationship between participants' amount of authentication and the frustration they express. Another study that considers physical authentication was performed by Bauer et al. in 2007, in which they instrumented doors at participants' workplace(s) for authentication using smartphones, and developed (and evaluated) access-control policies for unlocking those doors [4]. We are interested in all physical authentications in participants' daily lives, which ruled out instrumenting things for automatic authentication logging, leading us to use a self-reporting approach with a wearable digital diary.

We believe our study is unique in two ways. First, we enable the diary study with a wearable application to allow easier and more streamlined in-the-moment logging of authentication events. Our motivation is to reduce under-reporting and provide more accurate timing information for authentication events. Second, our study covers a wider range of authentication types, including authentication with locked cars, doors, bicycles, public transportation, and so forth. While there are studies that report on authentication with a few types of physical targets, we are unaware of a study that covers the breadth of physical authentication targets accessed by the participants in our study.

3. METHODOLOGY

In this section we define an authentication event and describe the wearable digital diary method for self logging and our study procedure.

3.1 Authentication event

We define an authentication event as one where an individual must demonstrate, actively, that he is the right person to gain access to a resource or service through something he *is* (or *does*), something he *knows*, or something he *has*. Examples include unlocking a phone, unlocking a house door, logging in to a password-protected website, or entering a PIN on an ATM machine. Accessing a website with cached credentials that does not even require a mouse click to choose among credentials involves no active user effort, so it does not count as an authentication event for our purposes, since we want to explore in-the-moment user authentication effort. Note that we also do not include lock or re-lock events. We define an *authentication target* as the device, resource, or service to which the individual requests access, and an *authenticator* as the evidence the individual provides to gain access. For example, when unlocking a phone with a PIN, the phone is the authentication target and the PIN is the authenticator; when opening a door with a badge, the door is the authentication target and the badge is the authenticator. Below is the list of targets and authenticators we use in the study. Note that some of the items represent a category. For instance, "Laptop" also covers desktop computers, while "Password" also covers passcodes, PINs, locker combinations or any knowledge-based authenticator.

Figure 2: Diary entry app on the smartwatch.

Authentication Targets: Laptop (also desktops), Phone, Tablet (also e-readers), Website (also online websites or any software), Door, Car, ATM, Public Transport, Bicycle (also motorcycle), Phone payment, Card payment, Bank check, Locker (also locked drawers), and Other.

Authenticators: Password (also PINs, locker combinations, etc.), Fingerprint, Face biometrics, Voice biometrics, Card (ID cards, credit cards, badges), Certificate (PKI), Mouse click (where the participant has to click to authenticate, e.g., to request autofill with a password manager), Lock key (physical key), Keyfob (remote key), Signature, 2-Factor, and Other.

We are also interested in whether an authentication succeeds and the location where it occurs. We asked our participants to log whether the authentication event was successful and the number of required attempts before it was successful. We wanted to collect semantic locations for authentication events, including Home, Work (includes School for student participants), Shop, Traveling, and Other. Thus, in our study an authentication event is represented as {*event-time, authentication-target, authenticator, success, location-label*}.

3.2 Wearable digital diary

To reduce the amount of under-reporting and poor recall that can affect diary studies [18], we wanted to enable immediate, easy logging of events. This is especially important for events such as authentication that can occur frequently and at times when it is inconvenient to pull out a paper diary and pen or even pull out a smartphone to bring up an app. We considered using a wearable voice recording device, but pilot study participants said they would not be happy talking to themselves when unlocking stuff. We chose a smartwatch (the commercially available Motorola MOTOACTV [24] Android smartwatch) as our primary logging device, as it is easily accessible and we could take over the display with our logging app for immediate entry; Figure 2 shows the logging interface available as a user raises his wrist. Indeed, most of our participants found logging events via the watch convenient compared to a smartphone; we further describe this in Section 3.3.1. Besides the logging app on the smartwatch, we also developed a companion smartphone app, where participants could view, edit, label, and comment upon their logged events using the bigger display.

3.2.1 Watch app

The MOTOACTV is not programmable out of the box. To use it as a digital diary we rooted the watch and installed our Android application, which always runs in the foreground so

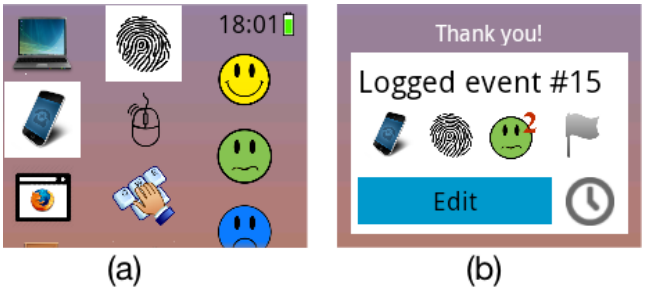


Figure 3: Watch App UI. a) Main watch app screen showing logging in progress for a phone event using a fingerprint unlock. b) Watch app screen confirming the logged event; the green icon with number two indicates that two retries were required to unlock the phone.

that it is immediately accessible to participants when they raise their wrists, which turns on the display (Figure 2). For an authentication event, we want to collect the authentication target, the authenticator, success or failure, number of attempts required (in case of a success), location, and time. The app automatically collects GPS location and time, but the participants have to log the other four details. Logging an event should be quick and easy so that it is less interruptive to the participants' current tasks, otherwise they are likely to delay logging and may later forget to do so. After several iterations and feedback from pilot study participants we came up with a novel "slot machine" like interface to log an authentication event with usually only two taps on the watch touchscreen. Figure 3 shows the logging interface. Participants generally liked the watch app interface: eight participants mentioned unprompted during their post-logging interviews that it was easy for them to log events through the watch. Participant P5 added that *"anything more than 2–3 taps is effort for me"*. Some participants did not like the watch's form factor: six participants wished the MOTOACTV watch had been smaller or more comfortable, and one participant chose not to wear or carry the watch and entered all his events from his phone.

Figure 3a shows the app logging screen. It presents three vertically scrollable columns of icons: the first column for authentication targets, the second for authenticators, and the third for success/failure. In Figure 3a the participant has selected phone (target) and fingerprint (authenticator). The success/failure column has three icons: (from top to bottom) a yellow happy face (for immediately successful authentication), a green unhappy face (for successful authentication that required more than one attempt), and a blue sad face (for a failed authentication or extremely problematic event). Examples of failed events include forgetting one's password or dropping one's car keys in the mud under the car. Tapping a face icon enters (logs) the event, except for the unhappy face (middle icon), which brings forth another column on the right side of the display. This fourth column contains a list of numbers (2, 3, 4, and 5+) indicating attempts performed for the successful authentication. The order of icons in each column is user-configurable for convenience, so participants can keep their most-often used targets and authenticators at the top for quick access. The app also caches the last chosen authenticator for each target and automatically selects it when the participant chooses a target, to reduce necessary taps in the common case. For example, choosing phone would automatically select fingerprint if the participant's last logged phone unlock event was with a fingerprint. Tapping the happy face would then log the event. With caching and configurable icon order, participants can log events with only two taps for their common cases.

The act of choosing a face icon enters the event and brings up a confirmation screen. Figure 3b shows a confirmation screen for a phone unlock event with a fingerprint in two attempts. The confirmation screen shows the authentication event logged and allows editing the event. It also allows flagging the event (flag icon) or adjusting the time of the event (clock icon) in case the event was performed in the past (e.g., 10 min ago). We asked participants to flag an event when there was something unusual about it or if they wanted to comment on it, which they could do on their smartphones when reviewing their event logs. We inquired about flagged events and any other odd events during the post-logging interviews. The confirmation screen persists long enough to allow users to edit the event if they wish and then returns to the logging interface.

3.2.2 *Smartphone app*

The watch allows participants to log an authentication event quickly without needing to reach for their phones, but its small screen size is not suitable for complex interactions such as viewing event logs or editing events in the log, so we provided participants with a companion smartphone app. The smartphone app periodically syncs with the watch and administers the daily survey at the participant's chosen time, usually in the evenings. The app also periodically syncs with the cloud, allowing us to monitor the study. The smartphone app provides a dashboard interface for participants where they can also manually sync the phone with their MOTOACTV watch, sync the app with the cloud, browse and edit their authentication logs, and take the daily survey.

Figure 4a shows an example of the event log UI, reachable from the dashboard or the daily survey. Each row represents an authentication event, with the time of the event displayed on the left, followed by the authentication target icon, the authenticator icon, an authentication success/fail icon, a comment icon (orange if the participant entered any comment for the event), a flag icon, and a location label. Tapping on any of these icons allows the participant to edit the field. An unassigned location label appears as "NA" and participants can tap on it to assign a label from a pop-down menu of five location labels (Home, Work, Shop, Travel, and Other). When a participant labels an event, the app automatically labels other events logged at the same location. Participant labeled events are orange; in the figure the top and bottom location labels were assigned by the participant and the other labels were assigned by the app. Although we chose the MOTOACTV watch in part due to its built-in GPS sensor, the GPS on the watch could not always provide a location, so the smartphone app collects GPS information every five minutes, and we also use this information to assign semantic location labels to events. When participants finished the study, we deleted the GPS information to keep only the semantic labels, as they are far less privacy-sensitive.

