Exploring the Usability, Security, and Privacy of Smart Locks from the Perspective of the End User

Hussein Hazazi and Mohamed Shehab,
University of North Carolina at Charlotte

https://www.usenix.org/conference/soups2023/presentation/hazazi

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

August 7–8, 2023 • Anaheim, CA, USA

978-1-939133-36-6

Exploring the Usability, Security, and Privacy of Smart Locks from the Perspective of the End User

Hussein Hazazi
University of North Carolina at Charlotte
hhazazi@uncc.edu

Mohamed Shehab
University of North Carolina at Charlotte
mshehab@uncc.edu

Abstract

Smart home devices have recently become a sought-after commodity among homeowners worldwide. Among these, smart locks have experienced a marked surge in market share, largely due to their role as a primary safeguard for homes and personal possessions. Various studies have delved into users' apprehensions regarding the usability, security, and privacy aspects of smart homes. However, research specifically addressing these facets concerning smart locks has been limited. To bridge this research gap, we undertook a semi-structured interview study with 29 participants, each of whom had been using smart locks for a minimum period of two months. Our aim was to uncover insights regarding any possible usability, security, or privacy concerns related to smart locks, drawing from their firsthand experiences. Our findings were multifaceted, shedding light on mitigation strategies employed by users to tackle their security and privacy concerns. Moreover, we investigated the lack of concern exhibited by some participants regarding certain security or privacy risks associated with the use of smart locks, and delved into the reasons underpinning such indifference. In addition, we explored the apparent unconcern displayed by some participants towards specific security or privacy risks linked with the use of smart locks.

1 Introduction

Over the past two decades, the Internet of Things (IoT) has seen a significant uptick in the complexity and range of its applications. These applications span various sectors, from healthcare and smart manufacturing to smart home solutions that aim to enhance users' quality of life by affording them greater control over their home devices. One of the emerging technologies within this space is smart locks, which were introduced as an advanced alternative to traditional locks [17]. These devices offer a broader array of features beyond mere door locking and unlocking. In recent years, the smart lock market has expanded and grown more competitive, leading to an array of diverse designs and operational characteristics being introduced [3]. As per the Statista Research Department [15], the global smart lock market size, valued at approximately 0.42 billion dollars in 2016, is predicted to exceed four billion dollars by 2027. Considering the anticipated market size and the critical role smart locks play as a primary line of defense against potential intruders, it's crucial to evaluate their usability, privacy, and security from the perspective of current users. Understanding these user evaluations can highlight potential areas of improvement, informing future design and functionality enhancements for these devices.

Several studies, such as [11,29–31], have assessed concerns related to the usability, security, and privacy of smart homes, primarily from the user's standpoint. While other researchers [13,21,28] have examined the issues and possible mitigation strategies related to the privacy and security of smart locks from the systems perspective, little research has been done on smart locks' usability, privacy, and security from the end user's perspective, creating a gap in the research. To address this, our study was carried out to investigate user perceptions of privacy, security, and usability associated with smart locks. As part of this study, we investigated the following research questions:

- RQ1: What aspects of the smart lock's design and functionalities make it appealing to users from a usability standpoint?
- RQ2: What privacy and security concerns do end users have regarding smart locks?
- RQ3: How do end users deal with their privacy and se-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

curity concerns?

- RQ4: What are the end user's perceptions regarding how the security and privacy of smart locks can be improved?

To help us answer these questions, we conducted semi-structured interviews with 29 smart lock users who had used their locks for at least 2 months before the interview and had used their smart locks to share access with other users. Our main goal was to better understand their concerns related to different aspects of smart locks as well as how they deal with those concerns. In general, our work makes the following contributions:

- Provide a thorough analysis of the usability, security, and privacy of smart locks from the perspective of the end user which gives us an understanding of how to improve each of the three aspects.
- Demonstrate that more work needs to be done to increase consumer awareness regarding security and privacy issues related to smart locks.
- Offer suggestions and recommendations for improving the security and privacy of smart locks based on our analysis of participant feedback.

2 Related Work

2.1 Smart Locks Security and Privacy

The comprehensive analysis of smart locks, with a particular focus on usability, privacy, and security from the user's perspective, remains largely unexplored. Despite this, there are multiple studies conducted by researchers, which delve into the examination of the overall security and privacy of the various smart lock models. For instance, Ye et al. [28] analyzed the security facets of the August smart lock, highlighting potential threats that could compromise the security and privacy of users. Their analysis reveals that these locks are vulnerable to several types of attacks, including Denial of Service (DoS), and loopholes that could allow attackers to access the owner's personal information, thereby risking their privacy. In a similar vein, Ho et al. [13] carry out a security and privacy analysis of five different commercially available smart locks to identify potential vulnerabilities and suggest effective defenses against these. Their findings indicate that some of these locks could fall victim to state consistency attacks, relay attacks, and unwarranted unlocking, among other problems. They also offer potential defensive strategies against such breaches. Several other studies [2, 5, 14, 20, 21, 26] aim to enhance the security and privacy of smart locks by proposing innovative frameworks, utilizing technologies such as blockchain [5], facial recognition [14, 20], and a combination of steganography and cryptography [2]. There is also an acknowledgment of the deficiencies in the access control management systems currently employed in commercial smart locks. These deficiencies could potentially jeopardize the security and privacy of these devices. Xin et al. [26] proposed replacing the prevalent role-based system with an attribute-based access control system, which could enhance the granularity of access control within smart locks and address issues like state consistency attacks, unauthorized unlocking, and cascading deletion of permissions.

2.2 Smart Home User Studies

As a member of the smart home device family, smart locks share several common attributes and functions with their counterparts. Most notably, these devices are typically managed through a dedicated companion app and maintain access logs. Previous studies have investigated various facets of smart home device usability, exploring topics like the motivation behind investing in such devices and the impact they have on enhancing domestic life quality. In [6], a significant number of participants expressed that the adoption of smart home devices elevated their sense of security and control within their homes. Participants also identified additional incentives for adopting these devices, such as the convenience they offer and the sense of staying abreast of technological advancements. Another study [4] proposed that smart home devices are generally expected to outperform their traditional counterparts in terms of functionality. However, the reliance solely on smartphone control and the absence of manual control options for some of the simplest yet most frequently used features was found to heighten user frustration [7]. This reflects the necessity for a balance between technological advancement and user-friendly design in the development of smart home devices.

Earlier studies have delved into the security and privacy apprehensions of end-users concerning smart home devices. For instance, Haney et al. [11], in their study involving interviews with 40 smart home device users, sought to understand any security or privacy worries these users may harbor and the strategies they adopt to alleviate these concerns. Their findings pointed out that the principal worry for users centered around devices equipped with audio and video features potentially being breached, a sentiment echoed by Zheng et al. [31] in their study. This suggests that users may express less concern over the security implications associated with other smart home devices lacking audio or video capabilities, such as smart locks. A number of studies, such as Haney et al. [9] and Tabassum et al. [22], report a seeming lack of concern among certain users regarding the security and privacy aspects of smart home devices. However, this apparent lack of concern doesn't necessarily denote lack of awareness. In fact, the studies indicate that this lack of concern often stems from a trust in the device manufacturer's ability to rectify any security issues, or a belief among users that they are unlikely to be targets for potential attackers [29]. Some users expressed that their concern was confined only to smart home devices located in sensitive areas within their homes, suggesting a nuanced understanding of privacy and security concerns in different contexts [30].

In [23], Tabassum et al. conducted a user study with 39 participants (18 owners of smart locks and video doorbells and 21 non-owners) to explore the users' perceptions of the configurations and controls available in smart locks and video doorbells. Some participants reported concerns regarding unauthorized attempts to unlock the smart lock but they mostly turn the notifications on in order to be alerted to such attempts. Other participants were also concerned about hacking attempts which might allow adversaries to remotely unlock the door and provide physical access to the home. For most of the security concerns, some participants stated that their only way to cope with those concerns was to put trust in the manufacturers' security measures. However, unlike [23], our study puts more focus on examining smart locks users' level of concern regarding specific aspects of the security and privacy of the smart locks as well as investigating the usage behaviors of smart lock users. Zlatolas et al. also conducted a survey study with 306 participants in order to get an insight into their security perceptions of IoT devices within the smart home [18]. The findings of the study revealed a positive impact of device vulnerability awareness on the perception of security importance. Meaning that users who were more aware of the security vulnerabilities of smart home devices also believed in the importance of implementing mitigation strategies in order to protect their smart home devices against possible security threats and vulnerabilities.

