Towards Usable and Secure Location-based Smartphone Authentication

Geumhwan Cho, *Sungkyunkwan University;* Sungsu Kwag and Jun Ho Huh, *Samsung Research;* Bedeuro Kim, *Sungkyunkwan University;* Choong-Hoon Lee, *Samsung Research;* Hyoungshick Kim, *Sungkyunkwan University*

https://www.usenix.org/conference/soups2021/presentation/cho

This paper is included in the Proceedings of the Seventeenth Symposium on Usable Privacy and Security.

August 9–10, 2021

978-1-939133-25-0

Open access to the Proceedings of the Seventeenth Symposium on Usable Privacy and Security is sponsored by

Towards Usable and Secure Location-based Smartphone Authentication

Geumhwan Cho
Sungkyunkwan University

Sungsu Kwag
Samsung Research

Jun Ho Huh
Samsung Research

Bedeuro Kim
Sungkyunkwan University

Choong-Hoon Lee
Samsung Research

Hyoungshick Kim
Sungkyunkwan University

Abstract

The concept of using location information to unlock smartphones is widely available on Android phones. To date, however, not much research has been conducted on investigating security and usability requirements for designing such location-based authentication services. To bridge this gap, we interviewed 18 participants, studying users' perceptions and identifying key design requirements such as the need to support fine-grained indoor location registration and location (unlock coverage) size adjustment. We then conducted a field study with 29 participants and a fully-functioning application to study real-world usage behaviors. On average, the participants were able to reduce about 36% of manual unlock attempts by using our application for three weeks. 28 participants enduringly used registered locations to unlock their phones despite being able to delete them during the study and unlock manually instead. Worryingly, however, 23 participants registered at least one insecure location – defined as a location where an unwanted adversary can physically access their phones – as a trusted location mainly due to convenience or low (perceived) likelihood of phones being attacked. 52 out of 65 total registered locations were classified as insecure by the definition above. Interestingly, regardless of whether locations were considered secure or insecure, the participants preferred to select large phone unlock coverage areas.

1 Introduction

Users' location information can be used as an additional factor to improve authentication security or usability [26]. For instance, users' daily location traits can be trained and used to detect anomalous use of smartphones. Banks detect financial frauds in a similar way [19,22]. In a risk-based authentication scheme [14], users may be allowed to use certain services without using explicit authentication if they are logging in from a secure location.

In 2014, Google launched an automatic phone unlock scheme for Android called "Smart Lock" [1]. One of its features allows users to freely select "trusted places" to automatically unlock phones, and keep them unlocked while users are using their phones within secure locations that are supposed to be safe from unauthorized access. Smart Lock's trusted places feature relies mainly on GPS to detect users' trusted locations. As a result, Google estimates that phones may remain unlocked within a radius of up to about 80 meters (from the registered spot) [1] – specifying a fine-grained indoor location area is almost infeasible. Users cannot customize trusted location sizes – there is no option to reduce or increase location sizes. Such limitations may raise security and usability concerns for users, and discourage them from adopting this scheme [20]. In this paper, we focus on this specific notion of unlocking smartphones based on location information – identifying key design requirements, gauging real-world usability benefits related to reducing manual (explicit) phone unlock burden, and analyzing potential security issues that could arise from freely allowing users to select trusted places.

The use of location information to unlock phones implies that we are treating this information – i.e., the physical security offered by trusted locations – to provide a comparable security level to those provided by existing screen unlock schemes. This assumption could potentially put smartphone users at severe risks of phone breaches. For instance, a user with low-security awareness might register public locations such as cafes or sports facilities for convenience. An adversary who manages to steal that phone would be able to easily unlock it by just going near those locations.

We first conducted an interview study with 18 participants to understand users' perceptions and expectations on

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

location-based smartphone authentication. We then developed a location-based screen unlock application for Android based on the design requirements identified from the first study, and conducted a real-world field study with 29 participants. The reason we developed our own application was to reuse the Smart Lock concepts (since this is the only known real-world application) while also providing support for indoor location detection based on WiFi RSSI information. After obtaining informed consent, we asked the participants to install our application on their own phones and use it for three weeks; we logged the participants' real-world usage behaviors. The key observations made from analyzing this data and paper contributions are summarized below:

- We identified security and usability requirements for developing location-based authentication systems through the first study: these requirements include the need to support fine-grained indoor location registration, and allow users to select and adjust location coverage sizes. The field study results confirmed that people indeed register indoor locations (e.g., homes and offices), and choose different location sizes.
- Using a fully functional application (implemented based on the requirements), we conducted a three-week field study to collect real-world usage data. Our findings indicate that the location-based automatic unlock feature would be immensely beneficial – the participants, on average, were able to reduce about 36% of their explicit unlock attempts.
- Even though the participants were free to delete all locations during the study (and go back to manual unlocks), 28 out of 29 participants continued using at least one location throughout the study. During the post-study interview, 22 participants said that they would continue using our application due to the automatic phone unlock convenience. These observations highlight the usability benefits.
- Worryingly, we identified two critical security issues: (1) many users have a tendency to register insecure locations (defined as locations that are vulnerable to unauthorized phone access) – 52 out of 65 registered locations were considered potentially insecure; and (2) regardless of whether locations are considered secure or insecure, the participants preferred to select large location coverage sizes.

2 Related work

The concept of using location information for authentication was first introduced by Denning and MacDoran [7]. The key idea is to use a user's physical location information as an additional factor to verify the validity of log in requests. Numerous existing studies [14, 19, 22] have applied this idea to improve authentication security by verifying users' known locations. For example, banks may compare users' phone locations and the payment terminal locations to detect frauds [19, 22]. Daniel et al. [14] proposed a location-based risk assessment framework to facilitate automatic adjustment of required authentication factors (steps) based on risk levels.

Several studies [4, 10, 15, 18] have demonstrated that users' physical location traits can be unique and be used to identify users. Fridman et al. [10] demonstrated that device location information could be used to identify users – using GPS coordinates as the main classification features, they were able to identify users with an FAR and an FRR below 0.1 and 0.05, respectively. Agadakos et al. [4] proposed a location-based authentication method that analyzes proximity information between users' phones and paired IoT devices. Two recent studies [5, 16] proposed phone theft detection techniques based on the use of acoustic signals to measure physical distance between users and phones. Li et al. [16] used frequency-modulated carrier waves to measure physical distances. Chen et al. [5] used information about users' motions to improve the accuracy of measuring distances.

An accurate algorithm for determining users' locations is essential in implementing location-based authentication. Several studies (e.g., [6]) discussed the use of wireless (e.g., WiFi) signals to identify device locations. Hilsenbeck et al. [13] presented a fusion approach using sensors: they were able to track a user with 1.52m accuracy 50% of the time, and 4.53m accuracy 90% of the time. Shu et al. [25] presented another fusion approach using magnetic and WiFi signals to achieve 3.5m accuracy 90% of the time. Abbas et al. [3] proposed a deep learning-based indoor localization technique to achieve 2.38m accuracy 50% of the time in a university building. Such techniques focus on developing classification models for accurate location detection. In this paper, we implemented a fully working indoor location-based authentication solution that does not require special hardware or a fingerprinted wireless signal map.

Mehrabi et al. [20] investigated how users perceive Smart Lock and its trusted places feature [1]. Their surveys, however, primarily focus on understanding why people are willing to use or not use the trusted places feature. We dived deep into understanding users' specific functional needs and expected behaviors to derive application design requirements. Moreover, through the field study, we investigated the real-world effectiveness of location-based automatic unlock schemes and identified security issues that need to be mitigated.

3 Requirement Study

3.1 Methodology

As the first step, we conducted a semi-structured interview study to understand users' perceptions and expectations with respect to the use of trusted physical locations to unlock their phones implicitly. We recruited 18 participants who are aged 18 years or older by posting advertisements on online notice boards at a university as well as selectively recruiting people from local communities based on their age and work expe-

riences to ensure that overall demographic proportions are similar to those presented in [2]. Two moderators together ensured that all of the interview questions were asked and consistently understood by the participants. Each study session took about 20 minutes on average to complete, and participants were compensated for their time with a USD 10 gift card. All interviews were recorded and transcribed.