Figure 4b shows the survey we administer daily to the participants. In the survey we ask participants to go over the

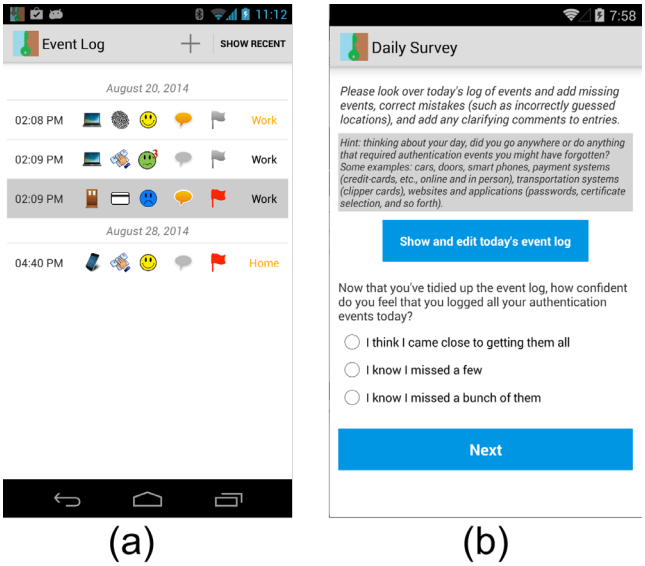


Figure 4: Phone App UI a) event log, b) end-of-day survey.

day's authentication event logs, add missing events, make any edits if necessary, add comments to events, and add location labels to the authentication events. To make it easier for participants to review their logs, the app only displays events that the participant logged since the last time they took the survey. Participants can see the complete log by choosing the 'show all events' option. In the survey we also ask them to rate how good they thought they were about logging all the events. On the Next screen in the survey we ask them to provide any comments they had, about the study or about their day, especially if they felt there was something unusual about the day.

3.3 Methodology successes and failures

Other researchers might be interested in deploying a wearable digital diary study for their own purposes, so we describe here the high-level successes and failures of our study methodology. We list other limitations of the implementation of our study in Section 5.

3.3.1 *Logging on the wrist versus the phone*

One of the reasons we created the phone app as well as the wearable app is that we worried many participants might prefer to log entries from their phones. After all, many people have their phones handy most of the time. We gave participants the choice of logging either from phone or watch. However, the immediate accessibility of the wrist wearable combined with our slot-machine style logging interface worked as intended. Except for three people, participants logged an average of 93% of their events on their watches. One participant (P25) did not like wearing a watch so he logged all events from his phone, and two other participants (P15 and P16) did not wear the watch because they thought it was not fashionable. Instead, they carried it clipped to their bags and logged about 40% of their events on the watch. Overall, the approach made logging easy enough that 84% of events in our study were logged from the wrist wearable despite the availability of the phone application. We suspect that this approach could lead to future wearable digital diary studies. The smartwatch was generally the preferred platform for logging in-the-moment events compared to the smartphone among our participants, and despite the clunkiness of the particular watch we used, one participant became a convert to watch use in general: *"I didn't used to wear a watch. I didn't think I liked them. But after this study I got used to just looking at my wrist and knowing what time it is. Now I want a watch." (P10)*

3.3.2 *Validity of self-reported phone events*

We captured phone unlock events in two ways: our phone app automatically logged phone unlock events (except for the five iOS users and a user whose phone was unable to do so), and a set of participants logged phone unlocks manually (including all the iOS users and a subset of the other users). Using the eight-person intersection of these groups, we compared their number of automatically and manually logged phone unlock events to get an estimate of under-reporting for phone unlock events. Under-reporting phone unlocks ranged from 7.8% to as high as 60.1% for one participant. We believe that participant decided not to worry about logging phone events, but since she did not explicitly inform us of this decision we count her data. On average we see 20.9% under-reporting, although one user over-reported by 31.9%. When queried, the over-reporter said that he was worried that phone unlocking was so automatic that he might not have recorded it so he would record it again just in case.

Automatic logging would be much better for accurately recording activities that involve many events, but where that is not possible, such as our case in which we cannot instrument all possible authentication targets, it is clear we must streamline the logging process however possible. Attempting to recall and record all authentication events after the fact seems close to hopeless. Some participants expressed a difference of feeling about logging phone events as compared to other events, saying that they were harder to recognize in the moment compared to other types of authentication and that they therefore had more trouble remembering to log them. Some participants either declined to log them or gave up logging them. These included our biggest users of phone unlocking, according to the automatically logged events. If compliance is inversely proportional to number of events, our participants' self-logging of event types other than phone unlocks may suffer from less under-reporting, but we have no good way to determine this. In addition, this makes comparisons between phone unlock and other authentication events less reliable.

3.4 Study procedure

We performed a 3-person 2-day pilot study to test the digital diary for logging, for our categorization of the authentication targets and authenticators, and to find bugs and refine our UI and procedure. We then executed the main study which we describe below.

3.4.1 *Recruitment and enrollment*

We recruited participants by word-of-mouth because our company's legal department required us to verify that participants be either affiliated with our company or US citizens at least indirectly known to members of our organization. These conditions also soothed management concerns that we be able to retrieve the smartwatches from participants after the study. We additionally screened participants to verify that they were comfortable using a smartphone. We provided

informed consent and information sheets to screened participants. If participants agreed with the documents, we invited them to come in person to our lab (or meet via Skype for remote participants) where they signed the consent form and we interviewed them and explained the study procedure. We required and received parental consent for participants under the age of 18. Enrollments occurred throughout the week, and participants were asked to perform the study for seven days from the enrollment day. We explained both in writing and in person what information we would collect. We also warned participants both in writing and in person to practice safe logging: "Please only log events on the watch and phone when it is safe to do so. Please do not use the devices while driving, biking, crossing streets, operating heavy machinery, or anything else that would be risky!" We also informed them that they could withdraw from the study at any time for any or no reason. One person did so, leaving 26 participants.

We gave each participant a MOTOACTV smartwatch with our app pre-installed and asked them to wear it on their wrist at all times (except when charging or in the shower or pool; the watch is not waterproof), but if they were uncomfortable wearing it on their wrists, they were allowed to attach it elsewhere via a provided clip. We installed the companion smartphone app on participants' Android smartphones. If a participant did not have an Android smartphone, we lent one for survey taking and syncing and editing event logs. Our study was approved by the ethics committee equivalent in our company. Study participants received $100 gift cards upon completion of the study.

3.4.2 Pre-logging interview

We conducted an in-person semi-structured interview with each participant to learn about their own pre-study perspectives on their daily authentication lives, the devices and resources they use, the authenticators they carry with them, and how they feel about various aspects of authentication. We asked participants to tell us about the authentication events they perform in a typical day by thinking through their daily routines and recalling their authentications. We also asked them to guess how often they might authenticate with various resources so that we could compare this information later with their reported data. We used a set of questions to guide these semi-structured interviews, but we allowed the participants to digress and describe their opinions and behaviors regarding authentication. See Appendix B for the list of interview questions. We answered any questions they had about how to enter various kinds of events.

3.4.3 Post-logging interview

We conducted another semi-structured interview with each participant after one week of self-logging. We asked them about flagged events, any logged entries that we did not understand, and about authentication failures they logged. We also asked about their thoughts on authentication, the watch UI, future inventions they would like to see in the area of authentication, their choice of best and worst authenticators, and about how their authentication behavior might have changed during (or as a result of) the study. See Appendix C for the list of questions.

4. USER STUDY PARTICIPANTS

The study includes 26 participants who logged their authentication events for one week each over the course of three months. Due to the conditions placed on our recruiting of subjects, our participants essentially form a "convenience sample" that is not as balanced across gender and other characteristics as we would have liked. We were able to aim for inclusion rather than balance. Participants' ages range from 13 to 64, with 7 participants each in age ranges 10 to 19 years and 20 to 29 years range, 8 participants in age range 30 to 49 years, and the remaining 4 participants in age range 50 to 64 years. The participants include 8 females and 18 males. Sixteen are from computer-related fields, 2 are from non-technical fields, one is from a medical-related field, and 7 are in grade-school. There are 10 students (3 are graduate students), and the rest are full-time employees. Our participants represent 7 different schools, 4 different companies, and 3 different regions of the US. Participants self-reported their ethnicities as 14 Caucasian, 2 African American, 7 East Indian, and 3 Asian.

5. LIMITATIONS

The goal of our study is to gain an understanding of authentication in participants' daily lives through self-reported quantitative data and qualitative interview data. Due to the nature of the data we obtained, the results should be interpreted carefully. We should avoid generalizing numerical results to a broader population, due to both the small number of participants and under-reporting of self-logged events. Instead, we can use the results to learn about authentication habits and the reasons behind them. With that in mind, we list the limitations of our study.

L1 *Small sample size.* Regardless of participant diversity, our convenience sample of twenty-six people is not a large enough group to give good statistics about the overall population or any particular demographic. We caution readers against generalizing the results.

L2 *Under-reporting.* We minimize the effort for reporting an event in our study, but it is not a zero-effort task, and participants failed to report some events, except for one participant who over-reported phone unlock events. Thus the number of self-reported authentication events in our study is generally a lower-bound of the actual number of authentication events performed by the participants. Moreover, whether a participant self-reports an event might be affected by context (e.g., current activity, location).

L3 *Self-logged vs. auto-logged data.* We asked some participants to report all authentication events, including phone unlock events, but our smartphone app also automatically logged phone authentication events. In our analysis (Section 6) the phone authentication events are from the automatically logged data for Android users (except one) and self-logged data for iOS users. The other (non-phone) authentication events are from participants' self-logged data. This exaggerates any differences between phone and other authentication events, which we should keep in mind when analyzing the results.

L4 *A snapshot of a week.* The data we obtained is a snapshot of authentications that participants encountered and reported during one week, which is not necessarily representative of their typical weeks. For instance,

there are most likely cases where a participant did not perform a type of authentication (e.g., using an ATM) during our study week that he might have performed during another week.

L5 *Participants with only daytime jobs.* None of our participants are night workers – they are all students or employees with daytime jobs – so we see only a few events at night.

L6 *Mostly Android participants.* Only five of our participants are iOS phone users with the rest being Android users. With more iOS users, for instance, we might see more fingerprint authentication, as fingerprint readers are less common on Android phones.

L7 *Missing location information.* GPS readings are not always reliable depending on location (for instance, indoors) and some participants' phones had more trouble getting frequent GPS readings than others'. As a result, about 25% of locations in the study have no semantic labels attached.