Our study results mostly align with previous work while identifying additional privacy and security concerns and mitigation strategies specific to smart locks. Furthermore, our study investigates the usage behaviors of the smart lock's end users.

3 Methodology

We conducted a semi-structured interview study with smart lock users in order to gain a deeper understanding of smart lock users' opinions on different aspects of the lock based on their experience using the lock and to explore their ideas about how the lock can be improved in terms of usability, privacy, and security.

3.1 Participants

We sought participants who had used their smart locks for at least two months and shared electronic keys (digital keys) with others (family members, neighbors, parcel delivery, etc.). The participants were recruited through a mass email sent to the students and employees at the university as well as an advertisement post on the SmartHomes sub-reddit on the Reddit forums. Potential participants were asked to fill out a screening survey which contained questions such as what type of smart locks they have, for how much time have they been using them, and how many people do they share the locks with. Such questions allowed us to verify the participants' eligibility to take part in the study. A total of 29 participants were recruited. Among the participants, 10 were males and 19 were females, and all of them live in the United States. Most of them (n=16) were in the age group of 26-35 while 10 participants were in the age group of 18-25 and 3 participants were in the age group of 36-50. The majority of participants (n=24) stated that they had been using at least one smart lock for more than 4 months while 5 other participants had used their locks for 2-4 months.

3.2 Procedure

A researcher contacted participants who were selected for the study based on the screening survey to arrange a date and time for the interview. According to each participant's preference, all interviews were conducted virtually over Zoom, Google Meet, or Webex. Interviews lasted about 40 minutes on average and each participant was given a $10 Amazon gift card for participating in the study. The study was approved by the university's Institutional Review Board (Protocol #21-0295). Each interview was divided into two sections. The first part focuses on exploring the usability aspect of the smart lock while the second part focuses more on the privacy and security aspect of smart locks. Each part contained open ended questions as well as Likert scale questions. Participants were asked to explain their reasons for choosing a particular answer in order to better understand their perspective. Towards the end of the privacy and security section of the interview, we ask the participants to watch a YouTube video that was prepared and uploaded by one of the researchers which contains a demonstration of 2 types of state consistency attacks that some smart locks are susceptible to. Once the participant finishes watching the video, the researcher asks them some questions regarding the two issues illustrated in the video.

3.3 Data Analysis

Each interview conducted was audio-recorded and subsequently transcribed for analysis. Our data collection was bifurcated into qualitative and quantitative components. The qualitative data was processed using an inductive coding approach. This procedure was carried out independently by two researchers who then engaged in discussions to finalize the coded data, thereby resolving any potential disagreements. The final codebook consisted of 13 main codes and 53 subcodes. The complete codebook is added in Appendix A.3. Turning to the quantitative data, our main approach involved the use of descriptive statistics, given that the bulk of our interview questions were not formulated to test for statistical significance among variables. Nevertheless, for the few questions that did require a test of statistical significance, we employed the non-parametric Wilcoxon Signed Ranks Test, considering the data didn't adhere to a normal distribution pattern.

4 Results

4.1 Usage Behaviors

The purpose of this section of the paper is to identify the popularly used smart lock features as well as understand end users' usage behaviors. Investigating these aspects of smart locks leads to a broader understanding of what aspects of the smart lock's design and functionalities make it appealing to end users from a usability standpoint (RQ1).

4.1.1 Adopting a Smart Lock

As an emerging technology, smart locks have their strengths and weaknesses in terms of privacy, security and usability, especially when compared to traditional locks that homeowners are already familiar with. In response to a question about whether participants hesitated before switching to a smart lock from a traditional lock, 12 participants said that they had some concerns initially and that it took them some time to become convinced that adopting a smart lock was the right choice. The two main reasons behind the hesitation were price and security. A smart lock can cost up to ten times as much as a traditional lock, which can be a big financial commitment. The security of smart locks was also a big concern among some participants who hesitated before adopting a smart lock.

Asked why they chose to switch from a traditional lock to a smart lock, the majority of participants (n=20) said it was because of how convenient using a smart lock is compared to using a traditional lock, whereas only 8 participants cited security as a reason for using one.

4.1.2 Automation

By using communication protocols such as Zigbee and Z-Wave, smart home devices can communicate with each other to automate tasks. In spite of this, only 4 out of 29 participants created automation scenarios that utilized smart locks. P2, for example, has an automation scenario set up so that when an authorized user unlocks the smart lock, the home security alarm is automatically disabled without having to manually disable it every time a resident enters the house. Many automation scenarios can be set up using the smart lock to increase the level of convenience and security of a house, but most participants were not aware of the possibility of creating automation scenarios that include the smart lock.

Reason for turning on notifications	**Count**
Get alerts when the deadbolt is jammed	10
Get alerts about who is accessing the house	8
Get security alerts	4
Get battery alerts	1

Table 1: Reasons for enabling smart lock notifications.

4.1.3 Features and Capabilities

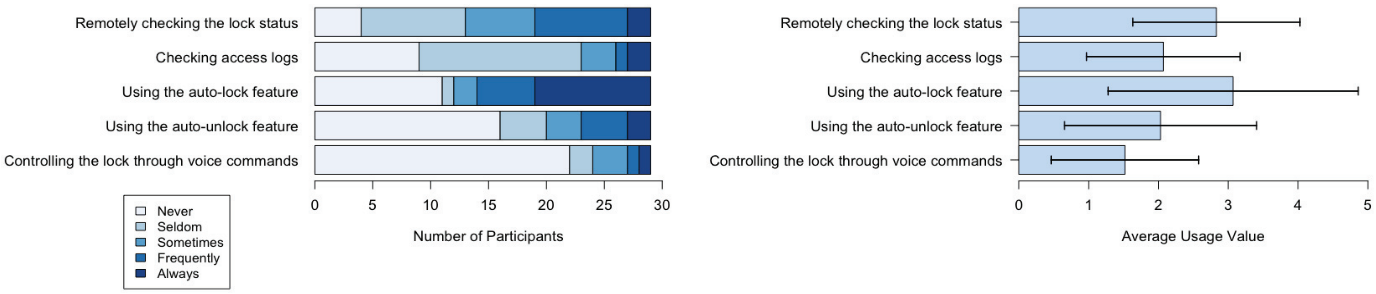
Compared to traditional locks, smart locks offer more features besides the basic function of locking and unlocking doors. The three most popular features that participants mentioned, unprompted, when asked to describe the features of their smart locks that they liked most were the ability to remotely control the lock (n=14), keyless entry (n=10), and the ease of giving others access (n=5). The ability to remotely check if the door is locked (n=3), the ability to unlock the door in multiple ways (n=3), and the auto lock feature (n=2) were not as popular among participants.

We also engaged the participants to evaluate their usage frequency of distinct smart lock features. To do this, we used a Likert scale that used the following designations: 'never', 'seldom', 'sometimes', 'frequently', and 'always', where 'never' corresponded to 1 and 'always' to 5. The "auto-lock" and the "remote lock status checking" features emerged as the most utilized among the smart lock features, as illustrated in Figure 1. The popular preference for these features stems from the heightened sense of security they afford to participants, particularly when they're away from home, by guaranteeing the door is securely locked – an observation underscored by a number of participants.

In terms of notifications, the majority of participants (n=21) stated that they keep smart lock notifications on. According to participants, the most common reason for enabling notifications is to be notified when the deadbolt jams on the door frame and does not lock properly, which is a common problem with smart locks. Notifications were also enabled to keep track of who was accessing the house in real-time, get alerts when the smart lock's battery was low, and see who was entering the apartment in real-time. in contrast, some participants (n=8) stated that they prefer to turn notifications off either because they don't prefer to use the app at all or because they find notifications annoying. Another participant was concerned that turning notifications on could violate other household members' privacy.

