Towards Usable and Secure Location-based Smartphone Authentication

Anonymous Author(s)

ABSTRACT

The concept of using location information to implicitly unlock smartphones is widely commercialized on Android phones: once a user registers a location that she is willing to trust, her phone would unlock automatically when the user physically moves to that trusted location. To date, however, there is no prior work that studies the requirements for designing such location-based authentication services to meet users' usability and security expectations. To bridge this gap, we conducted an interview study with 18 participants to study users' perceptions of location-based smartphone authentication and identified key design requirements, such as the need to support fine-grained indoor location registration. We then conducted a field study with 29 participants to study real-world usage behaviors with a fully working application that we implemented. Our findings suggest that people often register non-private (potentially unsafe) locations as trusted locations, and select large (phone unlock) coverage areas without considering security implications. As for usability benefits, however, the participants were able to reduce about 37% of manual unlock attempts on average by using our location-based implicit authentication service.

KEYWORDS

location-based authentication, continous authentication, implicit authentication, indoor positioning

ACM Reference Format:

Anonymous Author(s). 2018. Towards Usable and Secure Location-based Smartphone Authentication. In *ACSAC '20: Annual Computer Security Applications Conference, Dec 07–11, 2020, Austin, TX*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Implicit authentication schemes for smartphones have been proposed (e.g., [4, 11, 16, 18]) as alternatives to existing screen unlock schemes (e.g., PIN, pattern, fingerprint, and face) to improve both security and usability. Implicit authentication involves performing some form of statistical tests to *automatically* distinguish a device owner from other users without requiring users' explicit actions [11]. Despite the academic trends to build accurate implicit authentication schemes, commercialization efforts have not been that successful. Google's "Smart Lock" [2], launched in 2014, is the only commercialized implicit authentication system available on smartphones. Its schemes include the use of "trusted places" to automatically unlock phones and keep them unlocked while users are using their phones within a safe location that provides some level of physical security to prevent unauthorized phone access.

Smart Lock's trusted places feature relies mainly on the use of 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) [2] – 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. 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 might be a dangerous assumption to make and put smartphone users at severe risks of phone breaches. For instance, users with low-security awareness might register non-private locations such as cafes or shopping malls. An adversary would be able to easily unlock such users' phones by just going near those locations.

In this paper, we first conducted an interview study with 18 participants to understand users' perceptions and expectations on location-based smartphone authentication. We developed a location-based screen lock application for Android and conducted a real-world field study with 29 participants based on the requirements identified through the first study. After obtaining informed consent, we asked the participants to install our application on their phones and use it for three weeks. We recorded participants' real-world usage behaviors with our application and analyzed them. Through this analysis, we identified security risks associated with freely allowing users to choose locations for unlocking phones and offer design recommendations for enhancing location selection security. Our contributions are summarized as below:

- Through the first interview study we identified security and usability requirements for building location-based authentication systems: key requirements include the need to support fine-grained indoor location registration, and allow users to select and adjust location coverage sizes.
- Based on those requirements, we implemented a lightweight indoor location-based authentication application that uses Wi-Fi signal strength measurements collected from nearby access points to detect trusted locations and evaluated its detection accuracy through Wi-Fi data collected from three different environments.
- Using this fully working application, we conducted a 3-week field study to collect real-world usage data. Our findings raise two crucial security concerns: many users register non-private places as trusted locations and choose the largest possible phone unlock coverage areas for those places without considering

ACSAC '20, Dec 07–11, 2020, Austin, TX

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

phone security implications. As for improved usability, by using the location-based automatic unlock feature, the participants, on average, were able to reduce 37% of their explicit unlock attempts.

2 REQUIREMENT STUDY

2.1 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 experiences to reduce demographic bias. 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, two researchers separately coded each interview data, and created a common codebook through iterative discussions and reaching consensus. We first applied structural coding techniques [14] [20] to identify responses to each interview question on transcripts, and 24 topic codes were identified through thematic coding. After resolving coding disagreements, we achieved an inter-coder agreement of 89% Cohen's Kappa [7].

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 (1) what we mean by trusted places: "safe locations that provide some level of physical security or protection against unauthorized phone access," and (2) the concept of using such trusted places to automatically and implicitly unlock phones. 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 (physically secure) 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 information they would like to enter upon registering a trusted location, and what would be a tolerable setup time (i.e., time taken to register one location).

Finally, we asked the participants – based on the concepts we explained in the beginning – how they feel about the security of the concept of registering trusted locations, and keeping their phones unlocked within those safe locations. 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.

2.2 Results

2.2.1 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. We performed data collection and analyses concurrently until we reached theoretical saturation – no new codes were identified with the 17th and 18th participants (see Appendix A).

2.2.2 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."

Table 1: Types of trusted locations, and counts for each location type. Columns "One," "Two," "Three," and "Four" refer to the number of locations that each participant mentioned as trusted locations; for instance, column "Four (3)" indicates there were three participants who each mentioned four 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**

As for the reasons for selecting trusted locations, we identified 8 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 6 participants. P1 mentioned "my room" and the privacy it offers:

> *"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.

2.2.3 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 (σ = 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)

2.2.4 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, and drives the definition of our second study hypothesis. These observations indicate that location-based authentication services should allow users to select different location sizes.

2.2.5 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?"* Two 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. Two participants were willing to tolerate three failures. Four participants said they would tolerate 5 or 6 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.

2.2.6 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.