L8 *Extra phone unlock events.* There may be extra phone unlock events caused by the study, because participants might unlock their phones to take the daily survey or to log an event on the phone app. When queried, participants said they did not access their phones just for the survey or to log an event, but we have no way to verify this claim.

L9 *Change in participants' authentication behavior.* Participants may have changed their authentication behavior as a result of their participation in the study. One of our post-logging interview questions targets this concern. Three participants said they typed passwords more slowly to avoid errors, and one said he used his phone less often on some days, because he was embarrassed by how frequently he used it. Otherwise, all participants said they did not notice any change in their authentication behavior, but we have no way to verify their claims.

6. FINDINGS

In this section we present our findings from both logged events and participant interviews. We look at authentication patterns, the nature of the authentication burden on participants, and the rates of authentication errors participants experience. We see evidence that physical authenticators are part of the authentication problem for many people, and not just passwords. We find that people's authentication behavior and opinions vary greatly, and that many types of authentication suffer from high false reject rates. We report supplemental material about participants' estimates of how much authentication they do, their feelings about privacy, and further results about their authentication patterns in the Appendix.

Together, participants logged 7,225 authentication events: they manually logged 3,488 authentication events, and our phone app automatically logged 3,737 phone unlock authentication events. The log for one of our participants did not cover quite the full week; for calculations where this could affect results we use only data from 25 participants. We conducted semi-structured interviews with all participants before and after the data logging phase of the study. We took detailed notes from the interviews. Our notes include direct quotes from participants, summaries and paraphrases of participants' explanations, and descriptions about their authentication behavior and opinions. We identified themes and categories in our notes (coded) and formed a data matrix, with columns as themes and rows as participants [23]. As we describe our findings we include occasional quotations from participant interviews (with more in Appendix F) chosen because we found them especially interesting, representative of a particular point, or simply entertaining.

Table 1: Authentication targets and authenticators used in the study and the number of participants (N) who used them.

Targets	N	Authenticators	N
Laptop	26	Password	26
Website	26	Card	25
Door	24	Lock key	25
Phone	22	Keyfob	18
Car	20	Mouse click	15
Card Payment	20	Signature	13
Other	11	Fingerprint	6
Tablet	10	Other	8
Locker	9	Certificate	4
Bicycle	7	2-Factor	3
ATM	5		
Check	5		
Public Transport	3		
ID Verification	3		
Phone Payment	2		

6.1 Authentication patterns

We captured the different types of authentications that our participants performed, how often and where they authenticate, and various other characteristics. Table 1 presents a list of authentication targets and authenticators logged in the study and the number of participants who used them. Some targets and authenticators were very popular, but authentication behavior varied even at this high level. For instance, two participants, both teenagers, did not need to unlock doors during the study.

6.1.1 Distribution of events by authenticator

Overall we find that 74.4% of authentication events involve "things you know" (secrets such as passwords, PINs, swipe gestures, and locker combinations), 18.4% involve "things you have" (physical token-based authenticators such as badges, keys, cards, keyfobs, and 2-factor tokens), and 7.2% use other means, including biometrics and signatures, or "things you are or do."

Figure 5 shows the distribution of authentication events logged by each participant by category of authentication, secrets, physical tokens, and "Other." On average, 25% of a participant's authentications used a physical token for an authenticator. If we exclude the four participants who did not lock their phones, this number falls to 21%. Authenticating with keys and other physical tokens constitutes a significant part of most participants' authentication workload. There is high variance, though, as some participants performed almost no authentication with physical tokens.

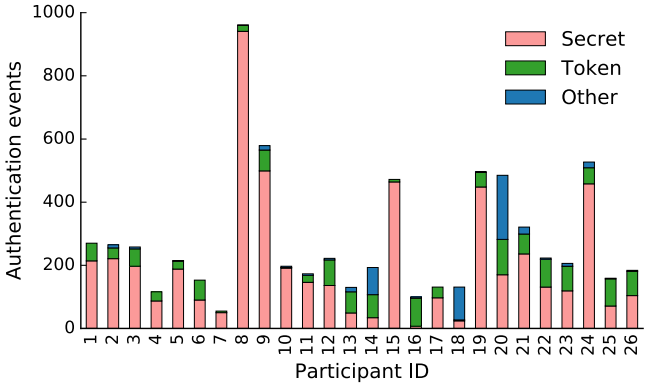


Figure 5: Authentication events for each participant, categorized by type of authenticator.

This is largely true for the teenage participants (P7, P8, P10, P15, and P19). The teenager P16 performed mostly token-based authentication, because he drives a car but does not lock his phone.

6.1.2 Distribution of events by target

We were also interested in learning how many authentication events involve digital versus physical targets. *Digital* events are those that require authentication to an electronic service or an electronic personal device, and *physical* events are those that require authentication to a physical resource or thing. Specifically, in our study, digital targets include Phone, Laptop, Website, or Tablet, and we consider all other targets physical. See Section 3.1 for a fuller definition of these targets. We debated using other possible categorizations, such as considering devices like phones and laptops to be physical infrastructure instead of digital targets. We use our current categorization so as not to overemphasize the importance of physical targets.

Among all the logged authentication events, 22.2% were physical authentication events. The average number of physical authentication events logged by each participant is 30.7% with a standard deviation of 20.2%. Again, we see substantial variations across participants, in part because of their widely varying ages. Middle-schoolers, for instance, do not need to unlock cars as often as adults, and most of them do not have credit cards. Alas, most of our adult participants drive cars more often than they bicycle.

6.1.3 Variation in authentication pattern

We also capture when, how often, and where participants authenticate themselves. Overall there is a high variance among participants. Authentication events per day across participants range from 0 to 208 with an average of 45 per day. Even in our day and age it is possible to have a day of zero authentications if you do not lock your phone and stay indoors the whole day. Authentication events per hour across participants in a 24 hr day range from 0 to 107 with an average of 2. Authentication events per hour across participants in a 9am–5pm day range from 0 to 83 with an average of 19.

We were interested in learning whether participants log more events on weekdays than on weekends, and when during the day they typically authenticate. We see no obvious distinction; only five participants (P3, P5, P6, P21, and P24) performed significantly more authentication events during a weekend than on a weekday ($p < 0.05$). We also analyzed the number of authentication events performed by participants at different hours of the day. All our participants have day jobs or generally follow a day-oriented schedule, and so we see more authentications between 9am–6pm, but there were authentications spread throughout the 24 hr day. There seems to be no hour of the day where someone isn't authenticating with something.

Table 2 shows the number of authentication events performed at different locations. We expected to see most events occur at Work (where school counts as work for students), but we were wrong. Home receives the largest number of authentications when averaged across all participants, and if we consider just phone unlock events, we see that participants unlock their phones 59.8% of the time when they are home and about 29.7% when they are at work. However, if we exclude teenagers we see that participants perform more authentication at work than at home (45% vs. 40%). For the overall participant pool there are roughly 10% fewer authentications on average at Work, with Shopping (which includes restaurants), Traveling and Other receiving far fewer events. Traveling includes driving, and unfortunately, we do see participants unlocking their phones while driving, as have others [19].

Table 2: Distribution of authentication events by location, across all participants and across participants excluding teenagers.

	All	Excluding teenagers
Home	43.6 %	40.1 %
Work	38.5 %	45.1 %
Shop	6.6 %	5.8 %
Travel	5.5 %	4.1 %
Other	5.8 %	4.8 %

Variation across age and gender. We see a slightly higher number of authentication events in teenagers and older participants (> 39 years) than those in their twenties and thirties, but we believe there are no general conclusions to draw from this and that it is likely due to individual behavior. We can, however, conclude that no participant escapes authentication.

We also compared authentication behavior between the 8 female and 18 male participants. Per person, both groups logged roughly the same number of authentication events, phone unlock events, and physical events. The average authentication events in a day logged by the female group and the male group were 42 (± 16) and 37 (± 33), respectively. The average number of phone unlock events in a day logged by the female group and the male group were 25 (± 23) and 22 (± 33), respectively. The high standard deviation highlights the wide variation in the study participants' authentication behavior. Overall, at least in our small sample size, we do not observe wildly different authentication behavior across gender.

6.2 Authentication burden

In this section we look further at whether, and in what ways, participants consider authentication a burden. We find that

Table 3: The number of authenticators carried by participants, added across all participants.

Authenticator	N	Comment
Credit card	60	Includes work, 4 not used
Loyalty/gift card	55	One gave no exact number
House/apartment key	27	One person carried 6
Membership card	22	
Car key	19	Regular or electric
Driver's license	18	
Other door key	17	One gave no exact number
Debit card	17	
Other ID card	16	2 expired
ID badge	15	Mostly corporate, also gym
Car fob	13	
Health insurance card	12	One noticed missing card
Transportation	10	Zip card/buses/metro
Car proof of insurance	9	Others kept these in car
Mail box key	7	One P.O. Box
Key of unknown function	7	
Scraps of paper	5	With writing
Bike key	4	Rest used combinations
Phone	4	Phone app for passwords
Motorcycle/scooter keys	4	Includes 2 trunk keys
Digital key	3	
Locker key	2	Rest used combinations
Blank checks	2	
Cabinet/drawer key	1	One attached to ID badge
Motorola skip	1	
Jewelry box key	1	
House alarm fob	1	
Work building fob	1	In lieu of ID badge

participants' opinions vary considerably, and that managing both "things you have" and "things you know" contribute to the burden.

6.2.1 Things people carry

While many problems with passwords are well documented, physical authenticators also offer challenges for users. Some of us have many resources we need to access frequently using physical authenticators, and this means we need to carry many authenticators with us. To find out more about this potential problem, we asked participants if they were willing to dump out the contents of their wallets, pockets, purses, bags, or other places where they carry authentication material. We told them we did not need to see what they dumped out, but that they could just enumerate for us what they found. Table 3 shows the results, added across participants.