4.1.4 Managing Electronic Keys

Electronic keys are usually shared and revoked through the companion application. They can be in the form of a token on the user's smartphone or an access code that the user needs to enter every time they unlock the door. Participants were asked to evaluate two factors - ease of use and reliability -



(a) Usage frequency

(b) Average usage frequency

Figure 1: Smart lock's features usage frequency.

when it came to sharing their smart locks with others. Twenty-two participants found sharing access to the smart lock quite easy, but seven found it quite challenging, especially for older or less tech-savvy individuals. Among the participants, only two found it difficult to revoke someone's access to the smart lock. It is also worth mentioning that 13 participants reported that they never felt the need to revoke another person's access. Participants did not report any issues with the reliability of the access sharing process. When they share access with others, the other person is always able to operate the lock based on their access rights with no issues.

Access Sharing Patterns Access to the smart lock is usually shared through sending an invitation either by phone or email. When the other person accepts the invitation, they would be able to control the lock to the extent of their access level. Another way to share access to the smart lock is through an access code, usually 4 to 6 digits long, that allows the other person to unlock the door. Out of 29 participants, 13 reported that they only share access to their locks with people who live with them, such as roommates or family members. They feel more secure knowing that only the residents can unlock the door. The rest of the participants (n=16) stated that they give access to those who live inside the house, as well as others who don't live in the house such as guests, babysitters, contractors, dog walkers, etc. However, it is common for them to give "temporary access" to some of those who do not live in the house. For example, a dog walker who walks the dog from 10am to 11am can only unlock the door during these hours. Others, such as visiting family members or friends, can access the house at any time, but do not have full access to the lock in terms of checking access logs, giving access to others, or any other features besides locking/unlocking the door.

4.1.5 Usability Improvements

Although some participants were fairly satisfied with the smart lock's current features, others believed that it could be significantly improved by making some modifications and adding some new features. Some of these modifications include:

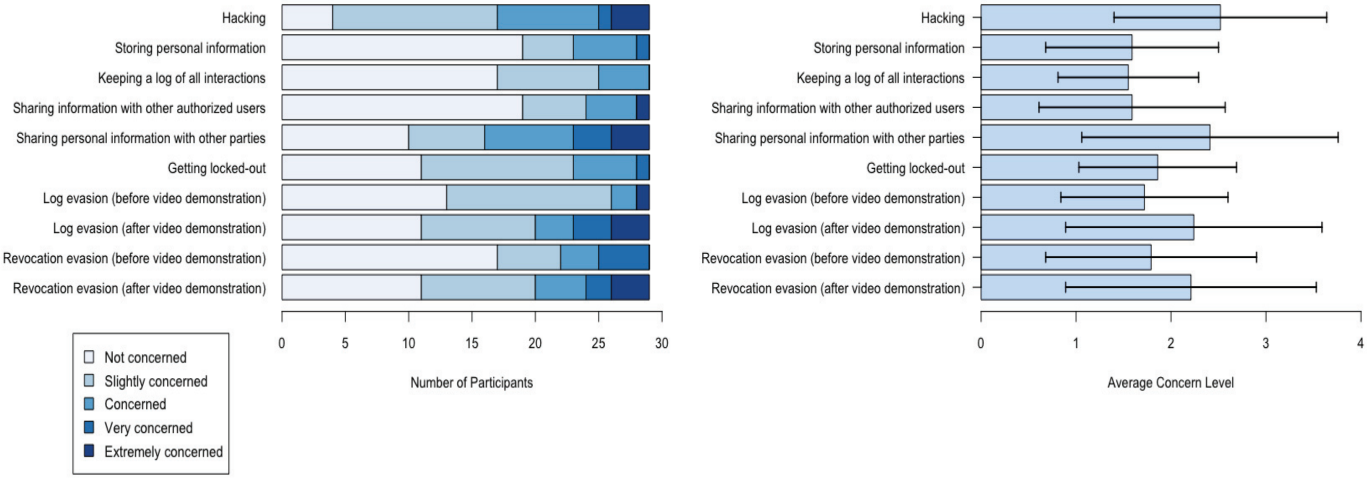
Improving the Battery In the case of smart locks, a dead battery can leave someone locked out of their home, especially if the lock doesn't offer any other means of unlocking it. Some participants (n=3) suggested different ways to improve the battery.

> **P27:** *"It would be nice if there was such thing as like a mini key fob that I could put on the bottom of the lock, just give it a charge so I can unlock it real quick to get into the house. That way, I could have that on my keys, and if I'm locked out when the battery's dead, I could just kind of like jump start it."*

Smart Watch Integration One of the participants suggested allowing smart locks to be operated by smart watches. This would be a very convenient feature especially for runners who prefer to leave their smartphones at home and only wear their smart watch. However, this feature already exists in some smart locks and watches such as the August smart locks that are compatible with Apple watches. Not all commercially available smart locks and smart watches support this feature though.

4.2 Security and Privacy Concerns

The purpose of this section is to explore and analyze the participants' insights regarding their privacy and security concerns (or lack thereof) with their smart locks (RQ2). In order



(a) Level of concern

(b) Average level of concern

Figure 2: The participants' level of concern associated with different smart locks privacy and security threats.

Security or privacy concern	Count
Hacking	9
Using and sharing access codes	7
Physical tampering with the lock	3
Losing the smartphone	2
Getting locked out	2
Revocation evasion	1

Table 2: The participants' security and privacy concerns related to smart locks (unprompted).

to ensure that they have had enough time to develop an opinion regarding the security and privacy controls of their smart locks, all participants have owned/used their smart locks for at least two months prior to the interview date and have used shared access to the lock with other users.

To gain an overall comprehension of the primary security and privacy concerns that smart lock users possess, we initially solicited from the participants any general security or privacy concerns they have associated with smart locks (Refer Table 2). This was followed by questions regarding their degree of concern about specific security and privacy issues related to smart locks (Refer Figure 2). The specific threats presented to the participants were formulated based on findings from previous research in the fields of smart locks and smart home security. These threats included concerns of log evasion, log revocation, and the possibility of being locked out, as discussed in previous studies such as [13, 16, 19, 25], which explored the security vulnerabilities prevalent in some smart lock systems. Furthermore, we asked the participants about concerns regarding hacking threats, storage of personal information, maintaining a log of all interactions, sharing personal details with other authorized users, and the possibility of information being disseminated to other parties. These additional concerns were also derived from previous research [11, 24, 29, 31], which delved into security concerns of smart home users associated with smart home devices. The participants' responses were recorded using a Likert scale, with designations ranging from 'not concerned' (assigned a score of 1) to 'extremely concerned' (score of 5).

4.2.1 Hacking

When asked, unprompted, about which privacy and security issue participants were concerned about the most when it comes to their smart locks, hacking was by far the most mentioned concern (N=9), which is in line with prior studies such as [11]. However, although 3 participants expressed extreme concern about hacking, a large portion of the participants were only slightly concerned (N=13) mostly because they don't believe themselves or their houses to be a potential or a high priority target for hackers, which seems to be a common thought process for a lot of homeowners [10, 22].