2.2.7 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?"* Appenidx B shows the distribution of responses indicating that tolerable battery usage percentage mainly ranged from 5 to 15%.

2.3 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 design 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 design 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 design should allow users to choose different location coverage sizes and adjust them based on location types.

(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) **Accuracy.** The majority of the participants said they are willing to tolerate one or two failures for every 10 lock or unlock attempts. 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.

2.4 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.

3 FIELD STUDY APPLICATION DESIGN

Our next goal was to design a location-based authentication service and use it to conduct a field study and analyze users' real-world behaviors. We aimed to implement a fully working Android application that follows the six design requirements listed in Section 2.3 to the extent possible, and provide sufficient quality and reliability for a field study to be conducted without hindering participants' daily smartphone use.

3.1 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, we also used Wi-Fi 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. We believe that choosing the size of a trusted location among these three levels is a reasonable and practical compromise between accuracy and user preference.

3.2 Design Details

Figure 1 shows an architectural overview of our location-based smartphone authentication application called "Loclock." Loclock consists of 4 key components: (1) Data Collector, (2) Context Detector, (3) Location Detector, and (4) User Service. We explain each component in detail.

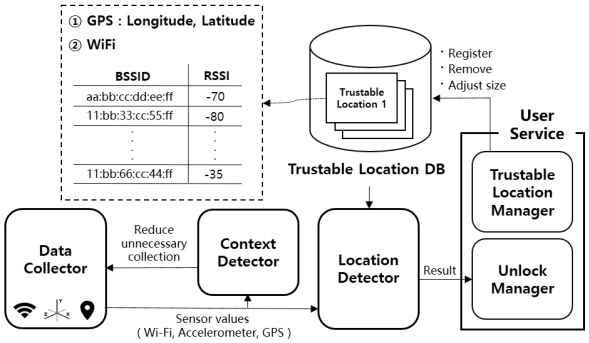


Figure 1: Overview of Loclock.

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 all Wi-Fi "received signal strength indication" (RSSI) values from nearby access points with matching "basic service set identifier" (BSSID). GPS data are used for large area (usually outdoor) detection, and Wi-Fi 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 Wi-Fi RSSI values because continuous and frequent Wi-Fi RSSI collection would use much battery – our design goal was to detect when it is unnecessary to monitor Wi-Fi RSSI values and optimize battery use to meet the "battery use" requirement. For instance, when a user is inside a trusted location coverage area, her phone is unlocked, and she leaves her phone on her desk, there is no need to collect Wi-Fi RSSI values frequently while the phone is sitting idle on the desk.

Location Detector. This component detects whether a phone is inside a registered location coverage area. As the first step, GPS information is used to approximately determine whether a registered location is inside a large coverage area. If the first GPS check indicates that a device is not near any of the registered trusted locations, then Loclock does not collect Wi-Fi RSSI data to avoid unnecessary battery drain. The location detector computes distance using the latitude and longitude information of a registered location and the current GPS data. If the phone is inside this large coverage area, it collects Wi-Fi RSSI values from the nearby access points of the current location and compares them against pre-stored (upon trusted location registration) RSSI values. using Euclidean distance $ED = \sqrt{\Sigma_{bssid \in (C \cap T)}(RSSI_C - RSSI_T)^2}/N$ where Wi-Fi RSSI values collected from current location are denoted as $C = \{(bssid_1 : RSSI_{bssid_1}) \ldots (bssid_i : RSSI_{bssid_i})\}$, and pre-stored Wi-Fi RSSI values of trusted locations are denoted as $T = \{(bssid_1 :$

$RSSI_{bssid_1}) \ldots (bssid_j : RSSI_{bssid_j})\}$. The number of common elements between C and T are denoted as $N = |\{\, i \mid bssid_i \in (C \cap T)\,\}|$. Wi-Fi RSSI values could be sensitive and differently measured under various environmental conditions. When a user stores the RSSI values for a trusted location (T) during the trusted location registration process, Loclock collects a sufficient number of RSSI values for one minute and uses the average value for each BSSID in order to avoid the bias by some outlier RSSI values.

The lower the ED measurement, the closer the current location is to a pre-registered trusted location. We set an ED threshold to determine whether the phone is inside a trusted location coverage area: if an ED value is lower than the threshold value, that particular location is classified as a trusted location, and the phone will be unlocked. We empirically determined the optimal threshold.

To consider situations where only a partial set of BSSIDs are visible, e.g., due to a device being placed far away from the originally-registered spot but still fairly close to one or two access points, we introduce a minimum BSSID match rate that is checked prior to ED computation. BSSID match rate checks the matching proportions of the BSSIDs visible from the current location and the list of BSSIDs stored upon trusted location registration. BSSID match rate is calculated as $|\{\, i \mid bssid_i \in (C \cap T)\,\}|/|\{\, j \mid bssid_j \in T\,\}|$. We use 0.5 as the minimum BSSID match rate, meaning that at least 50% of BSSIDs need to be matched before we start computing ED. The threshold of 0.5 was determined experimentally with a small number of test samples.

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. As for the "setup time" requirement, we designed Loclock to collect Wi-Fi RSSI values for just one minute upon registration. To satisfy the "adjustable location sizes" requirement, we allow users to choose between three coverage sizes: 0 to 5 meters, 5 to 10 meters, and 10 or more meters.

3.3 Lock/Unlock Failure Rate Evaluation

To demonstrate that Loclock is capable of achieving tolerable lock and unlock failure rates as described in the "accuracy" requirement, we collected Wi-Fi RSSI datasets from three different locations using Loclock, identified threshold values for different location coverage options, and evaluated the lock and unlock failure rates.