As for all open-ended questions, we applied structural coding techniques [17] [24] to identify responses to each interview question on transcripts, and 24 topic codes were identified through thematic coding. One researcher was the primary coder, responsible for creating and updating the codebook. The other two researchers independently coded interview transcripts, revised the codebook, and resolved disagreements. After resolving coding disagreements, we achieved inter-coder agreement of 89% Cohen's Kappa [9].

The participants were informed that participation is voluntary and confidential, and they have the right to terminate the study without penalty. We asked for their permission to audio-record entire interview sessions. The ethical perspective of the requirement study was validated through an institutional review board (IRB) at a university.

Before asking questions, the interviewers explained the basic concept of registering trusted locations, and using those registered locations to automatically unlock phones. We borrowed the exact instruction phrase from Smart Lock, which says "*Add location where device should be unlocked.*"

We then asked participants three simple questions about how this authentication service would work in practice (e.g., "*What happens to your phone when you physically move to a place that you already registered as a trusted location?*") to ensure that all participants had an adequate level of understanding of this concept before the interview. For those who answered any of the three questions wrong, we spent more time explaining this concept until they were comfortable with it.

The interview questions are as follows: The first question we asked was "*Provide a list of places that you would register as a trusted location and explain why.*" We then asked the participants to "*Select a size (that defines the area in which their phones would remain unlocked) for each of your trusted locations, and explain why.*" The participants were also asked to explain what would be a tolerable setup time (i.e., time taken to register one location), battery consumption level, and location detection accuracy.

Before conducting the interview, we conducted a pilot study with 3 participants and used their feedback to revise the study structure, interview questions, and guidelines.

3.2 Results

3.2.1 Demographics

We interviewed a total of 18 participants. 10 out of 18 were females, and the average age was 39.1 (σ = 11.6). 9 participants had a university degree, and 6 participants had a master (or doctoral) degree. 13 participants said they unlock their phones many times an hour. 15 participants said they store sensitive or confidential information on their phones. 9 different occupations were reported with "personal care and service occupations," "student," "education, training, and library occupations," and "management occupations" being the top ones. Only one participant used Smart Lock and registered home as a trusted place. To demonstrate the representativeness of the samples, we compared the age, gender, and education distributions against the US smartphone population reported in [2]. We used Fisher's exact tests to show that there are no significant differences in age ($p = 0.26$), gender ($p = 0.64$), and education ($p = 0.18$) distributions. The details of demographics are summarized in Appendix A. We performed data collection and analyses concurrently until we reached theoretical saturation. Figure 1 shows the code saturation results. There are no new codes between 17th and 18th participants. The number of codes reported in the requirement study is 23 in total.

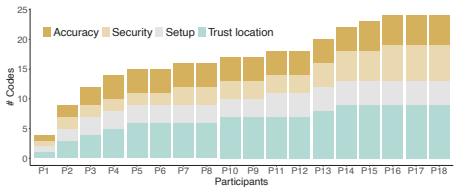


Figure 1: Code saturation results. "Accuracy" indicates unlock accuracy expectations; "Security" indicates security expectations; "Setup" indicates setup time; and "Trust location" indicates trust location considerations.

3.2.2 Trusted Location Considerations

The first question we asked was *"What physical locations or places would you register as trusted locations and allow your phone to be unlocked automatically? Explain why."* Table 1 shows different types of physical locations that the participants consider as trusted, and provides the number of times each location was mentioned. 6 out of 18 participants mentioned three different locations, 9 participants mentioned two different locations, and 3 participants mentioned one location. Unsurprisingly, "home" was the most frequently mentioned trusted location, followed by "office," and "my room."

As for the reasons for selecting trusted locations, we identified 7 different codes. Note that some participants provided multiple reasons. The most frequently cited reasons were `private space` and `frequently visited place`, each of which was mentioned by 7 participants. P1 mentioned "my room" and the privacy it offers:

Table 1: Types of trusted locations, and counts for each location type. Rows "One," "Two," and "Three" refer to the number of locations that each participant mentioned as trusted locations; for instance, row "Three (6)" indicates there were six participants who each mentioned three different locations.

# Locations (# Participants)	One (3)	Two (9)	Three (6)	**Total (18)**
Home	3	8	5	**16**
Office	0	7	3	**10**
My room	0	1	4	**5**
Office desk	0	1	1	**2**
Lecture room	0	0	2	**2**
Church	0	1	0	**1**
Bathroom	0	0	1	**1**
Cafe	0	0	1	**1**
Gym	0	0	1	**1**
Total	**3**	**18**	**18**	**39**

> *"My room... It's completely my own space. Even if I'm at home, there are things that I do not want to share with my family.."* (P1)

Another frequently cited reason was `spend a lot of time`, which was mentioned by 3 participants. P12 mentioned "home," because he spends most of the time at "home", and would like the phone to remain unlocked while he is at "home." P16 specifically mentioned that she registered "church" because she believes it is a `trustworthy place`.

3.2.3 Trusted Location Sizes

The participants were asked *"If you were able to specify a radius of a circle to indicate the size of a trusted location you mentioned earlier, what would be a radius size that you prefer? Answer in meters."* This question was designed to gauge users' preferences with respect to specifying trusted location coverage sizes.

Table 2: Numbers of preferred trusted location coverage sizes in meters for each location type.

Location	1–3m	4–6m	7–9m	10–12m	13–15m
Home	2	2	4	8	0
Office	1	6	2	1	0
My room	3	2	0	0	0
Office desk	2	0	0	0	0
Lecture room	0	0	0	1	1
Church	0	0	0	0	1
Bathroom	1	0	0	0	0
Cafe	0	0	0	0	1
Gym	0	0	0	0	1
Total	**9**	**10**	**6**	**10**	**4**

Table 2 shows the coverage sizes that users preferred for each location type. Smaller sizes, less than 6 meters, were mostly preferred for individual rooms and offices. P6 said he would like the phone to remain unlocked only when he is working at the desk. Larger sizes, larger than 7 meters, were preferred for homes. P3 mentioned that she trusts the entire space of her home and does not mind the phone being unlocked in her home. As for all the public (freely accessible) locations that were mentioned (lecture room, church, cafe, and gym), the participants preferred larger sizes – this observation raises potential security concerns. These observations indicate that location-based authentication services should allow users to select different location sizes.

3.2.4 Setup Time

To gauge what range of setup times users are willing to tolerate when registering trusted locations, we asked *"What do you consider to be an adequate time taken to register one trusted location (answer in seconds or minutes)?"* The average setup time the participants were willing to tolerate was 3.2 minutes ($\sigma = 2.5$). 7 participants emphasized that setup times need to be short. One response was:

> *"About one minute. If the setup time is too long I will not use it."* (P6)

Two participants mentioned that the setup times should be similar to that of setting up other unlock options like patterns or PINs. Here is a quote from P14:

> *"I don't want to use up more time than what I would normally spend setting up a pattern."* (P14)

3.2.5 Unlock Accuracy Expectations

To understand users' location detection accuracy expectations, we asked *"A location-based authentication error occurs when it fails to unlock your phone when you physically move to a registered trusted location. How many failures out of 10 attempts are you willing to tolerate before stopping the use of a location-based authentication service?"* 2 out of 18 participants mentioned they would not tolerate any unlock failure. 6 participants said they would tolerate just one failure. P9 mentioned:

> *"..it's impossible to have zero failure.. one [out of ten] failure would not be that inconvenient.."* (P9)

4 participants mentioned that they would tolerate two failures. 2 participants were willing to tolerate three failures. 4 participants said they would tolerate five or six failures. P14 was willing to tolerate 5 failures:

> *"..five.. current unlock methods also frequently fail anyway.."* (P14)

Overall, we observed a wide range of failure tolerance levels among the participants, ranging between 0 to 6 (out of 10 unlock attempts) failures. However, the majority of the participants expected one or two failures.