> **P22:** *"slightly concerned. I recognize that it can happen. But I don't see that our house is being a high priority target. It's not like we're particularly I don't feel like that we would be. I don't foresee us. Basically, security through obscurity is what I'm banking on. I don't see why anyone would want to get into our house specifically."*

4.2.2 Profiling and Information Collection

The majority of participants (n=19) expressed no concern about the smart lock collecting personal information about them and the residents of their home, which is consistent with previous research such as [11]. In fact, some participants appreciated that this sort of information is collected which can help improve the quality of the access logs. Some of those "not concerned" participants also believe that the information the lock collects is not significant and cannot harm them in any way, although when asked about the type of information they think the lock collects, some of them thought the lock only collects their name and email which is not accurate [1]. However, some other participants were more concerned about selling or sharing this information with other parties. P18, who was extremely concerned about sharing their information with third parties, says:

> **P18:** *"Sharing my privacy information with some other third parties is what I think is illegal and I don't feel it will be safe, because I trust that particular company and I don't trust the other."*

Based on the type of information the smart lock collects about its users and the fact that the smart lock also has the capability of sending and receiving information to and from other smart home devices, this creates the possibility of a profiling issue which is a huge privacy risk that most smart home users have to deal with. None of the participants explicitly mentioned "profiling" which could be because they are not familiar with that term or not even familiar with the type of information the smart lock collects and that it can lead to profiling. However, some participants were worried about others knowing the schedule of exactly when they are home and when they are not.

4.2.3 Using and Sharing Access Codes

Seven participants (n=7) expressed concern about the security implications of using or sharing their access codes. For example, two participants were concerned about an adversary observing them or other residents while using their access code to unlock their smart lock, which could allow the adversary to unlock their door later. Other participants (n=3) were more worried about the wear and tear of the keypads or touchpads that come with their smart locks (the most frequently used buttons wear faster than the others). Touchpads can show fingerprints, which can help an adversary figure out the access code based on observing how the keypad or touchpad looks based on which 4 buttons are used the most. Additionally, one participant was concerned about sharing access to the lock with others since they might not take security very seriously and make it easier for someone else to gain unauthorized access.

4.2.4 Physical Tampering with the Lock

The physical security of the smart lock was a concern for some participants (n=3). P5 is concerned about the lock itself being stolen for how expensive it is. Two other participants, on the other hand, were worried about the possibility of a burglar tampering with the lock and being able to gain access to the home. Especially in smart locks that have a physical keyhole as an extra option to unlock the door which can make it susceptible to picking just like traditional locks.

4.2.5 Losing the Smartphone

For a smart lock user, losing their smartphone is equivalent to losing their home key, especially if they do not secure their smartphone with a strong passcode or if they have the auto-unlock feature ON, which allows the lock to unlock itself when the smartphone is within a certain range of the lock without having to unlock the smartphone's passcode. Two participants were concerned that this could happen and an adversary could gain access to their homes. However, most smart locks already give their users the option to log in to their accounts through a website and disable the lost phone to avoid such an issue.

4.2.6 Getting Locked Out

Getting locked out of the home can be a huge security issue especially when it happens late at night or in a dangerous neighborhood. Although only about 28% of the participants (n=8) reported that they were locked out of their homes at least once because of the smart lock, the majority of participants (n=18) showed at least a slight concern that they might get locked out due to a smart lock related issue such as losing connectivity to the internet or a dead battery. Most of those who had already been locked out in the past also mentioned that it was indeed either an internet connectivity problem or a battery related issue.

4.2.7 Log Evasion and Revocation Evasion

Log evasion and revocation evasion affect smart locks that follow a Device-Gateway-Cloud architecture since they mostly rely on WiFi bridges or the user's smartphone to access the internet [13]. Through a companion app on the user's smartphone, these smart locks retrieve the access control list from a remote server, and verify it with the lock through Bluetooth to determine if a particular user is authorized to operate the lock. Unless the user's phone is connected to the internet or a WiFi bridge is available, the lock cannot retrieve the most recent access control list. As a result, even if user X's access to the smart lock was recently revoked, they can still operate the lock until the lock can connect to the internet and update the access control list. This is called revocation evasion which

Pre-Video (μ, σ)	Post-Video (μ, σ)	Z-value	P-value
Log Evasion Threat			
(1.72, 0.882)	(2.24, 1.354)	-2.334	0.020
Revocation Evasion			
(1.79, 1.114)	(2.21, 1.320)	-1.530	0.126

Table 3: The mean and standard deviation for the participants' level of concern regarding state consistency attacks in smart locks before and after watching the demonstration video.

is the first type of state consistency attacks. Likewise, a legitimate user, who has authorization to operate the lock, can also avoid appearing in the access logs simply by turning off their smartphone's internet connection. This is the second type of state consistency attack (evasion of access logs).

Although state consistency attacks have been heavily discussed in the literature [13, 16, 19, 25], only 3 participants stated that they were aware of the revocation evasion issue within smart locks while only 2 participants were aware of the log evasion issue. Users tend to be less concerned about security issues they are not familiar with. To give participants an overall understanding of the issues and how they can occur, we prepared a video demonstrating two types of state consistency attacks on one of the most popular smart locks on the market. We first asked the participants, on a scale of 1 to 5, how concerned they were regarding each of the two issues before watching the video and then again after watching the video towards the end of the interview. Our aim was to examine how raising the level of awareness of security threats affects users' level of concern about those threats.

The results showed an increase in the level of user concern regarding both of the security issues after watching the video as illustrated in Figure 1a and table 3. In order to determine whether statistically significant differences exist between the participants' level of concern before and after watching the video of the two security issues, a Wilcoxon Signed Ranks Test was performed. The tests revealed a statistically significant difference in the participants' level of concern in regards to log evasion (Z= -2.334, p=0.020, α= 0.05). However, The tests did not reveal a statistically significant difference in the participants' level of concern in regards to revocation evasion (Z= -1.530, p=0.126, α= 0.05). The reason behind this is that the participants were already more concerned about the possibility of revocation evasion compared to the possibility of log evasion even before knowing that the issues do exist. Therefore, although the participants' level of concern has mostly increased towards both issues after watching the video, it was more noticeable for log evasion.

After watching the video demonstration, most of the participants believed both issues to be very serious. However, they considered revocation evasion to be more serious compared to log evasion ($\bar{x} = 3.90$ and $\bar{x} = 3.49$, respectively). Referring to the revocation evasion problem, P13 says:

> **P13:** *"Extremely serious. That can really make or break someone's life extremely, especially with stalkers and domestic violence issues. I'm just trying to think about all the issues that someone has changed their locks because of some type of danger or harm that they felt that they might have been in to revoke someone's access into their home. So that person can still access their home, when they are not on Wi-Fi. That's scary."*

Furthermore, we asked the participants if they would switch back to traditional locks if they found that their smart locks had either of those problems. For both the revocation evasion and the log evasion issues, most participants (n=19 and n=23 respectively), stated that they would NOT go back to using a traditional lock. Some participants explained how they would buy a different smart lock instead of going back to a traditional lock because they appreciate the features that a smart lock offers. However, most of them stated that now that they know about those issues, they will make sure to test their smart locks and be more careful about which smart lock they buy in the future and who they share access to their locks with.

4.3 Reasons for the Lack of Concern

Using Mitigation Strategies Some participants mentioned that having added layers of security such as using a video doorbell or installing an alarm system on their smart locks was a factor that increased their trust in their smart locks and made them less concerned about possible security and privacy issues related to the smart locks.

Trusting Other Users Most of the participants who did not seem very concerned about most security issues related to smart locks stated that they only share access to their smart locks with people they absolutely trust and are not expecting any of these individuals to actively invade their privacy or compromise their security.

Trusting the Manufacturer The manufacturer's security and privacy policies play a crucial role in protecting the integrity and confidentiality of the data that is transferred from the end user to the manufacturer. Similar to previous research [22], Some participants stated that they trust the manufacturer to not sell or share their data with other third parties as well as keep their data secure on the cloud against any hacking attempts.

Everything about me is Already Out There! Some participants stated that their lack of concern with some privacy and security issues related to smart locks is due to the fact that their personal information is already on the internet one way or another and has already been sold to advertising agencies by other applications and services that they used in the past.

Therefore, they were not greatly concerned about their smart locks sharing personal information with other parties.

My House is not a Target! The participants were mostly aware of the fact that smart locks are susceptible to hacking. However, some of them did not show any concern regarding the possibility of hacking mainly because they were under the impression that hackers would have no interest in compromising their smart locks and gaining access to their homes.