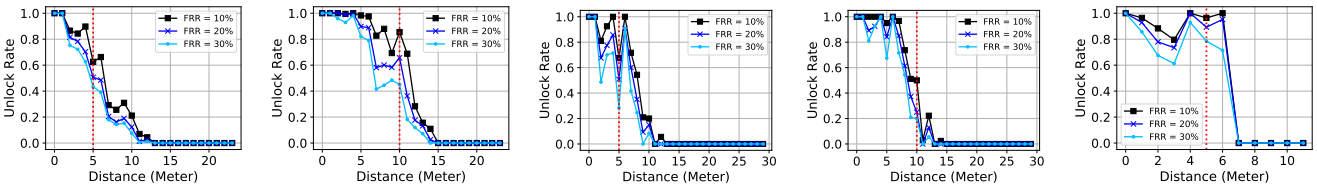
3.3.1 Methodology. Using the Loclock application installed on a Samsung Galaxy S8 phone, we collected Wi-Fi RSSI values from 3 locations. For each location, we created a grid layout with one meter spacing between two grid points, covering the entire floor space. At every grid point, we collected RSSI 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. Wi-Fi RSSI values, collected for a minute, were then used to compute the pre-stored trusted location RSSI vector (T). 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.

3.3.2 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.

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 rates – and measuring resulting three FARs based on the three threshold values. These FRR and FAR results are summarized in Table 3. 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 2 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 Wi-Fi 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. In Appendix C, we show how the ED values change with varying distances for each of the three locations. For L3, there is a sudden jump in ED when we walk out the laboratory door.

3.3.3 Fixing Threshold Values. After evaluating the lock and unlock failure rates of Loclock, we computed the RSSI threshold values to be used in the final version of the application for the field study.



(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 2: 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).

Table 3: 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%	-	-	-

Using the 20% FRR threshold values, we simply averaged the three values to compute a final threshold value for the smaller location size of 0 to 5 meters. Based on this final threshold value, the overall FAR and FRR computed across all three locations were 12.5% and 23.8%, respectively. Similarly, we average two 20% FRR threshold values to compute the final threshold value for the larger location size of 5 to 10 meters. Based on this final threshold value, the FAR and FRR computed across all two locations were 9.1% and 15.5%, respectively. As for the location size larger than 10 meters, we used BSSID matching rule alone (without ED computations) to model a sufficiently large coverage area.

3.4 Battery Usage Evaluation

We performed simple experiments using Galaxy S8 to approximately gauge battery consumption levels. We specifically considered the following two cases. The first case is a less intensive usage scenario where the device is sitting idle on a desk, and only the accelerometer values are collected for an hour. The second case is a more intensive battery usage scenario where both Wi-Fi RSSI and accelerometer data are collected continuously for an hour. In the first case, Loclock alone used up about 3% of battery in an hour; in the second case, it used up about 9%. Note, despite our preliminary efforts to minimize battery use, Loclock would still use more battery than what the participants were willing to tolerate.

3.5 Limitations

The use of Wi-Fi RSSI values alone cannot provide meter-level location detection accuracy because RSSI values can be affected by physical barriers, such as walls and people, other than physical distance between access points and user's location. Hence, our Loclock implementation would inevitably have some lock and unlock failure rates. Furthermore, new Wi-Fi access points may be added, or existing ones may be removed over time. Such changes would likely degrade detection accuracy. One way to resolve this issue is to periodically collect BSSIDs and RSSI values when trusted locations are detected and automatically update them.

Our failure rate evaluation results are based on the data collected from just three locations. We do not claim that these results can be generalized and applied to any indoor location – environments with a small number of access points, e.g., a home in a rural area, have not been studied.

Another limitation is that the battery use reported in the previous section is far greater than what the participants were willing to tolerate. Although we attempted to optimize battery use through context detection – i.e., stop RSSI and GPS monitoring when a phone is sitting idle – there were other functions, e.g., continuous logging for study purposes, that contributed to high battery use. Battery optimization deserves further in-depth investigation as part of future work.

4 FIELD STUDY

To study key requirements for location-based authentication solutions and their implications in depth, we derive two hypotheses from the requirements and the first study findings and conducted a 3-week field study to collect real-world usage data and test those hypotheses. The ethical perspective of the field study was validated through an IRB at a university.

4.1 Hypotheses

The first hypothesis is derived from the "indoor locations" and "multiple locations" requirements, and the first study participants' reasons (see Section 2.2.2) behind choosing certain physical locations as trusted locations.

> *H1: Upon adding a trusted location, people select private places, places they frequently visit, or places where they spend a lot of time.*

We define "private place" as "a place where one may reasonably expect to be safe from uninvited intrusion or surveillance but does not include a place to which the public has lawful access." [1] A "non-private" would then be defined as a place that may not be safe from uninvited intrusions and a place to which the public has free access.

We derive the second hypothesis from the "adjustable location sizes" requirement that states that users may be willing to choose different location coverage sizes, and users' tendency to prefer larger coverage areas while adding non-private (public) locations (see Table 2).

> *H2: People choose larger location coverage sizes upon adding non-private (potentially unsafe) locations.*

The field study has been designed to test those two hypotheses based on the collection and analysis of real-world location registration and usage behavior data.