There are several indicators that managing these carried authenticators can be troublesome. *"I don't like to carry around physical keys. It's just another thing to manage, and if I were to ever forget it...The Pebble is one exception 'cause it's always on your wrist. If it had a computer unlock I'd be totally happy." (P7)* Several participants attempted to divide up or stage their authentication material so that they did not need to carry all of it. For instance, one participant has bags for different purposes, with the appropriate ID cards or badges in the different bags. Another attaches a work cabinet key to her ID badge, and that key opens drawers with other cabinet keys in them. Another participant uses a phone cover with slots for cards in it. He carries his driver's license, a debit card, and his badge in the cover. The rest of his cards he puts in his wallet, which he keeps in his car and only carries on his person if he needs it in a store. Another participant stages his keys so that he carries a minimum but the keys he does carry allow him access to the rest of the authenticators. *"I'm at the limit of physical keys I can carry – can't tolerate any more. It's a layer system – the rest are kept in a pie tin at home. It's part of the family semaphoring system. Know who is doing what where...I have it set up usually so most things are automated and I don't have to carry as much. Never be without a house key – I teach all my kids that too." (P12)* Another participant rigged up his own "smartwatch" in the form of a Motorola skip clipped to his regular analog watch. He unlocks his phone by tapping it against the skip on his watch. Attaching it to the watch means he does not need to worry about carrying it – it is always with him since he wears his watch every day.

Another indicator of management burden is that people can't track what they carry. They carry authenticators with them that they no longer need or cannot identify. People carried expired school IDs, unused credit cards, and keys whose functions they couldn't remember. For instance, one carried two unidentified keys and said *"But I'm scared to remove them. They seem like they might have been important." (P21)* They also can't find material they were sure they were carrying. *"There should be two health cards – one for kids – but I can't see where that went." (P26)*

Some participants also make arrangements to carry authenticators on behalf of others. One teenager (P7) carries his brother's gym ID card "'cause he doesn't carry a wallet. We go together and my parents are worried he'd lose it." Another carries his own locker key and his friend's. Another carries his friend's house key, and two others carry their parents' house keys too. One participant carries loyalty cards shared with her husband.

A couple of participants volunteered that it's not just the hassle of carrying so much material that is the problem, but it's also their mental anxiety over wondering if they might have forgotten something. These people wanted someone or some tool to help them manage their keys and cards. *"From a technological point of view – [I want] someone [to] tell me your key is this place or your credential info is here...[It would help] best at home – [I] put my keys somewhere – depends on situation – baby crying, sofa, piano, and then I forget [where I put them]. But when I try to use car first have to find key or I can't use my car. So [if I could] have it be 'go to the car and someone gives me this key' that would be great!" (P13) "Did I forget something? Constant confusion if I forget something." (P8)*

Changes to routine also increase the chance that people won't have the authenticators they need with them. One participant mentioned *"Traveling has a problem with acquiring more keys and cards..." (P12)* Emergencies are a further problem: during a recent fire drill at a participant's company where emergency communications required particular tablets, *"The emergency crew didn't remember to bring the tablets with them when exiting the building, or they had them outside in their locked cars but didn't bring out the car keys." (P12)*

Finally, people carry scraps of paper in their wallets and bags with authentication material, sometimes obfuscated and sometimes not. For instance, one participant carries a paper with last year's gym locker combo on it *"'cause I was*

constantly forgetting it and asking the coach to open it for me." (P8) Another participant carries a paper in his wallet that is *"a letter of love to my wife – but it happens to be passwords encoded." (P11)*

6.2.2 Password management

Secrets constitute the largest portion of authenticators for our participants. They were used to unlock laptops, phones, lockers, bicycles, and even house doors. In our dataset, among all phone unlock events, 92% occurred with a PIN, 7.7% with a fingerprint reader, and 0.3% with a swipe gesture. For laptops, most participants used passwords, but in some instances (0.8%) the participant only had to click to login because the laptop was set to auto-login. For Website, which includes online services and access to software on phones or laptops, participants used passwords for 75.7% events and they used Mouse click (auto-filling the password with a password manager or cached passwords) for only 21.3% events. This surprised us, because we expected participants to use password managers or cache their passwords in the browser more often.

Many people feel that the rules around choosing and managing passwords have become onerous, especially in corporate environments. Across all our study participants, including those employed by our company, we found *no one* who followed all our company's workplace rules for passwords: change them frequently, don't reuse them, choose passwords of significant complexity, do not use the same password across multiple sites or accounts, do not write them down, do not cache them in browsers, and do not use a third-party cloud-based password manager to store them. *"It's awful. I'm dying...Everybody's got different rules and people are requiring I change them and then I can't remember them. Then life is hell...I use the same one [password] – I'm not a fool...All the tools to do my job are impossible to get to...This requirement that I change the password – They're causing us not to be able to remember the password, not to pick a good one, to use the same one and just change the postfix, or to write it down. They're forcing me into this corner – I don't know what to do. Maybe I'll write it on a sticky note and paste it on my computer." (P17)* Everyone "cheated" in at least some regard – and they were aware of it. Immediately after they told us about a bad practice, they confessed that it was bad or justified their action. *"About the management aspect – remembering a password – I reuse passwords is how I get around it, which is bad." (P2)* This may indicate that password management has become difficult enough that even otherwise conscientious tech-savvy employees are not willing to abide by the requirements.

To manage their many passwords, participants turned to a variety of tricks and tools: password-managers (n=9); password reuse (n=5); password reuse with permutations (n=8); passwords saved in an encrypted file (n=5); passwords saved in a plaintext file (n=3); passwords cached in browsers (n=5); passwords written on physical paper kept hidden (n=1); passwords kept in draft email (n=1); and passwords memorized (n=10). Several participants used more than one strategy. In a user study by Ion et al. 19% of non-expert users reused passwords, which matches our results [17]. We expected more participants in our study to use password managers, but only 34% of participants did, which is higher than the 24% of non-expert users but much lower than the 74% of expert users in Ion et al. [17] or the 81% of users in a study by Stobert et al. [30]. We suspect the low percentage of password manager use in our study is because many participants' organizations did not feel benign toward third-party cloud-based password managers. One participant mentioned that being able to share passwords was important for him, and that was one of the reasons he did not use password managers.

Table 4: Participant opinions regarding authentication and number of participants who gave a specific rating. N: normal ratings; N*: with volunteered ratings for when something goes wrong.

Opinion about Authentication	N	N*
(1) I don't even notice them.	1	1
(2) I notice them, but they rarely bug me.	9	6
(3) They bug me, but not too much.	10	8
(4) They bug me and I'd like to avoid them.	5	7
(5) They are extremely frustrating.	1	4

6.2.3 Opinions about authentication

Our participants' opinions on authentication vary widely. In the post-logging interview, we asked participants to rate their overall feelings about authentication on a scale from 1 to 5, with 5 being extremely frustrating. Table 4 shows that 16 participants found authentication at least somewhat burdensome. Seven participants, unprompted, gave two opinions when asked about how they feel about authentication: first for how they feel in the normal course of things (column N in the table), and second for how they feel when something goes wrong (column N* in the table), such as forgetting a password, losing a key, or having to change a password. Several participants gave fractional answers, which we rounded down. *"They bug me a little [rating 3] but they give me a sense of security. Shoots to a 5 when I have to set up an account or service or use the phone to enter 15 character password." (P20) "Most of the time it's just the cost of doing business [rating 2] – until it breaks. Then it's a 5 because it stops me doing what I need to do right now." (P12)*

We were interested in whether there was any correlation between participants' authentication opinions and the number of authentication events they performed or the failures they encountered. We expected participants who logged more events or encountered more failures would be more frustrated, but saw no correlation between number of authentications and opinion. This agrees with the NIST study findings [29]. Further, there is no strong correlation across number of failures and participant opinion. We also saw no significant difference between average opinion rating of female and male participants (2.9±1.0 vs. 2.8±0.9).

Best and worst authenticators. The kinds of authenticators participants most liked or disliked varied greatly, as seen in Table 5. Some participants' favorite authenticators were other participants' least favorite. Note that participants' answers were their own and not chosen from a predetermined list. (If they had been from a predetermined list, we might have seen more people choose authenticators such as "cached passwords" as most-liked.) While we supposed many people would complain about passwords, we were surprised by the number who disliked physical authenticators such as keys and badges. Participants also sometimes distinguished

Table 5: Authenticators participants most liked and disliked, and the number of participants (N) who did so. Flash-to-pass is one participant's authentication method that allows her to open her garage door by flashing her headlights, which then also unlocks her house from the garage entry.

Liked	N	Disliked	N
Fingerprints	7	Passwords	16
Badges and passes	6	Physical Keys	6
Pin codes	5	Pin codes	3
Key fobs	5	Badges and passes	2
Physical Keys	3	Fingerprints	1
Passwords	2	Credit cards	1
Cached passwords	2	Barcodes	1
Flash-to-pass	1	Key fob	1
		Everything	1

between the number of times they had to use a particular authenticator versus the amount of effort required each time.

Although the most disliked authenticator varied among participants, for most *having to remember* something (including carrying a physical token) was the explanation. *"I don't like my badge. I never remember to have it on me when I should." (P21) "Passwords, because I have to remember them." (P26)* Another reason to dislike an authenticator (especially keys) was the need to carry it: *"I don't like to carry around physical keys. It's just another thing to manage." (P7)*

Most participants liked an authenticator because it was either *automatic* (keyfobs or badges) or *quick* (4-digit PIN, fingerprint). Interestingly, participants who liked fingerprints and also used them during the study said they encounter failures with fingerprints often – indeed, we observed this in their logs – but they did not seem to mind the failures, because it was quick to try again. *"The fingerprint swipe for my phone [is my favorite]. It failed a lot but you don't have to do much." (P18)* Several participants who did not actually use a fingerprint reader during the study also said they like fingerprint authentication because of its speed and low effort. The need for quick, effortless authentication matches with the findings of De Luca et al. that participants did not favor Face Unlock because they found it slow [8]. Our results suggest that for the majority of participants, an authenticator being quick and effortless is more important than its being accurate in terms of false rejects. There were two exceptions, however. One participant whose wife has a fingerprint reader on her phone dislikes that mode of authentication due to its error rate. Another participant says *"I like the usability and quickness if I hold the phone correctly. But sometimes it really annoys me if there's water or something sticky – after washing my hands – it wouldn't work." (P20)* Perhaps we should require an authentication method to promote rather than punish good hygiene.