4.4 Mitigation Strategies

Despite the fact that some participants showed concerns related to the security and privacy of smart locks, they also made it clear how convenient it is to use the smart lock and enjoy the added features compared to its counterpart the traditional lock especially when its counterpart also has its own security and privacy issues. However, the participants reported that they tend to use specific protective measures and mitigation strategies to cope with those concerns and improve the security of their smart locks without losing the convenience factor of using a smart lock (RQ3).

4.4.1 Adding Another Layer of Security

When asked if they use any other devices or gadgets to increase the security and privacy of their smart locks, most participants (n=25) stated that they do. The majority of those (n=24) have a video doorbell installed, which records everything that happens around the area where the smart lock is installed. In addition, it allows users to see who is actually at the door before unlocking it. The second most commonly used device to improve the security of smart locks was a chain guard or a swing guard (n=4), which is a small device that, when engaged, can be installed on the door and door frame to make it harder for an intruder to access the home even if they managed to get the smart lock to unlock. Two participants (n=2) also installed a secondary lock on the door, so that even if the smart lock was unlocked, the intruder would still have trouble getting in. Several participants (n=2) reported that their home had a security system that could alert them in case of a break-in. Those systems usually require the user to input a passcode every time they get through the front/back to stop the alarm from going off.

However, we asked the participants if they would still feel safe with the smart lock if those other security layers were not installed. To our surprise, 21 participants said they would, indicating either that they are confident in the security features of smart locks or that they do not consider their homes a target for intruders.

4.4.2 Configuring the Network

Some participants (n=3) suggested improving the security of the network that the smart lock connects to as a solution to concerns related to hacking and remote manipulation of the lock.

> **P12:** *"My biggest concern was the connectivity to the internet and, obviously, the ability that someone else may have to access the lock remotely, or gain access to the code or anything of that nature. I've kind of mitigated that by using Bluetooth instead of connecting it directly to wireless. And then when it's connected on my phone through Bluetooth, I actually have a separate wireless network that I'm connected to the separate VLAN so that anytime I'm connected to that device, it's not on the center VLAN that I use to surf the web and stuff like that."*

We hypothesized that improving authentication through using Multi-factor Authentication (MFA) would be something that at least some participants might mention as a possible mitigation strategy but when asked unprompted, none of the participants mentioned it. For this reason, we asked the participants if the applications they use to control their smart locks support MFA. About half of the participants (n=14) stated that their application does offer it, while 10 participants stated that they don't have this feature and 3 other participants did not know if they had it or not.

For the 14 participants who had access to MFA, 10 of them had it in the form of a One-Time-Password (OTP) that is sent to their phone or email when they log in from a new device, 5 participants have it in the form of a PIN, fingerprint, or face ID, that is required every time they use the companion application, and 1 participant had it in the form of a confirmation from an already logged in person. However, only one person out of the 14 participants who have the MFA feature stated that they use it frequently (in the form of a PIN, fingerprint, or face ID) while the others either don't use it or are required to use it every time they log in from a new device.

4.4.3 Managing Access Codes Carefully

Some participants (n=3) stated that they choose to manage access codes more carefully and put some regulations in place when it comes to creating and sharing access codes. This includes things like changing the access codes frequently and giving access only to a limited number of people who absolutely need it. Moreover, the companion applications used to control smart locks are usually reliable when it comes to sending out notifications of every interaction with the lock in real time to the homeowner as well as keeping an access log that records every interaction with the lock along with other information such as who interacted with the lock, when, and how. Some participants (n=2) said that this has been very effective for them when it comes to dealing with their security concerns since they can always be notified of who is using the lock so they can confirm whether it was a person they recognize or not and can react to the situation accordingly.

4.4.4 Maintaining the Keypad/touchpad

As mentioned in the previous section, smart locks that are equipped with a touchpad/keypad have their own security issues especially when it comes to the wear and tear of the buttons and the touch screen itself. Participants (n=2) who have this sort of smart locks take some protective measures to deal with those possible security risks such as covering the touchpad/keypad with a plastic wrap so that it does not wear down as quickly as well as wiping off any fingerprints that it might catch after each use.

4.5 The Security of Smart Locks Compared to Traditional Locks

When asked whether it made them feel safer having a smart lock installed in their home compared to having a traditional lock, the majority of participants (n=19) said that it did. According to the participants, having features such as the ability to remotely lock the door, get security notifications, restrict others access time, and the ability to use the auto-lock feature made them feel that their home is secure even when they are away from home. However, other participants (n=10) did not necessarily feel more secure with the smart lock, but they appreciate its convenience. Some of them even felt less secure for various reasons such as the possibility of getting hacked, and the fact that others can see them as they type in their access codes and might be able to use that access code in the future.

4.6 Security and Privacy Improvements

In this section we report and discuss the participants' insights regarding how the smart lock's design and functionality can be altered in a way that enhances its overall security and privacy (RQ4).

4.6.1 Built-in Camera

Most commercially available smart locks don't have a built-in camera, but some of them can be easily integrated with other commercially available video doorbells. However, some participants (n=6) believe that having the doorbell camera already built-in can save the user money and time spent to integrate the two which sometimes might not even allow the user to use the full capabilities of both devices. Moreover, some participants lack the technological background to connect the two devices together. In fact, some participants (n=8) have both devices but do not have them connected due to different reasons such as not knowing how to connect them or the fact that they are not compatible in the first place. In terms of security, a built-in camera allows the users to see a video of who is interacting with the lock in real time as well as knowing exactly who is at the door before letting them in.

4.6.2 Improve Authentication

Some participants (n=6) believe that the authentication process within smart locks can be improved to increase the overall security of smart locks. According to the participants, they would feel more secure if instead of using an access code or a button on the companion application to authenticate, they would be able to use a more secure method such as face recognition or fingerprint (which is already available on some smart locks but not the most popular ones). However, some of participants also liked the idea of using Multi-factor Authentication (MFA) to improve the authentication process for logging into the companion application which was discussed at some point during the interview. Most of them were not familiar with the concept of MFA before the interview.

4.6.3 More Data Transparency

In line with previous work [27], several participants (n=5) believe that the manufacturer needs to be more transparent when it comes to explaining how the customer data is being used, who it's shared with, and how much of the user's information is shared.

> **P12:** *"I would say that it would be easier to have a little bit of better visibility into how your data is being used. It's not so transparent as to how your data is being used from third parties or from the company itself."*

4.6.4 Improving the Physical Security of the Lock

Two participants stated that the smart lock is not physically secure and could use some improvements in that aspect. This can be accomplished by implementing an intrusion detection system or a tamper detection system with specific sensors that can detect any tampering with the lock, attempts to break it, or hitting it with a strong force.

4.7 Limitations

Like many interview-based studies, our convenience sample size was limited and might not wholly reflect the broader population. Our recruitment efforts were predominantly focused on university students and employees, which confined us in terms of geographical diversity and the educational level of our participants. Therefore, nearly all our participants were from the United States with a generally high educational background. We attempted to address this lack of diversity by promoting the study on Reddit forums. However, our attempt was hindered by the fact that most of the responses to the screening survey posted on Reddit came from bot accounts or were instances of a single person submitting multiple surveys. We identified this anomaly thanks to the data analysis and insights provided by the survey platform we utilized, Qualtrics.

5 Discussion

In this section, we will discuss some of the key takeaways from our study as well as discuss implications and recommendations for researchers and smart lock designers.

Smart Lock Adoption Our study revealed that most participants chose to adopt a smart lock mainly because the features that the smart lock offers make it more convenient compared to a traditional lock. This, however, contradicts with a prior study that aimed to explore the key factors affecting smart lock adoption in which improving the security and safety of the home was the most important factor that influenced the participants intention to adopt a smart lock [17]. This contradiction can be due to the different backgrounds or demographics of the participants in the two studies. Another reason could be the fact the participants in our study have had at least 2 months of experience using the smart lock before the interview, while the participants in the study conducted by Mamonov et al. hadn't adopted the smart lock at that point in time.