4.2 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 achieve strong ecological validity, we asked the participants to install our Loclock Android application (described in Section 3) on their own phone, and use it for three weeks. The participants were compensated for their time with a USD 200 gift card. All user interactions with Loclock (e.g., registering trusted locations, trusted location size adjustments, changing location sizes), Wi-Fi data, GPS data, phone lock, and unlock events were logged. To comply with the ethical expectations of IRB, we collected all the data anonymously.

Before starting the study, the participants were informed about the purposes of the study, provided with instructions, and asked to sign a consent form. 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 purpose of the study and switch to using the lock options provided by Loclock during the 3-week study period. We then explained how trusted locations could be registered, removed, and modified (size changes). We also explained how an explicit unlock method, PIN, pattern, or password, can be registered with 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 Appendix D.

Participants were instructed to register and remove trusted locations freely and change trusted location sizes based on their needs for automatic phone unlock. 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 saying that they could freely remove any of the registered locations if they wanted to from that time. To ensure compliance, we disabled the "remove" button until the 10th day. However, in case the participants make mistakes in accidentally registering wrong or unwanted locations, we enabled the remove button just for an hour after initial location registration, and disabled it after an hour.

Our initial thought toward measuring actual lock and unlock failure rates was to provide a UI for the participants to correctly (and manually) label every lock and unlock event as they occur. However, since such interruptions would hinder their daily phone usage behaviors, and break the ecological validity of the study, we decided not to employ this method; instead, we sent an email every 2 days asking the participants to report the number of lock failures and unlock failures (for the last two days) to the best of their knowledge. The participants were aware that they would get this short survey email every two days and asked to try to remember failure counts. To ensure that the participants respond honestly, we explained that these failure counts would not affect the study rewards. We did not give any other instructions.

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, changing location sizes, and removing registered locations. 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. The post-study survey results are summarized in Appendix E. We helped them to uninstall Loclock. Before conducting the field study, we performed several rounds of pilot studies with three people to fix bugs and address unclear instructions and descriptions.

4.3 Results

4.3.1 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," "teacher" and "unemployed" being the top ones.

4.3.2 Registered Trusted Locations. To test the first hypothesis (see Section 4.1), we analyzed all trusted locations registered by participants, including those that were eventually removed, during the entire 3 weeks. As shown in Table 4, 24 participants (83%) registered more than two 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" and "living room" are also part of home, home seems to be the most representative trusted place for location-based authentication. All of those location types would be considered as private places based on our definition in Section 4.1.

Interestingly, 8 participants registered "church" as a trusted location. Although the numbers were small, some participants also registered other non-private locations such as sports facility, library, cafe, subway station entrance, and hospital. These observations are also consistent with the first study results (see Table 1). With respect to the first part of the hypothesis, these mixed observations indicate that private places such as homes and offices are commonly selected as trusted locations, but a wide range of non-private places are selected.

We also analyzed the trusted locations that remained at the end of the study. Table 5 shows the remaining location types and counts.

[1]The Wi-Fi scanning API was depreciated from Android 9.0

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

Table 4: Trusted locations registered during the field study and counts for each location type.

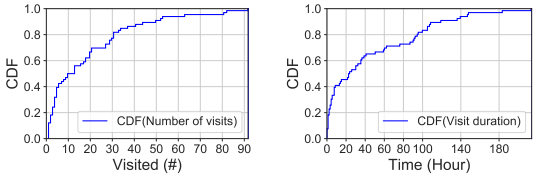
# Locations (# Participants)	One (5)	Two (13)	Three (5)	Four (4)	Five (1)	Six (1)	**Total (29)**
Home	0	10	3	3	1	0	**17**
Office	3	5	2	2	1	0	**13**
My room	2	2	3	2	0	0	**9**
Church	0	5	2	1	0	0	**8**
Living room	0	3	2	2	0	0	**7**
Sports facility	0	0	2	1	2	1	**6**
Lecture room	0	0	0	1	0	2	**3**
Library	0	0	1	0	0	1	**2**
Cafe	0	0	0	0	1	1	**2**
Kitchen	0	1	0	1	0	0	**2**
Bathroom	0	0	0	2	0	0	**2**
Subway station entrance	0	0	0	0	0	1	**1**
Hospital	0	0	0	1	0	0	**1**
Total	**5**	**26**	**15**	**16**	**5**	**6**	**73**

Table 5: Trusted locations remaining at the end of the study, and counts for each location type.

# Locations (# Participants)	One (7)	Two (13)	Three (3)	Four (3)	Five (1)	Six (1)	**Total (28)**
Home	0	10	2	2	1	0	**15**
Office	3	5	2	2	1	0	**13**
My room	3	4	1	1	0	0	**9**
Church	0	4	2	0	0	0	**6**
Living room	1	2	1	1	0	0	**5**
Sports facility	0	1	1	1	2	1	**6**
Lecture room	0	0	0	1	0	2	**3**
Library	0	0	0	0	0	1	**1**
Cafe	0	0	0	0	1	1	**2**
Kitchen	0	0	0	1	0	0	**1**
Bathroom	0	0	0	2	0	0	**2**
Subway station entrance	0	0	0	0	0	1	**1**
Hospital	0	0	0	1	0	0	**1**
Total	**7**	**26**	**9**	**12**	**5**	**6**	**65**

Compared to the results in Table 4, the total number of registered locations decreased from 73 to 65 – 5 participants removed one or more locations after the 10th day. One participant initially registered two locations but removed both of them after the 10th day. Hence, the total number of participants in Table 5 is one lower, 28. Our analyses on how users add or remove locations over time are in Appendix F and G, respectively.