6.3 Authentication failures

Authentication failures add to users' frustrations. We observed a higher percentage of authentication failures than we expected. We compute failure rate for an authenticator as the ratio of failed attempts with that authenticator and total attempts with that authenticator. Failed attempts is the number of times a participant tries to authenticate to a resource and fails; for instance, if a participant had to try three times to unlock her phone, and succeeded in the third attempt, she had two failed attempts and a total of three authentication attempts. We did not see any significant difference in failure rates across gender or age. Note that these are all false reject failures, not false accept failures, as self-reporting of events is unlikely to tell us if any of our participants attempted to break into something they should not have.

The six participants who used a fingerprint reader logged a high failure rate of 25%, because one of the participants (P18) injured the finger he uses for fingerprint authentication and thus suffered many failures (44%). The participant reported that he could not authenticate via fingerprint with the injured finger; he would retry until his phone required him to type his password. Two other participants used fingerprint authentication less than five times with a 50% failure rate, so the average failure rate across participants is high. If we exclude the injured participant and two light users of fingerprint authentication, we see a fingerprint biometric failure rate of about 3.1% (± 3.0), which is still higher than we expected.

We saw a 5.6% (± 10.8) failure rate for Mouse clicks, which refer to an authentication event in which participants used a mouse click to authenticate (e.g., choose a certificate, auto-fill a password entry). The failures in mouse click authentication are instances when the participant accidentally chose the wrong certificate or accidentally auto-filled the wrong username and password (e.g., for websites where the participant has multiple accounts). The failure rate with physical keys was about 3.3% (± 7.9). Failures with physical keys were due to events such as a participant selecting the wrong key from her key bunch and trying it on the lock.

Password failure rates

Overall, we found a 5.1% (± 5.8) error rate for passwords among participants. If we look closer, the password failure rates differ based on the target (Websites, Laptops and desktops, Phones, Tablets, and Lockers/Combination locks). Websites have the highest failure rates (11.4% ± 16.8) even though website logins account for only 4.7% of authentication events. Laptop has the second highest failure rate, 7.9% ± 9.1, which surprised us, because laptop or desktop passwords are frequently used, often typed several times a day, so we supposed muscle memory would help reduce this error rate. We observed a 2.3% ± 3.5 failure rate for Phone passwords, a 0.4% ± 1.1 failure rate for Tablet passwords, and a 1.7% ± 2.4 failure rate for locker combination passwords.

In our post-logging interview we asked participants about their high failure rate with passwords. Several participants commented on making mistakes typing passwords (because of the length and/or complexity of the passwords) and forgetting a password, especially for websites that are not often used. This observation matches with past findings by Adams, Sasse, and Lunt that users have trouble recalling infrequently used passwords [1]. Several participants quoted "typing too fast" for getting passwords wrong, either out of habit or because they do not want anyone to see their password. *"I always type it super fast and get it wrong a couple of times." (P16) "It can be stolen easily, that's why I'm always in a hurry in typing a password – it's a mental thing, even if no one is around. It makes me type it quickly – it's instinct." (P14)*

Typing an old password (due to muscle memory) when the laptop password was recently changed or getting confused between devices they use, and typing the password of one device on other, are two more reasons why participants incorrectly entered passwords. *"It's muscle memory and I usually mess up when I update a password. I'll type old ones first and of course it fails." (P2) "I'm on autopilot typing my password, which is different on my PC versus my Mac, so I have an ordered search of passwords I go through until one works." (P1) "I get them [desktop and laptop] mixed up, and I type the wrong password – it's muscle memory." (P3)* One participant commented on not being able to see a password when it is being typed, especially for long passwords. Another participant (P1) complained about his phone being less responsive if he ran too many apps in the background, and "typing in the numbers [PIN] registered too slowly," so he had to retry.

Participants attributed Laptop authentication failures to incorrectly typed passwords, even though they knew the password. They further attributed mistyping passwords during Laptop authentication to their desire to login in quickly. Perhaps certain passwords are easier to type for a user than others of the same length. If the user frequently makes the same mistake when typing a password, perhaps the authentication target can suggest changing the password to the frequently mistyped password. On the other hand, this requires keeping more authentication material in potentially vulnerable places.

7. USE OF AUTHENTICATION LOGS

We engaged in this study to gather information in aid of projects involving authentication. As an example, we used our authentication event logs as workload "traces" for energy consumption simulations of an authenticator device called Mobius.

The Mobius Ring is a prototype of a "universal authenticator." The idea behind Mobius is that the ring will perform authentication tasks on behalf of the user, and will thus take the place of a user's many authenticators: passwords and other secrets, and physical tokens such as keys and badges. Ideally, if Mobius works well, a user would only need to remember one authentication secret (to activate the ring) and carry one authentication token (the ring itself). The ring must sense its presence on a user's finger when activated and deactivate itself when it senses its removal from a user's finger. Existing examples of universal authenticators, some with only a subset of these features, include Pico [28], the Nymi band [27], the NFC Ring [33], and the Java Ring [7].

There are many issues to explore for Mobius, including how to authenticate with the device and how vulnerable it is as a potential central point of failure. One usability concern we explored is whether users must remove the ring for recharging, or whether we can keep it perpetually charged via energy harvesting. If users remove the ring for recharging, they must reauthenticate with it when they put it back on, and they are without their authenticator while it recharges.

The ring prototype is a 3D printed enclosure and its required electronics, including both Bluetooth Low Energy (BLE) and Near Field Communication (NFC). The ring's components and functions consume energy except for the harvesting we can perform during authentication events that use NFC or while holding an NFC-equipped phone with the hand wearing the ring. Using experimentally determined measurements of component and functional energy consumption and harvesting, we use our logs of authentication events as workloads to estimate the energy neutrality of ring operation. We assume that interactions with mobile phones, transportation transponders, and card-based doorlocks use NFC, while other events use BLE. We treat phone unlocks as phone usage events (NFC harvesting opportunities) and vary the length of the associated time a user might hold the phone. We find that for the average session of 2 minutes across users as reported in the LiveLab traces from Rice University [26], it is feasible to keep Mobius perpetually powered using only harvested power given our observed workloads (see Appendix G).

8. SUMMARY

We present the design and implementation of a wearable digital diary study, our findings about participants' authentication habits and opinions, and an example use of our study's event logs as a workload for evaluating a potential authentication device. Overall we find that authentication is a noticeable annoyance in participants' lives, but they are creative in devising ways to cope with it. On average our participants performed 25% of their authentications with a physical token, and several participants expressed frustration over the authentication material they have to carry. Participants encountered authentication failure rates of about 3-5% during the study, with higher failure rates (7–12%) for PCs and websites. Participants' opinions about how burdensome authentication is to them vary greatly, as do their likes and dislikes about authenticators, with no one authentication method favored by everyone. In the study we used a smartwatch app with a novel slot-machine type interface for quick logging of events, and most of our participants favored the smartwatch over the smartphone for in-the-moment logging. We believe such wearable digital diary studies may be good platforms to conduct future studies that benefit from in-the-moment logging.

We are making our study data publicly available. Please contact the authors for more details.

9. ACKNOWLEDGMENTS

We thank the many people who greatly helped us with user study advice or feedback from pilot studies: Sunny Consolvo, April Mitchell, Iris Beneli, Alvin AuYoung, Ben Eric Andow, Animesh Srivastava, Kassem Fawaz, Jim Mann, Aarathi Prasad, and Denise Anthony. We also thank the SOUPS reviewers for their very helpful comments, and our paper shepherd, Cormac Herley, for his excellent help and encouragement. Any remaining errors, misapprehensions, or stupidities are entirely the fault of the authors.

10. REFERENCES

[1] A. Adams, M. A. Sasse, and P. Lunt. Making passwords secure and usable. In *People and Computers XII*, pages 1–19. Springer London, Jan. 1997. DOI 10.1007/978-1-4471-3601-9_1.

[2] AnalogDevices. ADXL362. Online at http://www.analog.com/en/products/mems/mems-accelerometers/adxl362.html. Last accessed June 2016.

[3] AustrianMicrosystems. AS3953. Online at http://ams.com/eng/Products/Wireless-Connectivity/Sensor-Tags-Interfaces/AS3953. Last accessed June 2016.

[4] L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. Lessons learned from the deployment of a smartphone-based access-control system. In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pages 64–75, 2007. DOI 10.1145/1280680.1280689.

[5] L. F. Cranor. What's wrong with your pa$$w0rd? TED, Mar. 2014. Online at http://www.ted.com/talks/lorrie_faith_cranor_what_s_wrong_with_your_pa_w0rd?language=en. Last accessed June 2016.

[6] L. F. Cranor and S. Garfinkel. *Security and usability: Designing secure systems that people can use*. O'Reilly Media, Inc., 2005.

[7] S. M. Curry. An introduction to the java ring. Java World, April 1998. Online at http://www.javaworld.com/article/2076641/learn-java/an-introduction-to-the-java-ring.html. Last accessed June 2016.

[8] A. De Luca, A. Hang, E. von Zezschwitz, and H. Hussmann. 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 (CHI)*, pages 1411–1414, 2015. DOI 10.1145/2702123.2702141.

[9] S. Egelman, S. Jain, R. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are you ready to lock? In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Nov. 2014. DOI 10.1145/2660267.2660273.

[10] D. Florêncio and C. Herley. A large-scale study of web password habits. In *Proceedings of the International World Wide Web Conference (WWW)*. ACM, 2007.