Convenience Over Security Although several participants expressed their concerns about privacy and security issues related to smart locks, most of them believed that the convenience of using the smart lock outweighs its security flaws. After all, its counterpart, the traditional lock, is not necessarily flawless in terms of security since it's susceptible to picking and tampering. However, several participants did not seem to be extremely concerned about the security drawbacks of the smart lock. Some of these participants were not aware of the possible security threats while others trust the mitigation strategies they put in place to increase the privacy and security of the lock and the smart home in general.

Unique Security Concerns and Mitigation Strategies Our findings revealed security concerns and mitigation strategies unique to smart locks which have not been discussed in prior studies that aimed to investigate the security and privacy concerns and mitigation strategies related to smart home devices in general. For example, some participants in our study expressed concerns regarding shoulder surfing attacks or the fact that attackers might be able to figure out the smart lock's correct access code based on which keys on the keypad are more worn due to being pressed more frequently. These sorts of concerns also introduced mitigation strategies that are more unique to smart locks such as maintaining the keypad/touchpad more regularly and managing access codes more carefully. Furthermore, some participants were also concerned about the possibility of losing their smartphone which would be equivalent to losing their key to the house, while other participants showed concerns regarding the possibility of getting locked out of their homes due to internet connection or battery related issues with the smart lock. While it's possible to mitigate some of the security concerns regarding most smart home devices by installing the device in a different location within the house, or turning the device off for a specific amount of time [22, 29], this is not applicable in the case of smart locks due to obvious reasons. However, our findings show that using an extra layer of security is the main mitigation strategy used by smart lock users to deal with their privacy and security concerns. For most participants, this extra layer of security was a video doorbell due to the fact that video doorbells are usually installed near the smart lock which provides the user with a clear view of what is happening around the lock and who is trying to interact with it.

The Trust Factor The lack of concern that some participants showed when answering questions related to security and privacy concerns was sometimes due to them having trust either in the other users, the manufacturer, or the security company that installed the smart lock [10, 29]. Having complete trust to the point of neglecting security vulnerabilities could be detrimental to the security of the entire home. For example, one participant mentioned that they do not check access logs because they trust all the other lock users. However, checking the access logs does not necessarily mean a lack of trust, but simply allows the lock owner to verify that only those who should have access to the lock actually do.

Sharing Electronic Keys The security of the smart lock and therefore that of the entire household, since compromising the smart lock can lead to unauthorized access to the home, is largely dependent on how safely the access codes and electronic keys are being managed. Carefully assigning access codes and electronic keys along with choosing the right access type for each person that uses the lock is extremely critical. For that reason, almost half of the participants chose to only give access to those who live in the house while the other participants, who gave access to non-residents, try to carefully choose the access level based on who needs access to the home, when, and why.

5.1 Implications and Recommendations

5.1.1 Design and Functionality Improvements

Access Control Management Currently, the majority of smart locks implement a Role-based Access Control (RBAC) management system with 4 access levels: owner, resident, recurring guest, and temporary guest [13]. Each of the four access levels has specific access rights associated with it and the only two factors that the homeowner can manipulate when giving access to another user are the date and time (for the recurring guest and temporary guest access levels). However, more than half of the participants (n=16) stated that they share access to their smart locks with other users who don't live inside the house such as a babysitter, a pet walker, or a contractor. To improve the privacy and security of those who live inside the house, it's imperative to enable the homeowner to create more granular access control policies taking into account other environmental and contextual factors. For example, a homeowner might want the contractor to be able to use their access code only if no one is home to ensure the privacy of the home residents. Moreover, even when considering giving access to residents, prior studies, such as the study conducted by He et al., have proved that smart home users prefer to give access based on capability rather than device which also supports the need for more granular access control policies [12].

Video Doorbell Integration The fact that over 82% of the participants have a video doorbell installed next to their smart lock gives us an indication of how well these two devices complete each other and using them together can greatly improve the security and privacy of the household. However, many participants stated that although they have both devices, they don't necessarily have them connected either because they are not compatible, or because the user lacks the knowledge of how to connect them to get the most out of the two devices. We recommend, as well as many participants, that smart locks either have cameras already built-in or at least support seamless integration with other video doorbells in the market. The integration process needs to be simple with a clear and concise video tutorial to make it easier for those who are technically challenged to connect the two devices and get the added security and usability features.

Battery Many participants showed some concern regarding the battery life of the smart lock. Once the battery starts depleting, the lock becomes slower in responsiveness and sometimes does not even lock properly since it lacks the needed torque to properly lock the door. Prior work has indicated that smart locks suffer from sitting idle during extended periods of the day as well as having additional high peak current demands compared to other smart home devices [8]. Therefore, they require better power management in order to improve their battery life. Improving the battery life should be a priority along with increasing the frequency of battery level warnings that show on the user's smartphone before the lock gets to the stage where it struggles to unlock properly and not only when the battery is about to die completely.

5.1.2 Increasing Awareness

Our study shows that there is a general lack of awareness when it comes to security and privacy issues that the smart lock might be susceptible to. The lack of awareness often leads to lack of concern which can stop the smart lock user from implementing the correct protective measures and following the proper security practices to keep the lock secure. Therefore, more work needs to be done to educate the smart lock's user base about the possible security flaws and vulnerabilities. Our results show that the big majority of participants were not aware of state consistency attacks that some smart locks are susceptible to. Making them aware of those issues, however, has proved to increase the level of concern for some participants.

5.1.3 Transparency in Data Collection and Sharing

Our results revealed that the participants' level of concern regarding sharing their personal information with other parties is almost as high as the level of concern regarding hacking (Figure 2b). Therefore, it's imperative to give the users more control over what data is collected through the smart lock as well as more transparency about who gets access to such data. One way to improve the transparency in data collection and sharing is through adding more privacy controls and improving how privacy policies are displayed to the end user in a way that accommodates for users of different education levels, languages, and ages.

6 Conclusion

Given the continuous increase in the market size of smart locks year after year all over the world and the role smart locks play in maintaining the security and privacy of the household, more and more research needs to be done in order to improve the design and functionalities of smart locks. There have been numerous research papers published in the past discussing the security and privacy of smart locks from the perspective of the researchers, but little work has been done on the security and privacy of smart locks from the perspective of the end users. In this study, we focus on the end user's perspective of different aspects of the smart lock. We start our interviews by investigating the usage behaviors of smart locks' end users. We learned that big portion of smart lock users tend to share access to the lock with others who don't live in the house which justifies the need for improved access control policies. Our study also revealed that the convenience of smart locks was the number one factor in adopting a smart lock. The study also shows a lack of concern, as well as a lack of awareness, regarding some smart lock security and privacy threats.

Acknowledgments

We are extremely thankful to all the participants for their insights, time, and cooperation.

References

[1] August smart locks privacy policy | keeping your home & data locked down.

[2] Chaitanya Bapat, Ganesh Baleri, Shivani Inamdar, and Anant V Nimkar. Smart-lock security re-engineered using cryptography and steganography. In *International Symposium on Security in Computing and Communication*, pages 325–336. Springer, 2017.

[3] SANNE BJARTMAR HYLTA and PETRA SÖDERBERG. Smart locks for smart customers?: A study of the diffusion of smart locks in an urban area, 2017.

[4] Aykut Coskun, Gül Kaner, and İdil Bostan. Is smart home a necessity or a fantasy for the mainstream user? a study on users' expectations of smart household appliances. *International Journal of Design*, 12(1):7–20, 2018.

[5] Lucas de Camargo Silva, Mayra Samaniego, and Ralph Deters. Iot and blockchain for smart locks. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0262–0269. IEEE, 2019.

[6] Luis Carlos Rubino de Oliveira, Andrew May, Val Mitchell, Mike Coleman, Tom Kane, and Steven Firth. Pre-installation challenges: classifying barriers to the introduction of smart home technology. In *EnviroInfo and ICT for Sustainability 2015*, pages 117–125. Atlantis Press, 2015.

[7] Christine Geeng and Franziska Roesner. Who's in control? interactions in multi-user smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[8] Chris Glaser and Aramis P Alvarez. Extending battery life in smart e-locks.