4.3.3 Visit Frequency and Duration. To test the second part of the first hypothesis, 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 3(a)).



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

Figure 3: CDFs computed on the total number of visits and visit duration for all registered trusted locations.

Figure 3(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. Hence, we do not accept the second part of the hypothesis.

Similarly, to test the third part of the first hypothesis, we computed CDF for the total visit duration in hours during the 3 weeks across all registered trusted locations (see Figure 3(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.

4.3.4 Trusted Location Sizes. To test the second hypothesis (see Section 4.1), we analyzed the sizes of trusted locations as they were selected initially. Table 6 shows the number of registered sizes for each location type. "5–10m" (52%) was the most frequently selected location size, followed by "> 10m" (38%). Except for "my room," sizes "5–10m" and "> 10m" were preferred sizes for all other location types.

Table 6: Numbers of registered trusted location sizes for each location type (during the initial registration).

Location	0–5m	5–10m	> 10m
Home	0	10	7
Office	0	6	7
My room	4	4	1
Church	0	3	5
Living room	1	6	0
Sports facility	0	4	2
Lecture room	1	0	2
Library	0	0	2
Cafe	0	2	0
Kitchen	1	1	0
Bathroom	0	1	1
Subway station entrance	0	0	1
Hospital	0	1	0
Total	**7 (10%)**	**38 (52%)**	**28 (38%)**

As for non-private locations – locations other than homes and offices – most of the participants selected 5 to 10 meters or larger than 10 meters as the coverage area. We cannot accept the second hypothesis since many of the non-private locations were also registered with 5 to 10 meter coverage area, indicating that some participants wanted to control the phone unlock coverage for non-private locations. However, it is also true that a large portion of non-private locations was registered with sizes larger than 10 meters (12 out of 23 public locations), which does raise security concerns about some users' size preferences. For instance, 5 out of 8 "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 52% of the reasons behind size selection was *"chose adequate coverage area for daily phone usage."* Intriguingly, no participant mentioned security as a reason for choosing a certain location size. The participants' responses on their trust levels for registered locations are at Appendix H.

In contrast, some private locations like office, my room, living room, and kitchen that provide reasonable protection against intrusions were registered to be smaller than 5 meters – perhaps this is due to people being worried about social insider attacks described in [17]. For some homes and offices, the participants selected the largest coverage areas, showing that people have varying size preferences, even for private ones.

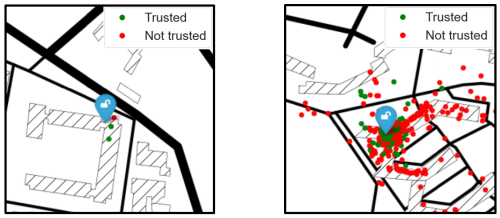
4.3.5 Adjusting Trusted Location Sizes. In total, the participants changed the trusted location coverage meters 9 times. Interestingly, 8 size adjustments involved increasing the coverage meters; just one adjustment led to a decrease in coverage meter from "> 10m" to "5-10m." Appendix I visually demonstrates size adjustments.

4.3.6 Unlock and Lock Failure Rates. As explained in Section 4.2, rather than requesting manual labeling after phone lock/unlock, we sent out emails every two days and asked the participants to report on the number of unlock and lock failures they witnessed during the past two days. By adding those failure counts, and using the total number of locks/unlocks that were initiated by Loclock, we approximately computed the FRR and FAR for each participant. We excluded responses from one participant who reported zero failure over the entire 3-week period since this is unrealistic.

The average FAR reported for 16 participants was 1.08%; the highest reported FAR was just 3.18%. The average FRR reported for 23 participants was 5.8%, and the highest reported FRR was 24.6%. Although these were self-reported failure rates, these results provide reasonable evidence that Loclock provided an adequate level of phone lock/unlock experience throughout the field study – inline with the tolerable failure rate requirements.

4.3.7 Number of Unlock Attempts. We logged the GPS data for all locations where the participants' phone screens were turned on, and Loclock either locked or unlocked the screen. Figure 4 approximately visualizes some parts of a real map and all locations where the phone screens of P2 and P15 were turned on, marked with red and green dots. Green dots represent places that were classified as trusted locations, and red dots represent places that were not classified as trusted locations. The blue unlock image represents where trusted locations were registered. Shading patterns indicate the inside of buildings. Figure 4(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 4(b) shows that P2 used the phone frequently near the registered trusted location. While P2 was using the phone in this particular area, Loclock would have automatically unlocked his or her phone many times.

Figure 5 shows the distribution of the ratios in which phones were unlocked automatically through Loclock. The x-axis represents the ratio of the number of times phone was unlocked automatically with Loclock to the total number of unlock attempts. The y-axis counts the number of users that belong to each ratio category. On average, the participants turned their phone screens on 44.4 times a day. This result is in line with the number reported in a prior work [9], which was 39.9. On average, Loclock reduced about 37% (σ = 17%) of manual unlock attempts. The Loclock-initiated automatic unlock ratio for two participants was below 10%. The key difference is that these two participants did not add "home" as a trusted location. In contrast, all three participants who



(a) P15 (b) P2

Figure 4: Partial map view (250 by 250 meters) of where the phone screen was turned on.