3.2.6 Security Expectations

Similarly, to understand the participants' security expectations, we asked *"A location-based authentication security failure occurs when it fails to lock your phone after physically walking away from registered trusted locations. How many security failures out of 10 attempts are you willing to tolerate before stopping the use of a location-based authentication service?"* The participants were more strict with security: 6 out of 18 participants mentioned that they would not tolerate any security failure. P17 mentioned:

> *"Because this technology is about automatically unlocking my phone, it needs to guarantee high [location detection] accuracy.."* (P17)

9 participants said they would tolerate one or two security failures. However, there were more participants (compared to those who were unwilling to tolerate any unlock failure) who expected no security failure.

3.2.7 Battery Use

To understand what level of battery use the participants are willing to tolerate, we asked *"How much battery use are you willing to tolerate before stopping the use of a location-based authentication service?"* The distribution of responses indicates that tolerable battery usage percentage per day mainly ranged from 5 to 15%. (see Appendix B).

3.3 Requirements

Based on the above observations, we summarize key design requirements that must be considered upon designing a usable and secure location-based authentication service:

1. **Indoor locations.** Many participants expressed their preferences to register indoor locations such as rooms and offices as trusted locations – the first requirement is that a service should allow users to register indoor locations as trusted locations.

2. **Multiple locations.** Except for one participant, everyone expressed the preference to register two or more trusted locations. The second requirement is that a service should allow users to register more than one trusted location.

3. **Adjustable location sizes.** The participants expressed different location coverage preferences. The third requirement is that a service should allow users to choose different location coverage sizes and adjust them individually.

4. **Setup time.** Based on responses about tolerable setup times, the fourth requirement is that users should be able to register a single location within 3.2 minutes.

5. **False rejection rates and false acceptance rates.** The majority of the participants said they were willing to tolerate one or two security/lock failures for every ten lock attempts (phones remaining unlocked when users move away from trusted locations). This error rate is referred to as false acceptance rates (FARs). Similarly, most were willing to tolerate one or two usability/unlock failures for every 10 unlock attempts (phones remaining locked when users try to use them inside trusted locations). The error rate is referred to as false rejection rates (FRRs). Such tolerable lock or unlock failure levels need to be satisfied at the minimum.

6. **Battery use.** The participants were willing to tolerate between 5 to 15% use of battery during daytime for running a location-based authentication service.

3.4 Limitations

In the requirement study, a small number of participants may not be sufficient to enumerate all possible codes to understand the requirements for location-based authentication. To address this issue, we tested whether code saturation was reached with two separate coders.

Moreover, the participants could have possibly misunderstood some of the questions/terms because all participants except one participant who has used Smart Lock did not use any location-based authentication scheme before the study. For example, the term of trusted location can be differently interpreted by each participant. To keep the chances of such misunderstanding low and ensure consistency, we had two researchers interviewing together in the requirement study and conducted a pilot study before the requirement study to resolve the ambiguity and misconceptions surrounding the terms and questions.

Since our studies were designed to use self-reported data, our results inherently depend on the participants' honesty and knowledge. We mitigated this limitation by conducting the field study with a fully working Android application that supports location-based authentication.

4 Field Study Application Design

As the next step, we implemented a fully functional location-based authentication application that follows the phone lock/unlock paradigms introduced through Smart Lock yet also contains new features that we identified as important through the first study. We used this application to conduct a field study and analyze users' real-world usage behaviors.

4.1 Design Overview

We named our location-based smartphone authentication application "Loclock". Because the GPS technology alone is not sufficient to support the first "indoor locations" requirement,

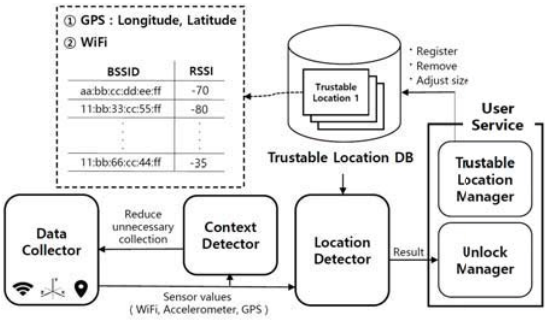


Figure 2: Overview of Loclock.

we also used WiFi information – more specifically, signal strengths of nearby access points – to create fingerprints for indoor locations. To satisfy the "adjustable location sizes" requirement, we designed Loclock to support three different location coverage sizes. Since we cannot guarantee meter-level location detection accuracy, we provide three coverage options that users can choose from: 0 to 5 meters, 5 to 10 meters, and 10 or more meters. Figure 2 shows the architectural overview of Loclock.

Data Collector. To satisfy the "battery use" requirement, we tried to minimize the number of sensors used for collecting data. We collect accelerometer sensor data, GPS data, and the WiFi "received signal strength indication" (RSSI) values from nearby access points. GPS data are used for large area (usually outdoor) detection, and WiFi RSSI values are used for more fine-grained indoor area detection. Accelerometer data are used for context detection.

Context Detector. The accelerometer data are used to detect when a phone is sitting idle on a specific place (e.g., desk). We use this contextual information to determine when to stop or start collecting WiFi RSSI values because continuous and frequent WiFi RSSI collection would use up too much battery. For instance, when a user leaves her phone on her desk, there is no need to collect WiFi RSSI values frequently while the phone is sitting idle on the desk. We measured battery consumption levels in a lab setting for intensive and less intensive battery use scenarios. The intensive battery use scenario collected all sensor data and WiFi signals, but the less intensive scenario collected sensor data only. Our evaluation results showed that the first scenario consumed about 9 percent per hour, while the less intensive scenario consumed about 3 percent per hour.

Location Detector. This component detects whether a phone is inside a registered location coverage area. As the first step, GPS information is used to determine whether a registered location is inside a large coverage area. To avoid unnecessary battery drain, in the case when the phone is inside the large coverage area, it collects WiFi RSSI values from the nearby access points of the current location and compares them against pre-stored (upon trusted location registration) RSSI values. WiFi RSSI values could be sensitive and differently measured under various environmental conditions. When a user stores the RSSI values for a trusted location during the trusted location registration process, we found that one minute is reasonable to collect a sufficient number of RSSI values while satisfying the "setup time" requirement. Loclock uses the average value for each access point to avoid the bias by some outlier RSSI values. The lower Euclidean distance between current WiFi RSSI values and pre-stored RSSI values (upon trusted location registration), the closer the current location is to a registered trusted location. We set a distance threshold to determine whether the phone is inside a trusted location coverage area: if a distance value is lower than the threshold – this indicates that a given location is a trusted location – the phone will be unlocked. We empirically determined the optimal threshold.

User Service. This component allows users to configure PIN, pattern, or password as a screen unlock scheme. Users must set up at least one scheme before using Loclock. Such schemes are used to unlock phones when users are not inside trusted location coverage areas, or when Loclock fails to unlock phones inside trusted locations. This component also provides the user interface for users to register, modify, or delete trusted locations.

4.2 Lock/Unlock Failure Rate Evaluation

To demonstrate that Loclock can achieve tolerable failure rates as described in the "FRR and FAR" requirement, we collected WiFi RSSI datasets from three different locations (two office buildings and one university laboratory) using Loclock and evaluated the lock and unlock failure rates with varying threshold values. We provide a summary of the evaluation results in Appendix C.

For each of the two coverage sizes, 5 and 10 meters, we measured three sets for FRR and FAR, fixing FRRs to 10, 20, and 30% – this would give us three specific RSSI threshold values that guarantee those three FRR rates – and measuring three FARs based on the three threshold values. At both FRR 10 and 20% threshold values, the FARs were contained around 20%. The half total error rates (HTER), computed by averaging FARs and FRRs, are all below 20% when FRRs are fixed at 10 and 20%. Referring back to the "FRR and FAR" requirement (willing to tolerate one or two out of 10 failures), these FRR/FAR results indicate the field study participants would likely experience tolerable error rates.