[9] Julie Haney, Susanne M Furman, Mary Theofanos, Yasemin Acar Fahl, et al. Perceptions of smart home privacy and security responsibility, concerns, and mitigations. 2019.

[10] Julie M Haney, Yasemin Acar, and Susanne Furman. " it's the company, the government, you and i": User perceptions of responsibility for smart home privacy and security. In *USENIX Security Symposium*, pages 411–428, 2021.

[11] Julie M Haney, Susanne M Furman, and Yasemin Acar. Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In *International Conference on Human-Computer Interaction*, pages 393–411. Springer, 2020.

[12] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (iot). In *USENIX Security Symposium*, pages 255–272, 2018.

[13] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security*, pages 461–472, 2016.

[14] S Jahnavi and C Nandini. Smart anti-theft door locking system. In *2019 1st International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE)*, pages 205–208. IEEE, 2019.

[15] Federica Laricchia. Global smart lock market size 2016-2027, Feb 2022.

[16] Yonglei Liu, Kun Hao, Jie Zhao, Li Wang, and Weilong Zhang. A novel smart lock protocol based on group signature. *International Journal of Network Security*, 24(1):130–139, 2022.

[17] Stanislav Mamonov and Raquel Benbunan-Fich. Unlocking the smart home: exploring key factors affecting the smart lock adoption intention. *Information Technology & People*, 34(2):835–861, 2020.

[18] Lili Nemec Zlatolas, Nataša Feher, and Marko Hölbl. Security perception of iot devices in smart homes. *Journal of Cybersecurity and Privacy*, 2(1):65–73, 2022.

[19] Saiprasanna Palle. *Smart Locks: Exploring Security Breaches and Access Extensions*. PhD thesis, Oklahoma State University, 2017.

[20] Varad Pandit, Prathamesh Majgaonkar, Pratik Meher, Shashank Sapaliga, and Sachin Bojewar. Intelligent security lock. In *2017 international conference on trends in electronics and informatics (ICEI)*, pages 713–716. IEEE, 2017.

[21] Bhagyesh Patil, Parjanya Vyas, and RK Shyamasundar. Secsmartlock: An architecture and protocol for designing secure smart locks. In *International Conference on Information Systems Security*, pages 24–43. Springer, 2018.

[22] Madiha Tabassum, Tomasz Kosinski, and Heather Richter Lipford. " i don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 435–450, 2019.

[23] Madiha Tabassum and Heather Lipford. Exploring privacy implications of awareness and control mechanisms in smart home devices. *Proceedings on Privacy Enhancing Technologies*, 1:571–588, 2023.

[24] Blase Ur, Jaeyeon Jung, and Stuart Schechter. Intruders versus intrusiveness: teens' and parents' perspectives on home-entryway surveillance. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 129–139, 2014.

[25] Arvid Viderberg. Security evaluation of smart door locks, 2019.

[26] Zhenghao Xin, Liang Liu, and Gerhard Hancke. Aacs: Attribute-based access control mechanism for smart locks. *Symmetry*, 12(6):1050, 2020.

[27] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 chi conference on human factors in computing systems*, pages 1–12, 2019.

[28] Mengmei Ye, Nan Jiang, Hao Yang, and Qiben Yan. Security analysis of internet-of-things: A case study of august smart lock. In *2017 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*, pages 499–504. IEEE, 2017.

[29] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, 2017.

[30] Eric Zeng and Franziska Roesner. Understanding and improving security and privacy in {Multi-User} smart homes: A design exploration and {In-Home} user study. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 159–176, 2019.

[31] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home iot privacy. *Proceedings of the ACM on human-computer interaction*, 2(CSCW):1–20, 2018.

A APPENDICES

A.1 Screening Survey

- What is your first name?
- What is your email address?
- What age group do you belong to?
- What is your gender?
- What is your level of education?
- What is your current occupation?
- How many smart locks do you have installed where you live?
- Which smart lock(s) do you have installed where you live?
- Who installed the lock(s)?
- How long have you been using it (them)?
- How does your smart lock connect to the internet?
- How many people do you share access to the lock(s) with?
- Which virtual meeting platform do you prefer for conducting the interview?

A.2 Interview Questions

A.2.1 Smart Locks Usability

- What made you move from using a traditional lock to using a smart lock?
- Did you hesitate before making the move from using traditional locks to smart locks? Why?
- Do you have your smart lock connected to your video doorbell? Why?
- What would you say the top features of your smart lock that you mostly use?
- Who else can operate the smart lock, and what are their access levels?
- How easy do you find it to share keys with others? And how reliable?
- How easy do you find it to revoke other people's keys? And how reliable?
- Do you have notifications turned on for your smart lock app? Why?
- Do you connect your smart lock to other smart devices in your home using services like IFTTT? If yes, please talk more about the scenarios you have set up?
- Which aspects of the smart lock do you dislike or wish they would have been implemented differently?

- Compared to a traditional lock, how do you rate the locking/unlocking experience using a smart lock?
- In terms of locking/unlocking the door, how reliable is the smart lock compared to a traditional lock?
- How often do you find yourself checking the smart lock app on your phone to see if your door is locked/unlocked? (never, seldom, sometimes, frequently, always)
- How often do you find yourself checking the smart lock app on your phone to see the access logs? (never, seldom, sometimes, frequently, always)
- How often do you use your smart lock's auto lock feature? (never, seldom, sometimes, frequently, always)
- How often do you use your smart lock's auto unlock feature? (never, seldom, sometimes, frequently, always)
- How often do you control your smart lock using voice commands? (never, seldom, sometimes, frequently, always)
- Can you think of more features that you would like smart locks to have?

A.2.2 Privacy and Security Concerns Related to Smart Locks:

- What security or privacy related concerns do you have with your smart lock? How do you mitigate (deal with) those concerns?
- How concerned are you that your smart lock may malfunction and lock you out one day? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- Has the smart lock ever locked you out of your home by accident? What was the reason?
- Would having a smart lock installed in your home make you feel safer compared to having a conventional lock? Why?
- How concerned are you that your smart lock might store your personal information and know your location at all times? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that the smart lock will keep a log of every time the lock is used along with the information of the person who used it? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that your smart lock might give others (such as your landlord) information about when you or your family members are home and when you are not? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that data collected by your smart lock might be shared with other parties? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that your smart lock might be hacked which allows unauthorized access to your home? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that the key revocation process might not be working correctly which allows others whose keys you have revoked to still have access to your home? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- How concerned are you that some locking/unlocking activities might not appear on the smart lock's access logs? (not concerned, slightly concerned, concerned, very concerned, extremely concerned)
- What other security or privacy related concerns do you have with your smart lock?
- Do you use any other gadgets/ devices to increase the security of your smart lock?
- Does the app you use to control the smart lock allow you to use multi-factor authentication (MFA)? If yes, what form of MFA does the app offer? and how often do you use it?
- Do you think the companies that manufacture smart locks should add more features to make them more secure and increase the user's privacy? Could you give examples of such features?
- What other concerns do you have in regards to smart locks security and privacy?

A.2.3 Security Awareness

Each question listed below was asked twice, once for the revocation evasion security issue and another time for the log evasion security issue

- Did you already know that this issue existed?
- On a scale of 1 to 5, how serious do you think this issue is?
- On a scale of 1 to 5, how concerned are you that your smart lock might be affected by this issue?

- Would this issue cause you to go back to using a traditional lock instead of a smart lock?