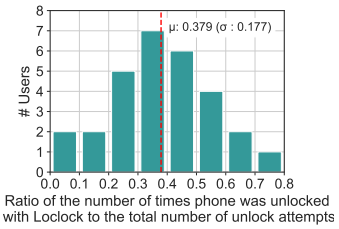


Figure 5: Distribution of the ratios in which phones were unlocked automatically through Loclock.

demonstrated an automatic unlock ratio greater than 60 percent had "home" or "my room" registered.

4.4 Limitations

We made it mandatory to register at least one trusted location and use it for at least 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.

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.

Our lock and unlock failure rates were measured through self-reported counts of failures, and may not accurately reflect real-world error rates.

5 DISCUSSIONS

5.1 Security Concerns and Mitigation

The results from the interviews and field studies raise two important security concerns: (1) people tend to add a variety of non-private, potentially unsafe locations without considering security implications, and (2) a significant proportion of such non-private locations are added with the largest coverage areas (larger than 10 meters). Moreover, some participants added infrequently visited locations and locations where they spend a small amount of time as trusted locations – most of them being non-private, unsafe places exposed to phone theft. All of those observations indicate that location-based authentication schemes, if not designed carefully, could expose new security threats that may be exploited by adversaries. For instance, if an adversary has some information about a victim's location history, the adversary could try to steal the victim's phone and go near

a pre-registered trusted location, and access the phone contents without having to guess PIN or pattern.

To mitigate such threats, we should design location-based authentication systems to adequately inform users about the security risks associated with registering non-private locations and selecting large coverage areas while doing so. As a protective measure, systems could be designed to disable large coverage area selection options when users select locations other than homes or offices. Another mitigation strategy would involve implicit use of other contextual information when phones are unlocked inside non-private locations: e.g., presence of a known Bluetooth device like smartwatches (that the device owner is also carrying) may also be monitored. In business or government environments with more strict security requirements, one might consider disallowing selection of any non-private locations. To deal with infrequently visited public locations becoming potential security holes (without offering much usability benefits), we can design systems to detect infrequently visited locations, and ask users to remove them.

5.2 Usability Improvements

As shown in Appendix E, 21% of the participants felt that the trusted location registration process was slow. Loclock required the participants to wait for a minute to collect Wi-Fi RSSI values. One possible improvement strategy is to automatically collect RSSI values based on users' frequently visited places (i.e., location patterns) and prompt suggestions, asking users whether they would like a frequently visited place to be added as a trusted location. 38% of the field study participants who registered three or more trusted locations (see Table 4) would benefit from this automation.

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 Wi-Fi 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 [19] 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 values based on their preferences to reduce unlock failures or lock failures.

6 RELATED WORK

Several implicit authentication methods [4, 11, 16, 18] have been proposed. Implicit authentication uses a user's behavioral biometrics to identify the user without requiring explicit user inputs [11]. However, to the best of our knowledge, just one prior research attempted to study usability and security aspects of implicit authentication [12]. According to the study results, 91% of participants found implicit authentication convenient, and 81% perceived the provided security level to be satisfactory. However, 35% chose false rejects as a cause of annoyance in using implicit authentication. 27% and 22% chose false accepts and detection delay, respectively, as security concerns. Their results are higher than our usability and security responses – this is mainly due to their study being conducted as a simulation experiment with a mock-up application; in contrast, our real-world study involved the deployment of a fully working application that affected users' daily phone use.

The location-based authentication concept that we explore in this paper is one type of implicit authentication: the goal is to automatically identify users or devices with geographical location information [6]. A few studies [8, 13, 15, 22] suggested that location factors can be used to authenticate users or devices. Fridman et al. [8] demonstrated that physical location of devices can be used to identify users accurately, and outperform other features such as stylometry or application usage information – classification on a single GPS coordinate was sufficient to correctly identify users with a false acceptance rate under 0.1, and a false rejection rate under 0.05. However, all of those studies have focused on developing classification models to identify users – there is no prior work on analyzing usability and security perceptions of location-based authentication. To the best of our knowledge, this is the first effort to study users' concerns and expectations on using location information to implicitly unlock smartphones in depth.

An accurate algorithm for determining users' locations is essential to implement a secure and usable location-based authentication scheme. Several studies discussed the use of wireless (e.g., Wi-Fi) signals to identify device locations. Hilsenbeck et al. [10] 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. [21] presented another fusion approach using magnetic signals and Wi-Fi signals to achieve 3.5m accuracy 90% of the time. Recently, 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 setting. Davidson et al. [5] provides an overview of existing indoor positioning techniques for smartphones. In this paper, we implemented a fully working indoor location-based authentication solution that does not require specialized hardware nor a fingerprinted wireless signal map. We used this application to conduct a 3-week field study – we believe we are the first group to collect such location data and analyze users' real-world registration and use of trusted locations.

7 CONCLUSION

Through the interviews and field studies, we identified essential requirements for building usable and secure location-based authentication services; users should be able to register fine-grained indoor locations and adjust location coverage sizes. Using a location-based authentication service, the participants, on average, were able to reduce 37% of explicit authentication attempts. Our findings also suggest that people will add non-private (potentially unsafe) locations, and select large coverage sizes without carefully considering security risks associated with phone breaches. Such risks may also exist in commercialized services like Google's Smart Lock and need to be mitigated. Future location-based authentication systems should be designed to effectively convey security risks associated with adding non-private locations and discourage users from choosing large coverage sizes for freely accessible non-private places.