5 Field Study

We designed the second field study based on the observations from the requirement study. The majority of the participants hypothetically selected at least two different trusted locations, mentioning various indoor location types ranging from homes to public places like cafes or gyms. Through the field study,

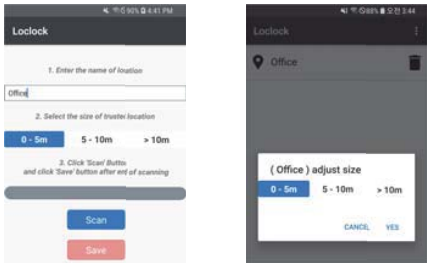
we wanted to investigate what type of trusted locations are registered in the real world, and gauge how useful the application is in reducing users' manual phone unlock burden.

Some of the public locations mentioned by the participants like cafes or gyms seem to be insecure with respect to preventing unauthorized phone access. It was our objective to analyze security implications of allowing users to freely register unlimited number of trusted locations, and select different location coverage sizes. By implementing an application based on the identified requirements (see Section 3.3), we also wanted to validate the relevance of those requirements. The ethical perspective of the field study was validated through an IRB at a university.

5.1 Methodology

We recruited 30 participants who are aged 18 years or older, and own a phone with Android 8.0 or below[1]. However, one participant dropped out on the second day of the study. Therefore, we performed our analyses on the 29 participants who completed the study. We posted advertisements for recruitment on online notice boards at a university and selectively invited people from local communities based on their age and work experiences to ensure that the overall demographic proportions are similar to those presented in [2]. To achieve strong ecological validity, we asked the participants to install our Loclock Android application (described in Section 4) on their own phone, and use it for 3 weeks. The participants were compensated for their time with a USD 200 gift card. All user interactions with Loclock (e.g., registering trusted locations, location size adjustments), WiFi data, GPS data, phone lock, and unlock events were logged. To comply with the ethical expectations of IRB, we collected all the data, removed their personally identifiable information, and stored them in an encrypted database. Moreover, only the three researchers who were approved by the IRB committee had access to the data.

Before starting the study, the participants were informed about the purposes of the study, provided with instructions, and asked to sign a consent form. They were also informed that participation is voluntary and confidential, and they can terminate the study without penalty. We asked them to submit their demographics information and install Loclock on their phones. We explained that their phones would be automatically unlocked when they move to registered trusted locations. We asked participants to turn off their current lock options for the study and switch to using the lock options provided by Loclock during the 3-week study period. We informed the participants that the only change in phone security configuration is that biometric lock mechanisms will not be available and that PIN/patterns/passwords can be used the same way. We then explained how trusted locations could be registered, removed, and modified (size changes). To ensure that the participants fully understood how Loclock works, we thoroughly explained all the features available and asked them to explain those features again. We also explained how an explicit unlock method, PIN, pattern, or password, can be registered on Loclock[2]. Loclock automatically locks a user's phone when the user carries it far away from a registered trusted location; the user should then use an explicit unlock method to unlock the phone. The setup screen of Loclock is illustrated in Figure 3. Users can freely remove or adjust the size of a registered trusted location.



(a) Location registration (b) Size adjustment

Figure 3: Loclock setup screen.

Participants were instructed to register and remove trusted locations freely, and select and adjust trusted location sizes based on their needs. However, since the field study is about analyzing the participants' behaviors with respect to using location-based authentication, we asked the participants to register at least one trusted location at the beginning of the study and use it at least until the 10th day (half of the study duration) – the intention was to collect sufficient data for meaningful analysis. We explained that they could freely remove registered locations after the 10th day if they wanted to. After the 10th day, we sent out a reminder email, informing the participants that they could freely remove any of the registered locations and discontinue using Loclock. To ensure compliance, we disabled the "remove" button until the 10th day. However, to handle cases where the participants accidentally register unwanted locations, we enabled the remove button just for an hour after initial location registration and disabled it after an hour.

Finally, a closure email was sent after 3 weeks, notifying the participants to revisit and participate in a short post-interview. We first asked the participants to explain their reasons for registering trusted locations, removing registered trusted locations, and selecting location sizes. For each of the registered trusted locations, we then asked the following scenario-based question to help categorize whether a selected location is secure from unauthorized access: *"Think about who could access your phone if it was left unattended for 10 minutes in that registered location. Is there someone who*

[1]The WiFi scanning API was depreciated from Android 9.0.

[2]Loclock does not support biometric-based unlock options like fingerprints or face detection.

should not have access?" If a participant said there are individuals who should not have access, we classified it as an "insecure" place; otherwise, we classified it as a "secure" place. We then asked the participants how they feel about the ease and time taken to register trusted locations. We also asked their feelings about the overall security and usability of using Loclock to unlock their phones. A five-level Likert scale was used to answer those questions. We helped them to uninstall Loclock. At the end of the interview, we asked "*Do you want to continue using location-based authentication after the study?*"

Before conducting the field study, we performed several rounds of pilot studies with three people to fix bugs and address unclear instructions and descriptions.

5.2 Results

5.2.1 Demographics

15 out of 29 participants were female. The participants' average age was 39.4 years (σ = 12.6). 12 participants graduated high school, 7 participants had a university degree, and 6 participants had a master (or doctoral) degree. 14 different occupations were reported with "student," "secretary," and "teacher" being the top ones. To demonstrate the representativeness of our demographics, we compared the distribution of age, gender, and education information with the US smartphone population reported in [2]. The Fisher's exact tests did not show significant differences in age ($p = 0.97$), gender ($p = 0.85$), and education ($p = 0.28$). We note that the field study participants were entirely disjunct from the requirement study participants. The details of demographics are in Appendix D.

5.2.2 Registered Trusted Locations

To satisfy the field study objectives described above, we analyzed all trusted locations registered by participants during the entire 3 weeks. Table 3 shows the trusted locations that remained at the end of the study. Participants initially registered 43 locations on the first day and additionally registered 30 locations (see Table 4). However, the total number of registered locations finally decreased from 73 to 65 because 8 trusted locations were removed after the 10th day.

As shown in Table 3, 21 participants (72%) registered two or more locations as trusted locations. Among all participants, "home" was the most frequently registered trusted location; the second most frequently registered location was "office," and the third was "my room." These results are consistent with the findings from the interview study (see Table 1). Since "my room," "living room," "bathroom," and "kitchen" are also part of "home", "home" seems to be the most representative trusted place for location-based authentication.

Interestingly, 6 participants registered "church" as a trusted location. Although the numbers were small, some participants also registered other public locations such as "sports facility," "cafe," "library," "hospital," and "subway station entrance." These observations are also consistent with the first study results (see Table 1).

Table 3: Trusted locations remaining at the end of the study, and counts for each location type.

# Locations (# Participants)	Zero (1)	One (7)	Two (13)	Three (3)	Four (3)	Five (1)	Six (1)	**Total (29)**
Home	0	0	10	2	2	1	0	**15**
Office	0	3	5	2	2	1	0	**13**
My room	0	3	4	1	1	0	0	**9**
Church	0	0	4	2	0	0	0	**6**
Sports facility	0	0	1	1	1	2	1	**6**
Living room	0	1	2	1	1	0	0	**5**
Lecture room	0	0	0	0	1	0	2	**3**
Bathroom	0	0	0	0	2	0	0	**2**
Cafe	0	0	0	0	0	1	1	**2**
Hospital	0	0	0	0	1	0	0	**1**
Kitchen	0	0	0	0	1	0	0	**1**
Library	0	0	0	0	0	0	1	**1**
Subway station entrance	0	0	0	0	0	0	1	**1**
Total	**0**	**7**	**26**	**9**	**12**	**5**	**6**	**65**

Table 4: Numbers of trusted locations registered each day of the field study.