A.3 Codebook

Code	Description
Motivation for adoption: Security	The core motivation to adopt a smart lock is to improve the security of the household
Motivation for adoption: Convenience	The core motivation to adopt a smart lock is to improve the convenience level within the home
Motivation for adoption: Did not personally install it	The user did not make the decision of purchasing and installing the smart lock (e.g., required by the landlord)
Motivation for adoption: Based on a recommendation	The user was motivated to adopt a smart lock based on a recommendation from other smart lock users
Hesitation to adopt: Price	The user hesitated before purchasing a smart lock because of its price
Hesitation to adopt: Security concerns	The user hesitated before purchasing a smart lock because of security or privacy concerns
Hesitation to adopt: Overwhelmed by the options	The user hesitated before purchasing a smart lock due to being overwhelmed by the different options on the market
Hesitation to adopt: Concerned about setup difficulties	The user hesitated before purchasing a smart lock because of concerns regarding the level of difficulty associated with its installation or setup
Most used features: Remote control	The user frequently locks and unlocks the door remotely
Most used features: Keyless entry	The user frequently unlocks the door without the need for a physical key
Most used features: Granting electronic keys	The user frequently grants access to other users electronically through the lock's companion application
Most used features: Remote status check	The user frequently checks the status of the lock to ensure that it's locked or unlocked
Most used features: Various unlocking options	The user unlocks the door through different methods such as using an access code, through the companion application, or using a fingerprint
Most used features: Auto-lock	The user configures the lock to automatically lock itself within a specific amount of time after being unlocked

Notifications on: Deadbolt Jammed	The user keeps the notifications on in order to get alerts when the deadbolt jams
Notifications on: Usage information	The user keeps the notifications on in order to get alerts about who is interacting with the smart lock, and when
Notifications on: Security alerts	The user keeps the notifications on in order to get security alerts such as the use of invalid access codes
Notifications on: Battery alerts	The user keeps the notifications on in order to get updates on the smart lock's battery level
Notifications off: Don't prefer using the companion application	The user does not get smart lock notifications because they don't prefer to use the companion application
Notifications off: Notifications can be annoying	The user turns the notifications off because they consider them to be annoying
Notifications off: Invasion of other residents' privacy	The user turns the notifications off to avoid invading the privacy of other home residents
Notifications off: Someone is always home	The user turns he notifications off because someone is always present at the house
Difficulty sharing access: Difficult for older or technologically challenged individuals	The user finds the process of sharing access to the smart lock to be difficult especially for older or technologically challenged individuals
Difficulty sharing access: All users must download the app	The user finds the process of sharing access to the smart lock to be difficult due to the fact that all the users need to download and configure the lock's companion application
Difficulty sharing access: Too many steps	The user finds the process of sharing access to the smart lock to be difficult due to the many steps the user needs to go through in order to grant the access
Access sharing patterns: Only share access with home residents	The user only shares access to the smart lock with those who live inside the house
Access sharing patterns: Share access with residents and non-residents	The user shares access to the smart lock with those who live inside the house as well as others who don't live inside the house
Usability improvements: Battery improvement	Improvements related to the smart lock's battery
Usability improvements: Smart watch integration	Allowing for a better integration between smart watches and smart locks
Privacy & security concerns: Hacking	Concerns about the possibility of hackers remotely manipulating the smart lock or gaining access to personal information
Privacy & security concerns: Shoulder surfing	Concerns about the possibility of others observing the user as he/she is using the access code to unlock the door
Privacy & security concerns: The wear and tear of keypads/touchpads	Concerns about the wear and tear of the most frequently used keys on the keypad/touchpad
Privacy & security concerns: Profiling	Concerns about other users or third parties obtaining information about who would be in the house (or not in the house) and when
Privacy & security concerns: Physical tampering with the lock	Concerns about physical tampering with the smart lock
Privacy & security concerns: Losing the smartphone	Concerns about a lost or stolen smartphone that can be used to operate the smart lock
Privacy & security concerns: Getting locked-out	Concerns about getting locked-out of the house
Privacy & security concerns: Revocation evasion	Concerns regarding the possibility that a revoked access might not be successfully revoked
Reasons for getting locked-out: Dead battery	The participant was locked out in the past due to a dead battery
Reasons for getting locked-out: Network or power issues	The participant was locked out in the past due to issues regarding the internet or a power outage

Reasons for getting locked-out: Auto-lock feature	The participant was locked out in the past due to the lock automatically locking itself while the phone is inside the house
Reasons for the lack of security concern: Using mitigation strategies	The user has showed a low level of concern about a possible security or privacy issue mainly due to them using a mitigation strategy to deal with possible threats
Reasons for the lack of security concern: Trusting other users	The user has showed a low level of concern about a possible security or privacy issue mainly due to having trust in other authorized users
Reasons for the lack of security concern: Trusting the manufacturer	The user has showed a low level of concern about a possible security or privacy issue mainly due to having trust in the security configurations the manufacturer has put in place
Reasons for the lack of security concern: Everything about me is already out there!	The user has showed a low level of concern about a possible security or privacy issue mainly because some of their personal information is already available to third parties
Reasons for the lack of security concern: My house is not a target!	The user has showed a low level of concern about a possible security or privacy issue mainly because they don't believe their house to be a target for hackers
Mitigation strategies: Adding another layer of security	The user installs other additional devices to increase the security of the home in case the smart lock is compromised
Mitigation strategies: Configuring the network	The user configures the network to improve the security of the smart lock
Mitigation strategies: Managing access codes carefully	The user creates and shares access codes carefully
Mitigation strategies: Maintaining the keypad/touchpad	The user maintains the keypad/touchpad so that it doesn't show more signs of wear and tear on the most frequently used keys
Security and privacy improvements: Built-in camera	Integrating a built-in camera can improve the security and privacy of the lock
Security and privacy improvements: Improve authentication	Implementing different authentication approaches can improve the security of the lock
Security and privacy improvements: More data transparency	More transparency about data collection and sharing would improve the users' privacy
Security and privacy improvements: Improving the physical security of the lock	Improving the physical security of the smart lock would improve the security of the overall security of the smart home

A.4 Demographics

Table A.1: Study participants demographic information

Participant	Gender	Age group	Education	Time spent using the smart lock	Connection to the internet
P1	Female	18-25	Bachelor’s	More than 4 months	Directly (has a built in Wi-Fi)
P2	Male	26-35	Graduate student	More than 4 months	Wi-Fi hub (bridge)
P3	Female	26-35	Bachelor’s	2-4 months	Wi-Fi hub (bridge)
P4	Male	26-35	Masters	More than 4 months	Not sure
P5	Male	26-35	Bachelor’s	2-4 months	Wi-Fi hub (bridge)
P6	Female	18-25	-	More than 4 months	Directly (has a built in Wi-Fi)
P7	Male	26-35	Bachelor’s	More than 4 months	Wi-Fi hub (bridge)
P8	Male	26-35	Bachelor’s	More than 4 months	Directly (has a built in Wi-Fi)
P9	Female	26-35	Masters	More than 4 months	Directly (has a built in Wi-Fi)
P10	Female	26-35	Some college	More than 4 months	Wi-Fi hub (bridge)
P11	Female	36-50	Graduate degree	2-4 months	Not sure
P12	Male	26-35	Master’s degree	More than 4 months	Smartphone’s internet connection
P13	Female	26-35	Some college	More than 4 months	Not sure
P14	Female	26-35	Some college	More than 4 months	Not sure
P15	Female	18-25	Some college	2-4 months	Wi-Fi hub (bridge)
P16	Female	26-35	Some college	2-4 months	Directly (has a built in Wi-Fi)
P17	Female	18-25	Some college	More than 4 months	Not sure
P18	Female	18-25	Grad student	More than 4 months	Not sure
P19	Female	26-35	Grad student	More than 4 months	Not sure
P20	Male	36-50	Masters	More than 4 months	Wi-Fi hub (bridge)
P21	Female	18-25	Some college	More than 4 months	Directly (has a built in Wi-Fi)
P22	Male	26-35	Some college	More than 4 months	Not sure
P23	Male	36-50	PhD	2-4 months	Wi-Fi hub (bridge)
P24	Female	26-35	Master’s	More than 4 months	Wi-Fi hub (bridge)
P25	Female	18-25	Some college	More than 4 months	Smartphone’s internet connection
P26	Female	18-25	Some college	More than 4 months	Not sure
P27	Female	26-35	Associate degree	More than 4 months	Directly (has a built in Wi-Fi)
P28	Female	26-35	Grad student	More than 4 months	Wi-Fi hub (bridge)
P29	Male	18-25	Some college	More than 4 months	Directly (has a built in Wi-Fi)