REFERENCES

[1] [n.d.]. *Chapter 21.–CRIMES AND PUNISHMENTS.* Kansas Statutes. https://www.ksrevisor.org/ksa.html

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

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

[4] A. Alzubaidi and J. Kalita. 2016. Authentication of Smartphone Users Using Behavioral Biometrics. *IEEE Communications Surveys Tutorials* 18, 3 (2016), 1998–2026. https://doi.org/10.1109/COMST.2016.2537748

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

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

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

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

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

[10] Sebastian Hilsenbeck, Dmytro Bobkov, Georg Schroth, Robert Huitl, and Eckehard Steinbach. 2014. 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.* 147–158.

[11] Hassan Khan, Aaron Atwater, and Urs Hengartner. 2014. Itus: An Implicit Authentication Framework for Android. In *Proceedings of the 20th ACM Annual International Conference on Mobile Computing and Networking.* 507–518.

[12] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2015. Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In *Proceedings of the 11th Symposium On Usable Privacy and Security.* 225–239.

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

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

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

[16] W. Meng, D. S. Wong, S. Furnell, and J. Zhou. 2014. Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys Tutorials* 17, 3 (2014), 1268–1293. https://doi.org/10.1109/COMST.2014.2386915

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

[18] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello. 2016. Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine* 33, 4 (2016), 49–61. https://doi.org/10.1109/MSP.2016.2555335

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

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

[21] Y. Shu, C. Bo, G. Shen, C. Zhao, L. Li, and F. Zhao. 2015. Magicol: Indoor Localization Using Pervasive Magnetic Field and Opportunistic WiFi Sensing. *IEEE Journal on Selected Areas in Communications* 33, 7 (2015), 1443–1457.

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

A CODE SATURATION IN THE REQUIREMENT STUDY

Figure 6 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.

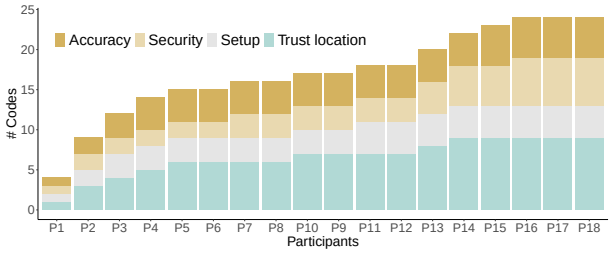


Figure 6: Code saturation results. "Accuracy" indicates unlock accuracy expectations; "Security" indicates security expectations; "Setup" indicates setup time; and "Trust location" indicates trust location considerations.

B TOLERABLE BATTERY CONSUMPTION

Table 7 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 7: Tolerable daily battery usage levels.

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

C CHANGES IN EUCLIDEAN DISTANCE

Figure 7 shows how ED changes while moving away from the originally registered spots. 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.

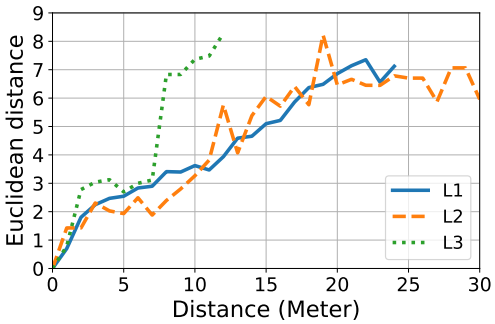
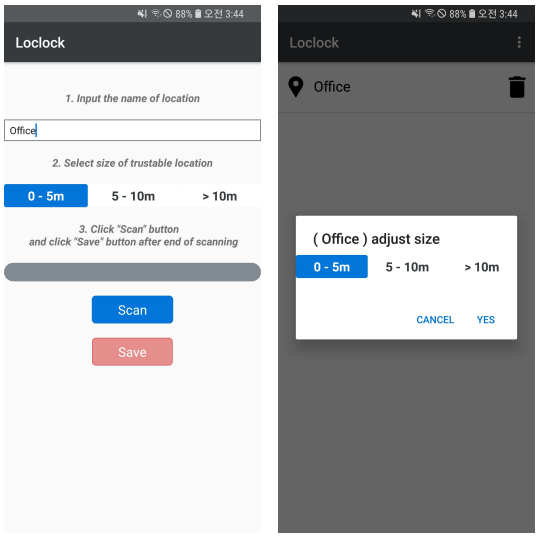


Figure 7: Changes in Euclidean distance while moving away from the originally registered spots in each of the three locations.

D LOCLOCK SETUP SCREEN

Figure 8 shows screenshots of Loclock for registering a trusted location. Users can freely remove or adjust the size of a registered trusted location.



(a) Registering a trusted location. (b) Adjusting the size of a registered trusted location.

Figure 8: Loclock setup screen.

E 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 9. About 86% felt that it was easy to register trusted locations, and there was no participant who felt it was difficult.

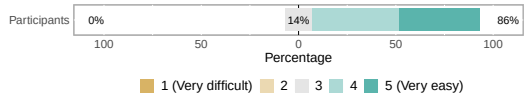


Figure 9: Easiness of registering trusted locations.

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 Wi-Fi RSSI values is one minute. Their responses are summarized in Figure 10. About 48% of the participants felt that the time taken to register trusted locations was fast. 21% felt that it was slow.

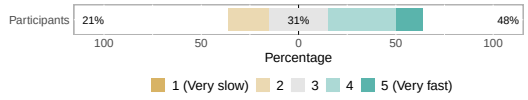


Figure 10: Fastness of registering trusted locations.