[11] A. Greenberg. The app I used to break into my neighbor's home. Wired, July 2014. Online at http://www.wired.com/2014/07/keyme-let-me-break-in/. Last accessed June 2016.

[12] J. Gummeson, B. Priyantha, and J. Liu. An energy harvesting wearable ring platform for gesture input on surfaces. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 162–175. ACM, 2014. DOI 10.1145/2594368.2594389.

[13] M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith. It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pages 213–230, July 2014. Online at https://www.usenix.org/system/files/conference/soups2014/soups14-paper-harbach.pdf. Last accessed June 2016.

[14] E. Hayashi and J. Hong. A diary study of password usage in daily life. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, pages 2627–2630, 2011. DOI 10.1145/1978942.1979326.

[15] C. Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the Workshop on New Security Paradigms Workshop (NSPW)*, pages 133–144, 2009. DOI 10.1145/1719030.1719050.

[16] D. Hintze, R. D. Findling, M. Muaaz, S. Scholz, and R. Mayrhofer. Diversity in locked and unlocked mobile device usage. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp Adjunct)*, pages 379–384, 2014. DOI 10.1145/2638728.2641697.

[17] I. Ion, R. Reeder, and S. Consolvo. "...no one can hack my mind": Comparing expert and non-expert security practices. In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pages 323–346, July 2015. Online at https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf. Last accessed June 2016.

[18] I. Lillegaard, E. Løken, and L. Andersen. Relative validation of a pre-coded food diary among children, under-reporting varies with reporting day and time of the day. *European journal of clinical nutrition*, 61(1):61–68, 2007. DOI 10.1038/sj.ejcn.1602487.

[19] I. Lookout, Harris Interactive. Mobile mindset study, June 2012. Online at https://www.lookout.com/static/ee_images/lookout-mobile-mindset-2012.pdf. Last accessed June 2016.

[20] Lookout, Inc., Harris Interactive. Survey reveals consumers exhibit risky behaviors despite valuing their privacy on mobile devices, Oct. 2013. Online at https://www.lookout.com/news-mobile-security/sprint-lookout-mobile-privacy-survey. Last accessed June 2016.

[21] MaximSemiconductor. MAX17058. Online at http://datasheets.maximintegrated.com/en/ds/MAX17058-MAX17059.pdf. Last accessed June 2016.

[22] MaximSemiconductor. MAX17710. Online at http://datasheets.maximintegrated.com/en/ds/MAX17710.pdf. Last accessed June 2016.

[23] M. B. Miles and A. M. Huberman. *Qualitative data analysis: An expanded sourcebook*. Sage, second edition, 1994.

[24] Motorola. Motorola MOTOACTV. Online at https://motoactv.com/home/page/features.html. Last accessed June 2016.

[25] NordicSemiconductor. nRF51822. Online at https://www.nordicsemi.com/eng/Products/Bluetooth-Smart-Bluetooth-low-energy/nRF51822. Last accessed June 2016.

[26] C. Shepard, A. Rahmati, C. Tossell, L. Zhong, and P. Kortum. Livelab: measuring wireless networks and smartphone users in the field. *ACM SIGMETRICS Performance Evaluation Review*, 38(3):15–20, 2011. DOI 10.1145/1925019.1925023.

[27] H. Slade. Bionym inks $14m to get password-replacing wearable, Nymi out the door. Forbes, Sept. 2014.

[28] F. Stajano. Pico: No more passwords! In *Security Protocols XIX*, volume 7114 of *Lecture Notes in Computer Science*, pages 49–81. Springer-Verlag Berlin, Mar. 2011. DOI 10.1007/978-3-642-25867-1_6.

[29] M. Steves, D. Chisnell, A. Sasse, K. Krol, M. Theofanos, and H. Wald. Report: Authentication diary study. Technical Report NISTIR 7983, National Institute of Standards and Technology (NIST), 2014. DOI 10.6028/NIST.IR.7983.

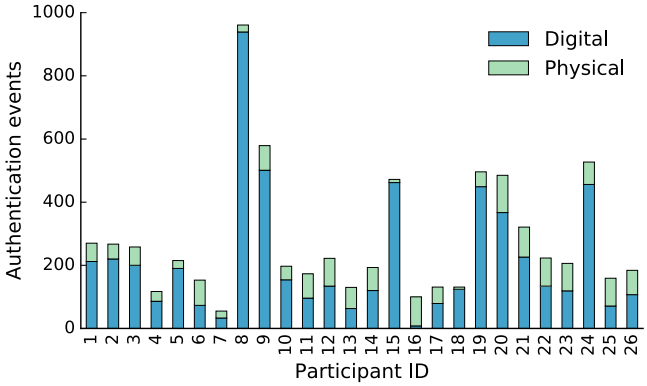


Figure 6: Authentication across participants, by category of target. (See Section 6.1.2 for target categorization.)

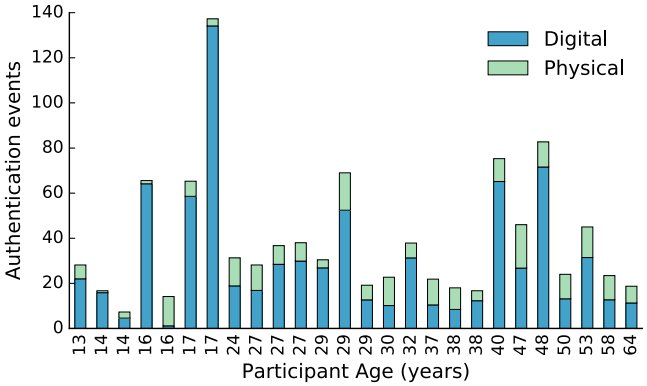


Figure 7: Average authentication events to digital and physical targets per day, by age of participants.

[30] E. Stobert and R. Biddle. The password life cycle: User behaviour in managing passwords. In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pages 243–255, July 2014. Online at https://www.usenix.org/system/files/conference/soups2014/soups14-paper-stobert.pdf. Last accessed June 2016.

[31] I. Urbina. The secret life of passwords. New York Times, Nov. 2014. Online at http://www.nytimes.com/2014/11/19/magazine/the-secret-life-of-passwords.html. Last accessed June 2016.

[32] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy. Modifying smartphone user locking behavior. In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, pages 10:1–10:14, July 2013. DOI 10.1145/2501604.2501614.

[33] R. Whitwam. NFC ring hands-on: Practice makes... pretty good. Android Police, Mar. 2014. Online at http://www.androidpolice.com/2014/03/09/nfc-ring-hands-on-practice-makes-pretty-good-video/. Last accessed June 2016.

[34] R. Witty and K. Brittain. Password Reset: Self-Service That You Will Love. Gartner Research, April 2002. Online at http://www.gartner.com/DisplayDocument?ref=g_search&id=354760. Last accessed June 2016.

APPENDIX

A. MORE AUTHENTICATION PATTERNS

Here we provide supplemental results for the authentication patterns covered in Section 6.1.

Distribution of events by target. Figure 6 shows the number of authentication events, for digital and physical targets, for each participant (see Section 6.1.2 for the categorization). All participants performed authentication with physical targets during the study, but there is high variance among them, with P8 logging only 2% of his authentications as physical and P16 logging 92% as physical. The average percentage of physical authentication events logged by each participant is 30.7% with a standard deviation of 20.2%.

Distribution of events by age. Figure 7 shows authentication events logged by participant age for digital and physical targets.

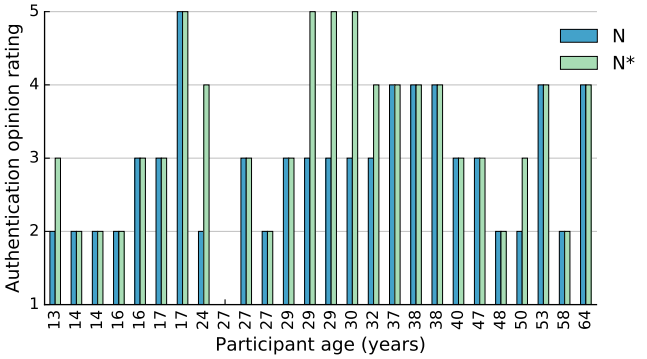


Figure 10: Participant opinions regarding authentication, by age of participants, both normally (N) and with ratings some participants volunteered for when something goes wrong (N*).

Weekday vs. Weekend. Figure 8 shows the average number of authentication events each participant logged during an average day Monday through Friday versus an average day on a weekend.

Distribution of events by hour of the day. Figure 9 shows the number of authentication events performed at different hours of a day, *averaged across both participants and days*. All our participants have day jobs or generally follow a day-oriented schedule, and this is evident from the figure, as there are few events after midnight. However, there is no hour where on average someone isn't authenticating with something.

Authentication opinion by age and logged events. In our post-logging interviews we asked participants to rate their authentication experience on a scale of 1 to 5, with 5 being extremely frustrating. Figure 10, Figure 11 and Figure 12 show the distribution of their opinion ratings by their age, the number of authentication events they performed, and the number of failed events they encountered in the study, both during the normal course of things (N) and when something goes wrong (N*). As we summarized in Section 6.2.3, we saw no correlation between participant opinions and their age, number of performed authentications, or number of encountered authentication failures.