Day	1st	2nd	3rd	4th	5th onwards	**Total since 2nd**
Home	11	4	0	1	1	**6**
Office	8	1	3	1	0	**5**
My room	6	2	0	0	1	**3**
Church	5	1	0	1	1	**3**
Sports facility	1	3	0	1	1	**5**
Living room	7	0	0	0	0	**0**
Lecture room	1	1	1	0	0	**2**
Bathroom	0	0	0	1	1	**2**
Cafe	0	0	0	1	1	**2**
Hospital	1	0	0	0	0	**0**
Kitchen	1	1	0	0	0	**1**
Library	1	0	0	0	1	**1**
Subway station entrance	1	0	0	0	0	**0**
Total	**43**	**13**	**4**	**6**	**7**	**30**

Table 5 shows the number of trusted locations that were removed after the 10th day by each location type. Eight location types, "office," "my room," "sports facility," "lecture room," "cafe," "bathroom," "subway station entrance," and "hospital" were never removed. A common characteristic between the location types that were removed – "home," "living room," "church," "library," and "kitchen" – is that they were places that could be occupied and used by other people as well. One participant (P20) initially registered two locations but removed both of them after the 10th day. When we asked why, P20 said it was simply due to curiosity. P5 initially registered four trusted locations but removed three locations. P5 said that she registered "church" because there was just one occasion where she had to stay for an entire day, and removed it after that day. P5 also explained that she removed "living room" because "my room" was registered to cover more than 10 meters, and "my room" alone was already covering the living room area as well.

Table 5: Columns "One," "Two," and "Three" refer to the number of trusted locations that were removed after the 10th day; for example, row "Two (1)" indicates there was one participant who removed two trusted locations.

# Locations (# Participants)	One (3)	Two (1)	Three (1)	**Total (5)**
Home	0	1	1	**2**
Office	0	0	0	**0**
My room	0	0	0	**0**
Church	0	1	1	**2**
Sports facility	0	0	0	**0**
Living room	1	0	1	**2**
Lecture room	0	0	0	**0**
Bathroom	0	0	0	**0**
Cafe	0	0	0	**0**
Hospital	0	0	0	**0**
Kitchen	1	0	0	**1**
Library	1	0	0	**1**
Subway station entrance	0	0	0	**0**
Total	**3**	**2**	**3**	**8**

5.2.3 Trusted Location Sizes

Next, we analyzed the sizes of trusted locations that remained at the end of the study. Table 6 shows the number of registered sizes for each location type. "5–10m" (54%) was the most frequently selected location size, followed by "> 10m" (45%). Only one instance of "my room" was registered with a size smaller than 5 meters. Even for "my room," "5–10m" (78%) was the most preferred size. These observations indicate that regardless of location types, the participants' preferred sizes are greatly divided into "5–10m" and "> 10m."

Table 6: Numbers of remaining trusted location sizes for each location type, counted at the end of the study.

Location	0–5m	5–10m	> 10m
Home	0	6	9
Office	0	6	7
My room	1	7	1
Church	0	2	4
Sports facility	0	4	2
Living room	0	5	0
Lecture room	0	0	3
Bathroom	0	1	1
Cafe	0	2	0
Hospital	0	1	0
Kitchen	0	1	0
Library	0	0	1
Subway station entrance	0	0	1
Total	**1 (2%)**	**35 (54%)**	**29 (45%)**

Worryingly, a large portion of public locations was registered with sizes larger than 10 meters (11 out of 20 public locations), which does raise security concerns about some users' size preferences. For instance, 4 out of 6 "church" locations were registered to be larger than 10 meters in size. P8 added "subway station entrance" with the largest coverage area, explaining that he always checked the subway arrival time before entering the station and wanted the phone to be unlocked automatically at that moment. About 42% of the reasons behind size selection was a general one: "to choose a location size that sufficiently covers my daily phone usage trails." No participant mentioned security as a reason for choosing a certain location size.

5.2.4 Adjusting Trusted Location Sizes

9 participants made one attempt to change the trusted location coverage meters. Interestingly, 8 of those 9 size adjustments involved increasing the coverage meters; just one adjustment led to a decrease in coverage meter from "> 10m" to "5-10m." Figure 4 visually demonstrates size adjustments. Blue arrows show adjustments leading to size increases, and red arrows show adjustments leading to size decreases.

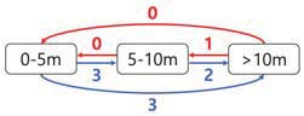
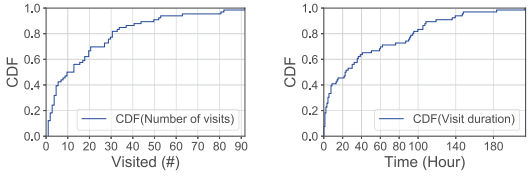


Figure 4: Size adjustments of trusted locations.

Seven participants explained that they changed location coverage size because previously chosen size was small, and did not fully cover selected locations. Two participants said that they changed location sizes just out of curiosity.

5.2.5 Visit Frequency and Duration

To examine the characteristics of trusted locations, we analyzed the number of times each trusted location was visited during the 3 weeks across all the participants, then computed cumulative distribution function (CDF) based on the number of visits for all registered trusted locations (see Figure 5(a)).

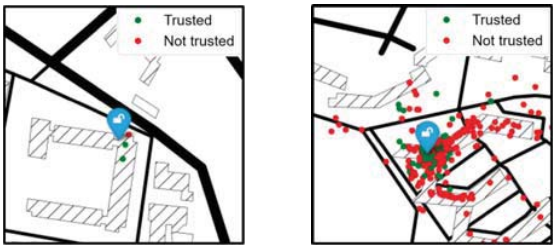


(a) Number of visits (b) Visit duration (hours)

Figure 5: CDFs computed on the total number of visits and visit duration for all registered trusted locations.

Figure 5(a) shows a significant proportion of the trusted locations were infrequently visited: over 40% of the locations were visited just 10 times or less during the 3 weeks.

We also computed CDF for the total visit duration in hours during the 3 weeks across all registered trusted locations (see Figure 5(b)). Again, it is evident that a significant proportion of the registered locations were locations where the participants did not spend much time. The participants spent 20 or fewer hours in about 45% of the registered trusted locations. These two observations indicate that some users would register places where they do not visit frequently or places where they do not necessarily spend much time.



(a) P15 (b) P2

Figure 6: Partial map view (250 by 250 meters) of where the phone was used.

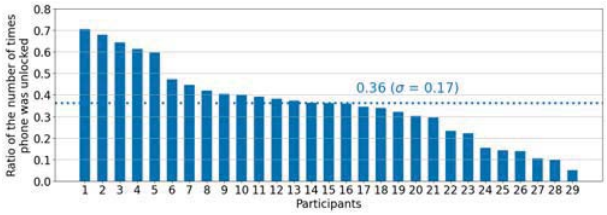


Figure 7: Distribution of the ratios in which phones were unlocked automatically through Loclock.

5.2.6 Number of Unlock Attempts

We logged the GPS and WiFi data for all locations where the participants' phone screens were turned on. We assumed that turning on the phone screen implies the intention to use it. Under this assumption, to measure the reduction of explicit unlock attempts, we counted the number of times a phone screen was turned on while the phone was unlocked by Loclock. On average, the participants tried to use their phones 44.9 times a day. This number is similar to the daily phone unlock attempts (39.9) reported in reported in [11].

Based on our assumption we counted the occurrences of `ACTION_SCREEN_ON`, which checks whether phone screens are turned on or activated. Considering that the actual number of unlocking attempts may be lower than the number of screen activation – 47.8 vs. 83.3 per day as demonstrated by [12] – the number of unlock attempts that we present may have been overestimated.

Figure 6 visualizes some locations where P2 and P15 unlocked their phones – green dots represent places where Loclock automatically unlocked phones as trusted locations, and red dots represent places where Loclock did not unlock phones. The blue unlock image represents where trusted locations were registered. Shading patterns indicate the inside of buildings. Figure 6(a) is a partial view of P15's use of the phone, showing that he or she hardly used the phone near the registered trusted location. In contrast, Figure 6(b) shows that P2 used the phone frequently near the registered trusted location. While P2 was using the phone in this area, Loclock would have automatically unlocked his or her phone many times.