Security of Loclock. We asked how the participants felt about the security offered by location-based authentication; their responses are summarized in Figure 11. About 62% of the participants felt that using Loclock was secure; only 7% felt that it was insecure. The low reported FARs (1.08% on average) are one explanation as to why the participants may have felt that Loclock was secure to use.

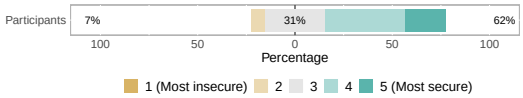


Figure 11: Security of using Loclock.

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 12. 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 that they could not use fingerprint scanner, which was their original daily unlock method. Only one participant mentioned battery drain as the reason.

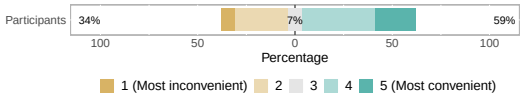


Figure 12: Convenience of using Loclock.

F NUMBER OF TRUSTED LOCATIONS REGISTERED OVER TIME

P20 initially registered two trusted locations but removed both locations 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 8 shows the number of trusted locations registered each day of the 3-week study period for each location type. Participants initially registered 43 locations on the first day, and additionally registered 29 locations.

G TRUSTED LOCATION REMOVAL

Table 9 shows those results by each location type. There were only five participants who removed at least one trusted location after the 10th day. Eight location types, "office," "my room," "sports facility," "lecture room," "cafe," "bathroom," "subway station entrance,"

Table 8: 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	**17**
Office	8	1	3	1	0	**13**
My room	6	2	0	0	1	**9**
Church	5	1	0	1	1	**8**
Living room	7	0	0	0	0	**7**
Sports facility	1	3	0	1	1	**6**
Lecture room	1	1	1	0	0	**3**
Library	1	0	0	0	1	**2**
Cafe	0	0	0	1	1	**2**
Kitchen	1	1	0	0	0	**2**
Bathroom	0	0	0	1	1	**2**
Subway station entrance	1	0	0	0	0	**1**
Hospital	1	0	0	0	0	**1**
Total	**43**	**13**	**4**	**6**	**7**	**29**

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.

Table 9: Columns "one," "two," and "three" refer to the number of trusted locations that were removed after the 10th day; for example, column "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**
Living room	1	0	1	**2**
Sports facility	0	0	0	**0**
Lecture room	0	0	0	**0**
Library	1	0	0	**1**
Cafe	0	0	0	**0**
Kitchen	1	0	0	**1**
Bathroom	0	0	0	**0**
Subway station entrance	0	0	0	**0**
Hospital	0	0	0	**0**
Total	**3**	**2**	**3**	**8**

H TRUST LEVELS OF REGISTERED LOCATIONS

We asked participants to rate the trust level of each location that they registered on a five-point Likert scale ("not at all trusted," "not very trusted," "neutral," "trusted," and "highly trusted"). Among 73 locations (see Table 4) that were registered during the field study, 37 (50.7%) of those locations were rated as "highly trusted," 26 (35.6%) as "trusted," and 10 (13.7%) as "neutral." No one rated the trust level of any registered location as "not very trusted," or "not at all trusted." These results seem intuitively reasonable because we explicitly asked the participants to register "trusted" locations.

Figure 13 shows the proportion of registered trusted locations, categorized by the coverage size. Interestingly, for the locations registered with sizes "0–5m" and "5–10m," "highly trusted" was more preferred while for the locations registered with "> 10m," "trusted" was more preferred. This implies that participants' trust level would be decreased when the size of registered locations is larger than 10m.

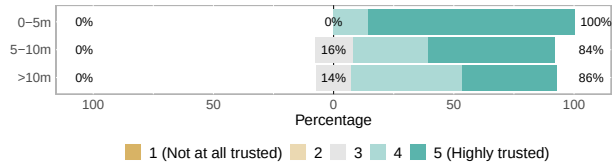


Figure 13: Proportion of registered locations in each size of trusted location.

We also analyzed the distribution of trust levels of registered locations by location type in Figure 14. For all registered locations except for "home," "office," "cafe," "sports facility," "hospital," and "subway station entrance," the participants selected either "highly trusted" or "trusted" as trust levels. Interestingly, 6% of the participants mentioned "neutral" trust level for "home."

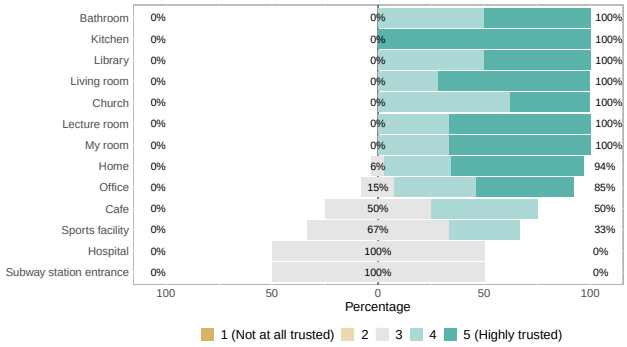


Figure 14: Trust levels of registered locations by location type.

I SIZE ADJUSTMENTS OF REGISTERED LOCATIONS

Figure 15 visually demonstrates size adjustments. Blue arrows show adjustments leading to size increases, and red arrows show adjustments leading to size decreases.

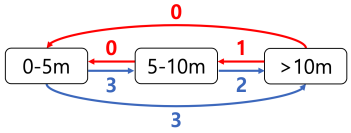


Figure 15: Size adjustments of trusted locations.