B. PRE-LOGGING INTERVIEW

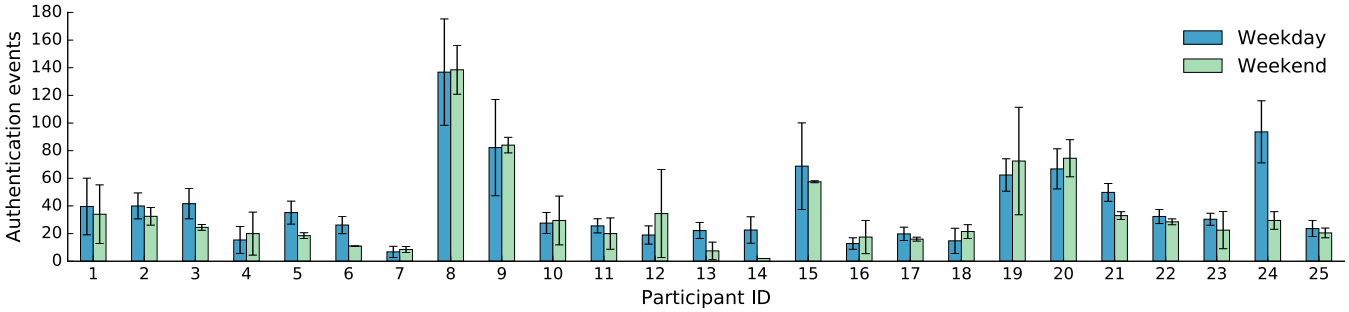


Figure 8: Number of authentication events participants performed on a weekday (averaged across Monday through Friday) versus a weekend day (averaged across Saturday and Sunday). Error bars show standard deviations.

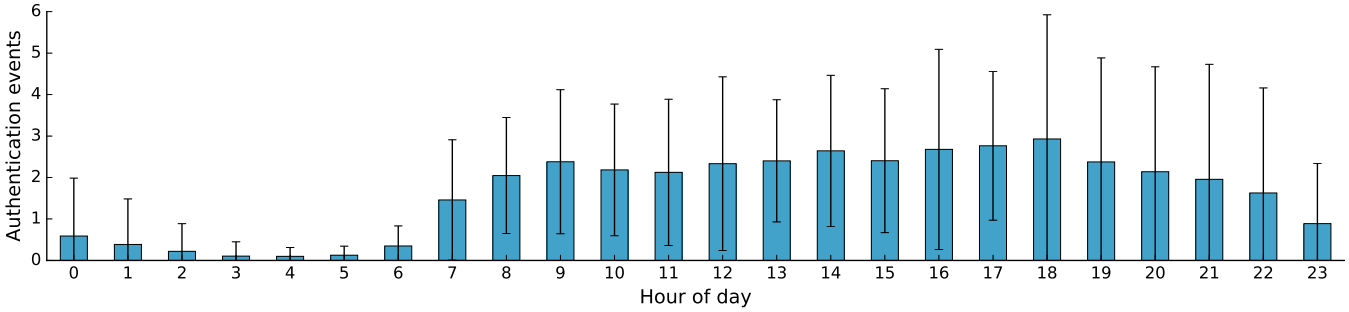


Figure 9: Number of authentication events performed at different hours of the day, averaged (± standard deviation) across participants and days.

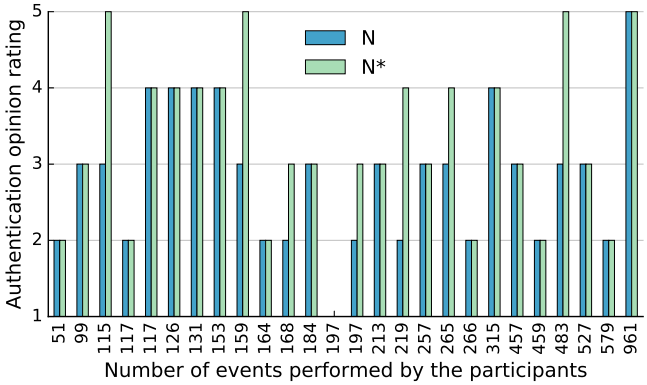


Figure 11: Participant opinions regarding authentication, by the number of authentication events performed by participants, both normally (N) and with ratings some participants volunteered for when something goes wrong (N*).

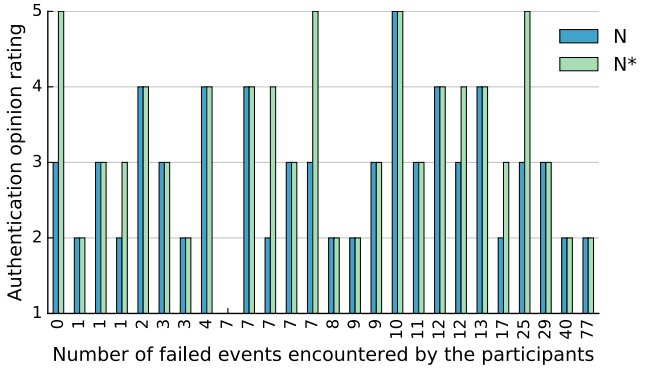


Figure 12: Participant opinions regarding authentication, by the number of failed events encountered by participants, both normally (N) and with ratings some participants volunteered for when something goes wrong (N*).

We used the following questions to guide our semi-structured interviews, before the participants began self-logging their authentication events. In addition to these questions, we welcomed topics and discussions about authentication initiated by participants.

- What is your typical day, in terms of authentication events?
- What targets and authenticators do you use? [We explained the meaning of targets and authenticators.]
- What do you carry with you? [We guided them to look in their bags, wallets, pockets, and purses.])
- How many times a day do you think you authenticate yourself with something?
- How do you manage your passwords?
- How do you choose/create passwords?

C. POST-LOGGING INTERVIEW

We used the following questions to guide our semi-structured interviews after participants logged their authentication events for one week. In addition to these questions, we probed participants about their authentication behavior, based on the logged data.

- What are your favorite authenticators?
- What are your least favorite authenticators?

- Did you log all events?
- Did your participation in the study lead you to be more aware of authentication events?
- How did your participation in the study change your authentication behavior?
- Did you notice any patterns in your authentication behavior?
- How do you feel about authentication events? (Multiple choice question)
  1. I don't even notice them.
  2. I notice them, but they rarely bug me.
  3. They bug me, but not too much.
  4. They bug me and I'd like to avoid them.
  5. They are extremely frustrating.
- How do you feel about passwords?
- In the future, what kinds of changes or inventions would you like to see related to authentication?
- Do you have any comments/suggestions/concerns about the study?

D. GUESSING ABOUT AUTHENTICATION

How accurate are people's feelings about how much authentication they perform in a day? In the pre-logging interview we asked participants how many times they believe they authenticate themselves every day on average. Fifteen participants overestimated their daily authentications and all but one of them did so significantly (by more than 25%). Eleven underestimated. Combined, the average of guessed daily authentication events was 47 ($\pm$ 31) vs. 39 ($\pm$ 29) logged authentications. Most of our participants overestimated, and only two participants came within 10% of their self-reported numbers.

E. PRIVACY ATTITUDES

One question many related studies consider is how much people care about privacy. We observed a higher level of care than we expected from our participants, with only two of the seven teenagers leaving their phones unlocked and two of the adults doing so. While our study does not include enough participants to make broad generalizations, we see evidence that teenagers and not just adults are interested in privacy and security, although teens may have less useful understandings of how to achieve it. We asked all participants why they chose to lock or leave unlocked their personal devices and resources. Both of the teenagers who did not lock their phones said it was because their phones always remained under their physical control, or in a safe environment (a desk at home). One of them also said he was careful not to keep anything private on his phone, and that he backed it up so nothing would be lost if his phone were lost. The other five teenagers all locked their personal devices with the intent of keeping them safe from the prying eyes of friends and sometimes parents and siblings. *"[I lock my phone] so people don't just go inside my phone – it's not pleasant for anyone this kind of snooping." (P8)* Three of the teenagers and seven of the adults also mentioned that besides having activity timeouts on their personal devices that automatically lock them, they deliberately lock their devices whenever they put them down or walk away from them, regardless of timeouts. On the other hand, both teenage girls (but none of the teenage boys) mentioned that they share their phone passwords with selected friends. This sharing seems to have social significance, and one of the teenagers suggested at the end of her post-logging interview that any kind of new authentication technology needs to support sharing of access. *"I want to use thumbprints on everything but I can't pass thumbprints to others – some friends can have access to my phone but not everyone." (P19)*

F. QUOTES FROM PARTICIPANTS

Here we include a few more participant comments, in addition to those already in the paper, because we found them especially interesting, representative of a particular point, or entertaining.

F.1 Feelings about authentication

"It's important – necessary, so you just do it." (P3)

"Most of the time it's just the cost of doing business – until it breaks. Then it's a 5 because it stops me doing what I need to do right now." (P12)

"It's kind of evil. It's a constant reminder that there are bad people. It makes me feel kind of bad, kind of angry." (P15)

"Sometimes it's annoying, but not all the time. I'm also very thankful for it." (P19)

"They bug me a little but they give me a sense of security. Shoots to a 5 when I have to set up an account or service or use the phone to enter 15 character password..." (P20)

"But when things go wrong, that's the worst. My worst was that I locked my keys in the car as I was getting out of it with two cats in two carriers to take them to their vet appointment. I also had my infant son with me in his car seat and I put down the carriers to go around to the other side of the car and get my son out, but I'd somehow locked the door when I closed it and my keys were inside the door and so my son was locked in the car. I couldn't leave him there and I couldn't leave the cats and it was horrible. But a guy in the parking lot was able to break into my car for me. I was never happier in my life to meet a competent criminal." (P21)

F.2 Likes and dislikes for authenticators

Likes:

"[phone PIN] my fingers know where to go on the keypad." (P6)

"Fingerprint, cause it's very quick. The rest all take significantly more time. Even for a key fob – you have to take something out – it would be great if I could use a fingerprint at the [company] entrance." (P14)

Dislikes:

"[Most effort are physical keys] first you have to find it in your purse, then pick out the right key from the ring, then get it in your hand correctly to unlock the door. There's a difference between fast but many times and lots of effort but only a few times. So keys were a lot of effort, and the phone unlock wasn't, but I had to do it most often so it adds up." (P3)

"Typing passwords on the phone and laptop took the most effort for frequency and chance for failure. I hate passwords!

