Bachelor Degree Project

Smart locks: User perception on security vs convenience

Author: Oliver Berglöf, Hampus Brunzell
Supervisor: Arianit Kurti
Examiner: Ola Flygt
Semester: VT2023
Subject: Computer Science

Abstract

This thesis aims to find out trade-offs between security, privacy and convenience when it comes to smart locks. If users know about security and privacy risks associated with smart locks and how they perceive the trade-offs, if they think that the security and privacy risks are worth it for some added convenience. In this project both a literature review and online survey was used to gather information. The results are that there are conveniences with smart locks but that they come with potential security and privacy risks. That overall users seems to know that there are potential security and privacy risks and users seem to think that any potential security and privacy risks are worth taking for the sake of convince.

Keywords: Smart lock, security, privacy, convenience

Preface

We extend our gratitude to our supervisor, Arianit Kurti, for his invaluable guidance and support throughout the thesis. His expertise and constructive feedback have greatly contributed to the quality of our research. We appreciate his dedication to our academic development and are thankful for the opportunity to have worked under his supervision. We would also like to thank all those who have participated in the survey. Finally we would like to thank our program coordinator Ola Flygt who has given us very much knowledge and understanding for cybersecurity and computer science. Without all these people this would not have been possible.

Contents

1 Introduction

With the smart home market growing, security aspects surrounding them are becoming more relevant and people are becoming more aware and concerned about their security and privacy. [1].

This is a 15 HEC bachelor's thesis in Computer science about the security vs the convenience of smart locks. This work has been done as a pair. We have worked together on everything but Hampus Brunzell has taken responsibility for sections 1, 2, 5, 7 and Oliver Berglöf has taken responsibility for sections 3, 4, 6. We will be investigating the security of the smart locks today to see if they are secure, and then we will look at the benefit of having a smart lock to see if the potential attack vectors outweigh the convenience benefits it gives.

The security of the smart locks will be investigated through a literature review of earlier reports on the security of smart locks. Earlier work on this has been done and will be shown more in the related work section. A survey will be conducted to determine users perception on security, privacy and security when it comes to smart locks.

1.1 Background

According to market research, the smart home market, which includes smart home security devices, is steadily growing and is expected to grow by 27% until 2030 compared to 2020 [2]. Among these devices are smart locks, which replace traditional deadbolt locks with technology. These technologies offer added features such as opening the door through a pin or tag, remote control, and the ability to monitor who is home and at what times. These additional features may also increase the vulnerability of the lock to potential attacks.

Given that smart locks are designed to replace traditional deadbolt locks and are responsible for home security, it is critical that they are secure. This investigation will assess whether the convenience offered by smart locks is worth the trade off in security. The issue of privacy is also pertinent, as smart locks can track the presence of occupants in the home, and this aspect will be considered in evaluating whether the convenience of smart locks justifies the associated security and privacy risks.

A lock can be considered a smart lock if it is an electromechanical device that can unlock/lock wirelessly [3]. However for this thesis we consider a smart lock to be a lock that is connected to the internet. Most smart locks can be controlled through a mobile app, voice assistant, or by using a physical key, and often include additional features such as the ability to generate access codes for guests, track entry and exit logs, and integrate with other smart home devices.

1.2 Related work

People in the world are using more and more digital devices, this has lead to questions about the security and privacy, if the convenience of these devices are worth the added risk [1, 4, 5, 6].

Previous work has been done with testing, literature studies, and case studies, within the area of the security of smart locks. There are a few that tested the security of different smart locks, and some of those also did a literature study of the security of smart locks [6, 7, 8, 9]. There has also been some work about the convenience vs. security of smart home devices [4, 10]. But the user perception has not been investigated in this work, and that is what will be done in this work. In this work, the user's perception of security and

convenience will be investigated to understand how users feel about the security risks and convenience smart locks add.

In Tegg Westbrook's report "Home Security and Emergency Response: The Convenience vs Security Trade-off," it discusses the evolving landscape of home security due to increased connectivity. With the advent of more affordable and user-friendly advanced security technologies, the convenience they offer raises questions about the associated risks. The report concludes that reducing the trade-off between convenience and security is crucial, emphasizing the significant role technology firms play in achieving this balance [4].