Figure 7 shows the ratios of phones being unlocked automatically. The x-axis represents the participants, and the y-axis represents the ratio of the number of times a participant's phone was unlocked automatically with Loclock to the total number of unlock attempts. On average, Loclock reduced manual unlock attempts by 36% (σ=17%) – this is shown as the dashed line in Figure 7. About 25% reduction occurred from homes, and 8% occurred from offices. 20 out of 29 participants benefited from reducing more than 30% of manual unlock attempts. The largest reduction (first participant) in manual unlock attempts was 71%: from that 71%, 49.8% auto-unlock occurred from "home," and 20.5% occurred from "my room." The smallest reduction (last participant) was just 5%: this participant did not register home or office as trusted locations.

5.2.7 Security of Registered Locations

Based on the unauthorized access scenario question and responses (see Section 5.1), we labeled a given registered location as "insecure" if a participant said her phone can be accessed by unwanted individuals (who should not have access); otherwise, we labeled it as "secure." Surprisingly, based on this labeling method, 52 out of 65 registered locations were considered insecure. Table 7 shows the number of secure and insecure locations. All public places (e.g., library or sports facility) were considered "insecure" except for one instance of church registration. Interestingly, 12 "home" were considered "insecure"; four "my room," two "living room," and two "bathroom" were also considered insecure, indicating that insider threats [8, 21] may exist. Even after learning that those 52 locations are exposed to potential unauthorized access, the participants wanted to continue using 45 of them to automatically unlock phones mainly due to "phone unlock convenience" (31) or "low (perceived) likelihood of phones being attacked" (14). As for the 13 locations considered secure, 11 of them were "home" related locations.

Table 7: Counts for secure and insecure locations.

# Locations	Secure	Insecure	**Total**
Home	3	12	**15**
Office	1	12	**13**
My room	5	4	**9**
Church	1	5	**6**
Sports facility	0	6	**6**
Living room	3	2	**5**
Lecture room	0	3	**3**
Bathroom	0	2	**2**
Cafe	0	2	**2**
Hospital	0	1	**1**
Kitchen	0	1	**1**
Library	0	1	**1**
Subway station entrance	0	1	**1**
Total	**13**	**52**	**65**

As for the location coverage sizes, regardless of whether locations are considered secure or insecure, the participants

preferred selecting sizes larger than 5 meters in radius ($p = 1.00$, Fisher's exact test). These results are summarized in Table 8.

Table 8: Secure and insecure locations and coverage sizes.

Location	0–5m	5–10m	> 10m	**Total**
Secure	2	6	5	**13**
Insecure	8	23	21	**52**

5.2.8 Post Study Survey Results

Location registration difficulty. As part of the post study survey, we asked the participants about their feelings toward the easiness of registering a trusted location. The participants' responses are summarized in Figure 8. About 86% felt that it was easy to register trusted locations, and there was no participant who felt it was difficult.

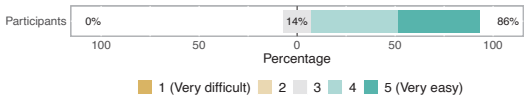


Figure 8: Easiness of registering trusted locations.

Time taken to register trusted locations. We also asked how the participants felt about the time it took for them to register trusted locations. Note, the time taken to collect and store WiFi RSSI values is one minute. Their responses are summarized in Figure 9. About 48% of the participants felt that the time taken to register trusted locations was fast. 21% felt that it was slow.

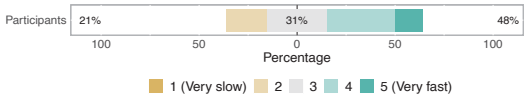


Figure 9: Fastness of registering trusted locations.

Security of Loclock. We asked how the participants felt about the security offered by location-based authentication; their responses are summarized in Figure 10. About 62% of the participants felt that using Loclock was secure; only 7% felt that it was insecure. The low reported FARs (1% on average) are one explanation as to why the participants may have felt that Loclock was secure to use.

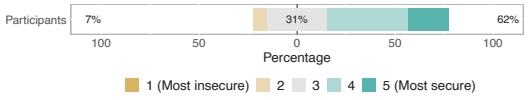


Figure 10: Security of using Loclock.

Convenience of Loclock. We also asked how the participants feel about the convenience associated using Loclock to automatically unlock their phones. Their responses are summarized in Figure 11. About 59% of the participants felt that Loclock was convenient to use. The common reason was because of its automatic unlock capabilities. P15 mentioned that he wants to continue using Loclock even after the study. 10 participants felt that it was inconvenient. 7 of those 10 had to deal with unintended termination of Loclock due to insufficient memory or communication errors at some point during the study, and mentioned this as the main reason. Two participants mentioned "no support for fingerprint scanner." Only one participant mentioned battery drain as the reason.

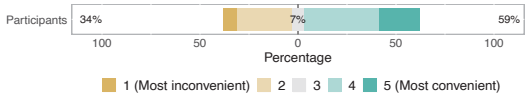


Figure 11: Convenience of using Loclock.

Intentions for future use. Finally, the participants were asked whether they would continue to use Loclock. 22 out of 28 participants said "yes," indicating "phone unlock convenience" as the main reason. As for the 6 participants who said "no," the main reason for not willing to use it in the future was "concerns about information leakage."

5.3 Limitations

We made it mandatory to register at least one trusted location and use it for the first 10 days. Also, Loclock does not support biometric-based authentication options. These constraints may have affected the ecological validity of the field study. To study the effects of having previous biometric authentication experience, we divided the field study participants into two groups: 16 participants who were using at least one biometric scheme prior to the study and 12 participants who were not using any. We analyzed the statistical differences between the two groups. As for the number of registered locations, we did not find any significant difference between them ($p = 0.82$, Mann-Whitney U test). However, as for the location coverage sizes, we did find a significant difference between the two ($p < 0.001$, Fisher's exact test). One possible explanation is that those who were previously using biometric schemes tried to minimize the burden of using passwords (for the study) by selecting large location coverage areas.

Loclock was not optimized for location detection accuracy and battery use. Also, its GUI was not optimized for usability. All of these limitations may have affected the way the participants felt about the overall security and usability of Loclock.

As explained above, while measuring the benefits of reducing the number of explicit unlock attempts we counted the number of times phone screen was activated – we could have overestimated the manual unlock benefits due to this limitation.

6 Discussions

6.1 Security Concerns

The results from the interviews and field studies raise two important security concerns: (1) people tend to add a variety of insecure locations (52 out of 65 registered locations were considered insecure by our definition) and are willing to continue to use them even after becoming aware of potential unauthorized phone access threats, and (2) a significant proportion of such insecure locations are added with the largest coverage areas (larger than 10 meters). Moreover, some participants added locations where they spend a small amount of time as trusted locations – many of them being public places exposed to phone theft. All of those observations indicate that location-based authentication schemes could expose new security threats that adversaries may exploit. For instance, if an adversary has some information about a victim's location history, the adversary could try to steal the victim's phone, go near a pre-registered trusted location, and access the phone contents without having to guess PIN or pattern. An insider could try to access phone contents when the victim leaves the phone unattended inside a registered trusted location. Such threats could compromise the entire phone security and need to be mitigated carefully.

To mitigate them, location-based authentication systems need to be designed to help users adequately understand the security risks associated with adding certain locations or choosing large sizes. For instance, we could ask a similar phone access scenario question (see Section 5.1) while adding a new location, and help users become aware of any unwanted access that might occur. Current Smart Lock implementation provides a simple guide for users to add their homes as trusted locations ("Keep device unlocked at Home") without informing users about the possibility of insider threats. Again, security risks related to insider threats need to be conveyed before offering recommendations to add homes.

However, such mitigation strategies might not be sufficient (as observed from Section 5.2.7) if users still select and use insecure locations, thinking that threat likelihood is low or focusing merely on the usability benefits. Therefore, we believe more protective measures need to be deployed with a location-based authentication scheme: for instance, one could design it so that phones must first be unlocked with an explicit unlock scheme – it would then stay unlocked within a detected trusted location. Since most usability benefits came from homes and offices, another security measure could disallow the registration of any other location. Infrequently visited locations could be deleted automatically after notifying users.