We cannot do patterns or face recognition to get our work email...They have improved the initial pin interface on the Galaxy but still there's a greater than 20% or 25% failure. Initially the keyboard was large and mis-hitting was high. But still there is a problem when I am sleepy or in the dark or when I don't wear my glasses...I'm also not happy with door key unlocking. The door key at my home takes a lot of pressure and when carrying your son's books and toys and your bag on the other arm or carrying your son on one arm sleeping, it is really hard...Also my car if I carry the [fob] is supposed to unlock from a button on the handle. I don't have to press the fob. But to unlock it for everyone you have to press it twice from the driver side and only once from the passenger side. This is confusing and I lock it sometimes instead. So sometimes I bring out the fob and deliberately use it to unlock even though I'm not supposed to have to do that." (P4)

"Credit cards because you have to pull them out of your wallet." (P6)

"Passwords – they are complicated and annoying." (P8)

"You're booting some device and have to type in a long password and you can't be sure you got it right 'cause you can't see it. Is it typed wrong or is the keyboard in the wrong mode? You gotta preserve this password over all other values to keep the devices running." (P11)

"I like [the] key fob as opposed to physical stuff. Remote authentication without physical contact is a much better experience than physical contact or swiping. But the fob is too big – it's difficult to carry." (P14)

"Long-assed passwords for sites I rarely go to are obnoxious. But keys could also be bad...Which one is which and they all get tangled up and you have to find it and if it were my phone I could just do it and then I realize I'm just a bratty girl from Silicon Valley and I should be okay with taking the 15 seconds to do it." (P15)

"I don't like my badge. I never remember to have it on me when I should...Also, I feel embarrassed wearing it – kind of like I'm a kid in kindergarten with a name tag. And I hate my photo that's on it. If you forget it then you're kind of humiliated at the front desk in the lobby. It doesn't fit on my keychain, so where else should I put it? In my purse – 'cause I always bring my purse to work. But I have to put it in a special pocket or I can't find it in my purse and think I've left it somewhere even if I haven't." (P21)

G. MOBIUS RING ENERGY SIMULATIONS

The Mobius ring, depicted in Figure 13, includes the following components:

- 3D printed enclosure.
- Near Field Communications (NFC) using the AS3953 [3] NFC interface chip.
- Bluetooth Low Energy System on Chip (SoC), the Nordic Semiconductor nRF51822 [25]. We intend to use the flash memory of this SoC to store encrypted passwords and pins in our prototype.
- A low power 3-axis accelerometer, the ADXL362 [2], for tap detection for entering the activation pin for the ring (the one secret the user must remember).

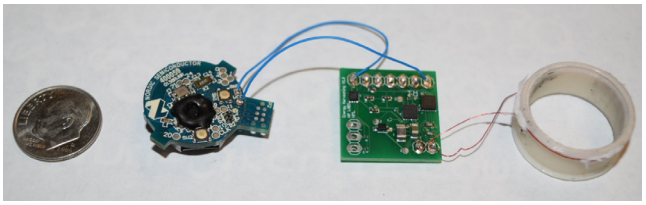


Figure 13: The components used in our current Mobius prototype are no larger than a typical Signet ring. A 10 mAh battery is behind the harvesting board (green).

- Pressure sensor (not yet implemented) mounted on the inside periphery of the ring to sense whether the ring is on the user's finger.
- The NFC interface stores the excess energy beyond what is required for authentication purposes in a small 10 mAh battery.
- We embed the NFC tag coil by winding a few turns of magnet wire around the circumference of the ring, similar to the approach used by Gummeson et al. [12].
- Prior to storage, the energy is conditioned by a MAX17710 energy harvesting chip [22], with charge state monitored using a MAX17058 fuel gauge IC [21].

Our first measurement result looks at how much energy we can harvest from NFC sources and effectively store in the ring's battery. To understand the end-to-end efficiency of energy storage, we monitor battery state using the onboard fuel gauge IC. Placing the ring within 5 mm above the NFC antenna embedded inside a Motorola Moto X, we observe an average harvesting rate of 1.67 mW.

Next, we look at the power consumption of different ring components to help understand the ring's steady state energy balance. The CPU portion of the BLE SoC consumes 1.08 μW of power in sleep state, and 4.32 mW while active. The BLE radio consumes 12.6 mW of power while transmitting at a power of -8 dBm and 23.4 mW of power while in receive mode. The accelerometer consumes 5 μW of power while actively detecting PIN entries, and consumes 270 nW while in a low power wakeup mode that is used to initiate authentication with a remote target. Using the 133.2 Joule buffer in Mobius, the ring can sustain itself in a low power wakeup mode for 132.6 days without any charging while polling its removal sensor at a rate of one hertz.

We model the energy consumed by a BLE authentication event by considering several steps of operation: 1) after a user taps the ring to wake it up, Mobius sends advertisement beacons to make authentication targets aware of its presence, 2) the authentication target initiates an unencrypted connection with Mobius, 3) Mobius and the authentication target encrypt the connection using a shared long term key that was previously established during bonding, 4) the ring sends an encrypted "unlock" command to the authentication target, and 5) the connection terminates.

When considering the power costs of processing and communication, an advertising interval of one second, a latency of four seconds to establish a connection, a BLE connection interval of 10 ms, and a BLE connection length of one second, Mobius consumes 419 μJ of energy per BLE authentication event. With our current energy buffer, we can handle

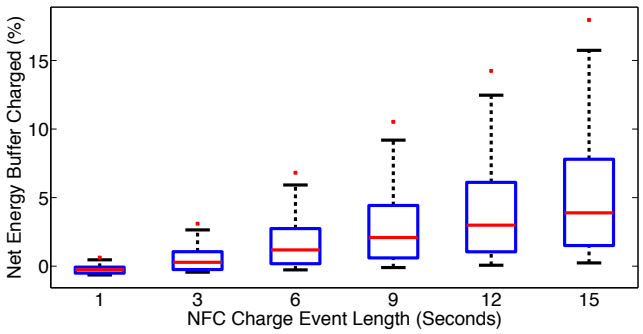


Figure 14: We model NFC charging events as interactions with mobile phones, transportation transponders, and card-based door-locks. We only need phone interactions to be an average of 15 seconds in length to keep the ring's buffer energy neutral across an entire week of authentication.

286,109 BLE authentication events – this assumes the last 10% of the battery is unusable due to low voltage.

Equipped with information about various hardware costs and the results from our user study, we seek to understand the feasibility of using Mobius as a perpetually powered universal authenticator. Since our hardware design is preliminary, our evaluation criterion is the overall energy neutrality of operation during the week we conducted the user study. During each simulation, Mobius' energy buffer is initialized to be at 50% capacity to avoid any coldstart effects.

The user study event logs allow us to estimate the impact a hypothetical Mobius workload has on the energy neutrality of operation. For our power simulations, we exclude data from participants for whom we have no automatically logged phone unlocks.

Our first results look at how changes in the length of mobile phone usage impact the energy neutrality of Mobius. In this experiment, we assume that doors unlocked with a card and transportation authentication targets each provide Mobius two seconds of charge time, but we vary the charge time provided through use of mobile phones. We assume that all other authentication targets use BLE for authentication and that when not authenticating, Mobius is in its low power mode where it seeks to detect removal events. We show the results of this study in Figure 14. When considering a very limited charge opportunity of one second during mobile phone use, no user experienced more than a ∼0.7% decrease in buffered energy, meaning that Mobius could run for more than 100 weeks before depleting its battery. After increasing the phone use length to 15 seconds, all but one user sees an overall increase in buffered energy after a week of operation; this user experiences a decrease of 0.01%. When we consider more realistic measures of the length of mobile phone use, such as an average of two minutes across users as reported in the LiveLab traces from Rice University [26], it seems feasible to keep Mobius perpetually powered using only harvested power.

Our final evaluation considers how decreasing the size of the energy buffer impacts the availability of Mobius for authentication. Our current design does not use the current battery for any fundamental reason; it was available off the shelf and amenable to the ring form factor. Since the battery used in our implementation is bigger than it needs to be, we currently do not experience any failures in authentication due to energy starvation. If we scale the energy buffer size down, we start to see failures in BLE-enabled authentication events based on their temporal distribution among charging opportunities and energy lost to sleep. For example, a significant amount of energy will be lost at night when users are sleeping rather than accessing their mobile phones. Figure 15 shows the number of failures across all users for five orders of magnitude of energy buffer size; we find that there are no authentication failures as a result of energy starvation for an energy buffer greater than or equal to one Joule in energy capacity. This result shows that the battery we are currently using is more than two orders of magnitude larger than it needs to be, indicating that there are opportunities for further platform miniaturization.

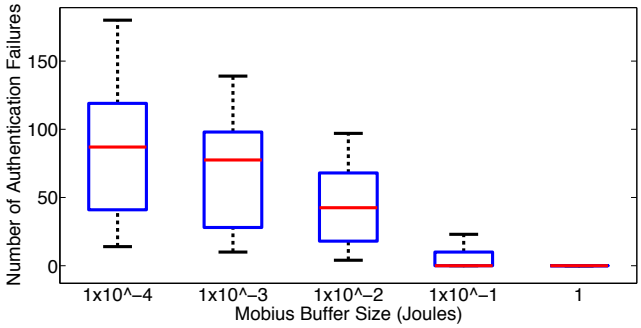


Figure 15: The battery currently used in our Mobius prototype is more than two orders of magnitude larger than it needs to be. A one Joule buffer has sufficient energy capacity to completely avoid failures due to energy starvation.

Our simulation study has several possible sources of inaccuracy that affect our ability to calculate how well charged we are able to keep the ring. First, the number of phone unlock events does not tell us how long the user keeps his phone in his hand after unlocking it. This means we do not know the length of time the ring can recharge due to its proximity to the NFC reader in the phone. However, we make a conservative assumption that is smaller than the unlock durations observed in the LiveLab traces. Second, the user does not necessarily hold his phone in the hand wearing the ring and the specific hand placement will result in variation of harvesting power – we leave a more detailed harvesting study to future work.