6.2 Usability

Our field study results show that the participants were willing to continue to use Loclock. As described in Section 5.1, after the 10th day, we informed the participants that they could freely remove all registered locations and use manual unlock instead. Just one participant (out of 29) stopped using Loclock after the 10th day. Table 4 and 5 show that the number of registered locations increased from 43 to 65 during the 3-week period. Through the use of Loclock, the participants managed to reduce about 36% of manual unlock attempts (mostly used at homes or offices) – demonstrating clear usability benefits (and usefulness) of location-based authentication schemes.

As shown in Section 5.2.8, 21% of the participants felt that the trusted location registration process was slow. The current Loclock implementation required the participants to wait for a minute to collect WiFi RSSI values but the entire one minute data might not be necessary to maintain the reported accuracy. Future design should consider shortening this setup time (e.g., to 30 seconds) while trying to maintain similar level of detection accuracy.

One participant mentioned the battery drain issue and said Loclock was inconvenient to use because of its heavy battery usage. Although the background logging services contributed to more battery being used, overall, its battery use was far greater than the tolerable levels mentioned in the requirements. Since continuous WiFi sensing is a battery-intensive operation, future work should look at other possible indicators that would help identify a physical location and use less battery; e.g., detecting the presence of known (previously paired) Bluetooth devices.

Even though the reported FARs and FRRs were small, we imagine that real-world error rates may be higher. A recent study [23] demonstrates that it is important to provide a well-designed user-in-the-loop user experience so that users can manually deal with inaccuracies. Following their design guidelines, we may give users the ability to adjust the threshold based on their preferences to reduce error rates.

7 Conclusion

Through interviews and a field study, we identified essential requirements for building usable and secure location-based authentication services: users prefer to register fine-grained indoor locations and adjust location coverage sizes. Using a location-based authentication application, the participants, on average, were able to reduce 36% of explicit authentication attempts, demonstrating clear usability benefits. Most of the participants continued using the automatic unlock feature despite being informed that they could stop using it and return to manual unlocks. However, the field study findings also revealed that people tend to register insecure locations due to convenience or perceived low likelihood of phones being attacked in those locations. Even after being informed about potential phone access threats, most of the participants said they would continue using insecure locations. Such risks would probably exist in commercialized services like Smart Lock, and need to be mitigated.

Acknowledgments

This work was supported by Samsung Research, NRFK (2019R1C1C1007118) and IITP (2019-0-01343). The authors would like to thank all the anonymous reviewers. Note that Hyoungshick Kim is the corresponding author.

References

[1] Choose when your Android device can stay unlocked. https://support.google.com/android/answer/9075927?hl=en.

[2] Mobile Technology and Home Broadband 2019. https://www.pewresearch.org/internet/2019/06/13/mobile-technology-and-home-broadband-2019/.

[3] M. Abbas, M. Elhamshary, H. Rizk, M. Torki, and M. Youssef. WiDeep: WiFi-based Accurate and Robust Indoor Localization System using Deep Learning. In *Proceedings of the 17th International Conference on Pervasive Computing and Communications*, 2019.

[4] Ioannis Agadakos, Per Hallgren, Dimitrios Damopoulos, Andrei Sabelfeld, and Georgios Portokalidis. Location-Enhanced Authentication Using the IoT: Because You Cannot Be in Two Places at Once. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pages 251–264, 2016.

[5] Jiayi Chen, Urs Hengartner, Hassan Khan, and Mohammad Mannan. Chaperone: Real-time Locking and Loss Prevention for Smartphones. In *Proceedings of the 29th USENIX Security Symposium*, pages 325–342, 2020.

[6] P. Davidson and R. Piché. A Survey of Selected Indoor Positioning Methods for Smartphones. *IEEE Communications Surveys Tutorials*, 19(2):1347–1370, 2017.

[7] Dorothy E Denning and Peter F MacDoran. Location-based authentication: Grounding cyberspace for better security. *Computer Fraud & Security*, 1996(2):12–16, 1996.

[8] Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. Are You Ready to Lock? In *Proceedings of the 21st ACM SIGSAC Conference on Computer and Communications Security*, page 750–761, 2014.

[9] Joseph L Fleiss, Bruce Levin, and Myunghee Cho Paik. *Statistical methods for rates and proportions*. John Wiley & Sons, 2013.

[10] L. Fridman, S. Weber, R. Greenstadt, and M. Kam. Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location. *IEEE Systems Journal*, 11(2):513–521, 2017.

[11] Marian Harbach, Alexander De Luca, and Serge Egelman. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proceedings of the 34th Conference on Human Factors in Computing Systems*, pages 4806–4817, 2016.

[12] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. It's a Hard Lock Life: A Field Study of Smartphone (Un) Locking Behavior and Risk Perception. In *Proceedings of the 10th Symposium On Usable Privacy and Security*, pages 213–230, 2014.

[13] Sebastian Hilsenbeck, Dmytro Bobkov, Georg Schroth, Robert Huitl, and Eckehard Steinbach. Graph-based Data Fusion of Pedometer and WiFi Measurements for Mobile Indoor Positioning. In *Proceedings of the 14th ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 147–158, 2014.

[14] Daniel Hintze, Eckhard Koch, Sebastian Scholz, and Rene Mayrhofer. Location-Based Risk Assessment for Mobile Authentication. In *Proceedings of the 7th International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, page 85–88, 2016.

[15] Fudong Li, Nathan Clarke, Maria Papadaki, and Paul Dowland. Active authentication for mobile devices utilising behaviour profiling. *International Journal of Information Security*, 13(3):229–244, 2014.

[16] Tao Li, Yimin Chen, Jingchao Sun, Xiaocong Jin, and Yanchao Zhang. ILock: Immediate and Automatic Locking of Mobile Devices against Data Theft. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, page 933–944, 2016.

[17] Kathleen Macqueen, Eleanor McLellan-Lemal, K. Bartholow, and B. Milstein. Team-based codebook development: Structure, process, and agreement. *Handbook for team-based qualitative research*, pages 119–135, 2008.

[18] Upal Mahbub and Rama Chellappa. PATH: Person authentication using trace histories. In *Proceedings of the 7th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*, pages 1–8, 2016.

[19] Claudio Marforio, Nikolaos Karapanos, Claudio Soriente, Kari Kostiainen, and Srdjan Capkun. Smartphones as Practical and Secure Location Verification Tokens for Payments. In *Proceedings of the Network and Distributed System Security Symposium*, pages 23–26, 2014.

[20] Masoud Mehrabi Koushki, Borke Obada-Obieh, Jun Ho Huh, and Konstantin Beznosov. Is Implicit Authentication on Smartphones Really Popular? On Android Users' Perception of "Smart Lock for Android". In *Proceedings of the 22nd International Conference on Human-Computer Interaction with Mobile Devices and Services*, pages 1–17, 2020.

[21] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pages 271–280, 2013.

[22] F. S. Park, C. Gangakhedkar, and P. Traynor. Leveraging Cellular Infrastructure to Improve Fraud Prevention. In *Proceedings of the 25th Annual Computer Security Applications Conference*, pages 350–359, 2009.

[23] Quentin Roy, Futian Zhang, and Daniel Vogel. Automation Accuracy Is Good, but High Controllability May Be Better. In *Proceedings of the 37th ACM Conference on Human Factors in Computing Systems*, 2019.

[24] Johnny Saldaña. *The coding manual for qualitative researchers*. Sage, 2015.

[25] Y. Shu, C. Bo, G. Shen, C. Zhao, L. Li, and F. Zhao. Magicol: Indoor Localization Using Pervasive Magnetic Field and Op-

portunistic WiFi Sensing. *IEEE Journal on Selected Areas in Communications*, 33(7):1443–1457, 2015.

[26] Feng Zhang, Aron Kondoro, and Sead Muftic. Location-Based Authentication and Authorization Using Smart Phones. In *Proceedings of the 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1285–1292, 2012.

A Demographics in the Requirement Study

Table 9 presents the demographics of the participants in the requirement study.

Table 9: The demographics of the requirement study.

Gender		
Female	10	(55.6%)
Male	8	(44.4%)
Age		
19–24	2	(11.1%)
25–34	5	(27.8%)
35–44	6	(33.3%)
45–54	2	(11.1%)
55–64	3	(16.7%)
Education		
Less than high school	0	(0.0%)
High school	3	(16.7%)
Professional School	0	(0.0%)
University (Bachelor's)	9	(50.0%)
Master of PhD	6	(33.3%)
Other	0	(0.0%)
Occupation		
Managers	3	(16.7%)
Professionals	2	(11.1%)
Clerical Support Workers	4	(22.2%)
Service and Sales Workers	3	(16.7%)
Craft and Trades Workers	1	(5.6%)
Machine Operators	1	(5.6%)
Elementary Occupations	0	(0.0%)
Students	3	(16.7%)
Self-employed	0	(0.0%)
Unemployed/Retired/Disabled	1	(5.6%)

B Tolerable battery consumption

Table 10 shows the distribution of participants' responses in the requirement study. We can see that tolerable battery usage percentage mainly ranged from 5 to 15%.

Table 10: Tolerable daily battery usage levels.

Battery usage	5–10%	10–15%	15–20%	20–25%	**Total**
Frequency	9	6	1	2	**18**

C Lock/Unlock Failure Rate Evaluation

C.1 Methodology

Using the Loclock application installed on a Samsung Galaxy S8 phone, we collected WiFi RSSI values from 3 locations. For each location, we created a grid layout with one meter spacing between two grid points, covering the entire floor space. At every grid point, we collected RSSI values for one minute. The first data collection took place at a single floor in a small office building (L1) – its size is 46 by 10 meters; the number of collected BSSIDs ranged from 100 to 120. Similarly, the second location was a single floor in another office building (L2) – its size is 55 by 20 meters; the number of collected BSSIDs ranged from 15 to 20. The last location was a university laboratory (L3) that consists of 14 computer desks – its size is 11 by 7 meters; the number of collected BSSIDs ranged from 60 to 80.

After creating meter-by-meter RSSI maps for the three locations, respectively, we physically moved to a *central* position in the grid for each location, and registered that central spot as a trusted location starting point using Loclock. WiFi RSSI values, collected for a minute, were then used to compute the pre-stored trusted location RSSI vector. Using the meter-by-meter RSSI maps and pre-stored trusted location RSSI vectors, we measured unlock failure and lock failure rates for different trusted location coverage areas.

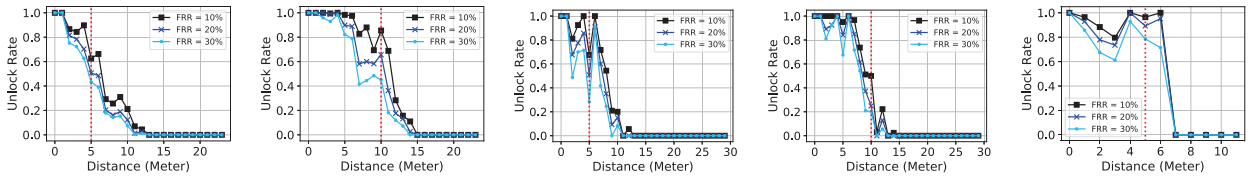
C.2 Evaluation Results

We measured lock and unlock failure rates of Loclock. Lock failure rates represent "false acceptance rates" (FAR) that measure the error rates reflecting the number of times a phone accidentally unlocks itself when a user is not inside a trusted location coverage area. This error rate is associated with the security of Loclock since the user's phone would be unlocked automatically in unknown (potentially untrusted) environments. Unlock failure rates represent "false rejection rates" (FRR), measuring the error rates for when a phone does not unlock automatically when a user has physically moved to a trusted location coverage area. This error rate would affect the usability of Loclock since users would have to unlock their phones manually.

Table 11: Lock and unlock failure rates of Loclock.

Coverage		5m			10m		
FRR		10%	20%	30%	10%	20%	30%
FAR	L1	20.0%	13.8%	11.3%	23.0%	14.9%	9.1%
	L2	13.2%	9.8%	6.4%	3.8%	1.8%	1.2%
	L3	20.9%	19.6%	16.1%	-	-	-
HTER	L1	15.0%	16.9%	20.7%	16.5%	17.5%	19.6%
	L2	11.6%	14.9%	18.2%	6.9%	10.9%	15.6%
	L3	15.5%	19.8%	23.1%	-	-	-

For the two locations (L1) and (L2), we measured FRRs and FARs for two trusted location coverage sizes: one with a circular coverage radius of 5 meters and another with a coverage radius of 10 meters. As for the third location (L3), the university laboratory, we only evaluated error rates for 5 meter radius coverage because its size is 11 by 7 meters. For each coverage area, we measured three sets for FRR and FAR, fixing FRRs to 10, 20, and 30% – this would give us three specific RSSI threshold values that guarantee those three FRR



(a) L1 (radius of 5 meters) (b) L1 (radius of 10 meters) (c) L2 (radius of 5 meters) (d) L2 (radius of 10 meters) (e) L3 (radius of 5 meters)

Figure 12: Measuring phone unlock rates with varying trusted location coverage areas (5 and 10 meters) in small office building (L1), large office building (L2) and small university laboratory (L3).

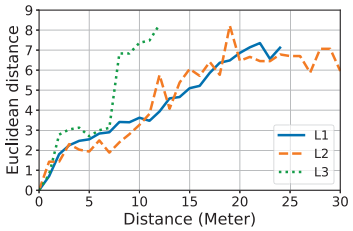


Figure 13: Changes in Euclidean distance while moving away from the originally registered spots in each of the three locations.

rates – and measuring resulting three FARs based on the three threshold values. These FRR and FAR results are summarized in Table 11. As the results show, at both FRR 10 and 20% threshold values, the FARs were contained around 20% (except for L2 that went as high as 23%). The half total error rates (HTER), computed by averaging FARs and FRRs, are all below 20% when FRRs are fixed at 10 and 20%. Referring back to the "unlock/lock failures" requirement (willing to tolerate one or two out of 10 failures), these FRR/FAR results indicate the next field study participants would likely experience reasonable and tolerable error rates. Further, Figure 12 shows the phone unlock rates in L1, L2, and L3, measuring the number of times the phone would be unlocked within the radius meters shown in the x-axis. The dotted vertical red lines show the coverage radius, 5 and 10 meters, respectively. We note that the change in WiFi RSSI values is not only determined by physical distances between access points and a user's phone; there are other factors such as physical barriers between phone and access points – the unlock rate results do not always decrease linearly based on varying distances (moving away from registered spots), and guaranteeing meter-level accuracy with just RSSI values would be infeasible. Figure 13 shows how the Euclidean distance (ED) values change with varying distances for each of the three locations. Each of the three lines in the graph represent the three different locations, and how ED changes differently based on their physical characteristics. As for L3, the sudden jump in ED is caused by walking out the laboratory door.

D Demographics in the Field Study

Table 12 presents the demographics of the participants in the field study.

Table 12: The demographics of the field study.

Gender		
Female	15	(51.7%)
Male	14	(48.3%)
Age		
19–24	4	(13.8%)
25–34	7	(24.1%)
35–44	6	(20.7%)
45–54	8	(27.6%)
55–64	4	(13.8%)
Education		
Less than high school	0	(0.0%)
High school	13	(44.8%)
Professional School	3	(10.3%)
University (Bachelor's)	7	(24.2%)
Master of PhD	6	(20.7%)
Other	0	(0.0%)
Occupation		
Managers	0	(0.0%)
Professionals	3	(10.3%)
Clerical Support Workers	8	(27.6%)
Service and Sales Workers	2	(6.9%)
Craft and Trades Workers	0	(0.0%)
Machine Operators	0	(0.0%)
Elementary Occupations	0	(0.0%)
Students	10	(34.5%)
Self-employed	2	(6.9%)
Unemployed/Retired/Disabled	4	(13.8%)
Current unlock methods		
Password	4	(8.9%)
Pattern	22	(48.9%)
PIN	2	(4.4%)
Finger	15	(33.4%)
Face	1	(2.2%)
Knock Code	1	(2.2%)