In the report "Security evaluation of smart door locks" by Arvid Viderberg it says that smart locks might not add security but instead adds new attack surfaces compared to deadbolt locks. But that smart locks comes with a lot of convenient features for every day use. It can also be said that it is safer with virtual keys rather then physical keys since it is easier to revoke a virtual key then having to replace the deadbolt lock if a key is lost. Research also shows that there are vulnerabilities and flaws that exist in smart locks [9].

1.3 Problem formulation

The introduction of smart locks has revolutionized the way people secure their buildings. Smart locks let the user remotely control the security of their home, they offer conveniences such as enhanced security control and easy access control. But with any technology these conveniences come with trade-offs, in this case the main trade-off is between the security and convenience. Security is the level of protection that the smart locks provide against unauthorized access, while the convenience is the ease of use and accessibility the smart locks have. This thesis aims to investigate the users perception and trade offs associated with smart locks. Specifically, this research will seek to answer the following research questions:

1. What are the security, privacy, and convenience trade-offs associated with using a smart lock?

2. How do users perceive the security and convenience of smart locks?

3. Do users know the security risks associated with smart locks?

1.4 Motivation

The growing popularity of smart home devices presents security and privacy concerns for users [1]. This investigation will evaluate whether the convenience offered by smart locks justifies the associated risks for users. It will contribute to the literature on smart home device security, raise awareness among consumers, and provide insights for manufacturers to improve the security of their products. The question arises whether the convenience provided by smart locks is worth the added security risks posed by the various attack vectors they introduce.

1.5 Results

The results expected of this thesis will provide current state of the security, privacy and convenience of smart locks. It will also test these findings with user perception and expectations in regard to the security and convenience aspects. As well as the user knowledge on smart locks security risks.

1.6 Scope/Limitation

In this thesis our scope is the current state of security and convenience of smart locks, the users perception on this and users knowledge of security risks associated with smart locks. We will look at the current security risks and conveniences of smart locks, then look at what the users of smart locks think of the security and the convenience of them.

The thesis was limited since lack of information on the deeper level of the security used in smart locks, no technical data on this was found. Another limitation was the demographic group of users the survey reached, if the survey reached a more spread out group of people it might have gotten different results.

1.7 Target group

The target groups for this work are manufacturers that create smart locks, users that use smart locks or people that want to buy smart locks and others working with the area of security and/or convenience of smart locks. From this work manufactures will get a better understanding on how their users see security and convenience. Users of smart locks can also get a better understanding of the current state of the art on smart locks.

1.8 Outline

This report is structured as follows:

- Chapter 2: Methodology - Discussing the methods used for this project.
- Chapter 3: Theoretical Background - Providing a comprehensive overview of relevant theories.
- Chapter 4: Research project – Implementation - Presents how the thesis was done.
- Chapter 5: Result & Analysis - Presenting the results as well as analyzing the results.
- Chapter 6: Discussion - Discussing the implications and significance of the findings.
- Chapter 7: Conclusion and Future Work - Concluding the report and suggesting potential avenues for further research.

2 Method

The scientific method is a process that is used to understand and explore the world. The process involves a systematic approach to gathering empirical evidence, formulating and testing hypotheses, and drawing conclusions based on the data collected [11].

This method is an important tool that is used for scientist to ensure that the findings are reliable and reproducible [11].

A literature review was conducted on the security of the smart locks, to gather as much information as possible in the allocated time frame for it. The information was taken from a previous thesis about smart locks security and other reports in that area. The information was first processed and then critically analyzed. The keywords used for finding the relevant information were, "smart locks", "security", "privacy", "convenience" and "user". The databases that were used were Diva, Google´s search engines and One Search.

With the information obtained from the literature review, questions for a survey were created to get knowledge about user perception of smart locks security vs convenience. A survey was used to get the users perception, and was the best way to get as many different participants on this as possible instead of going more in depth with less participants [12]. The survey was a Web-Based survey and uses a Likert scale.

2.1 Research Project

We plan to do this by first conducting a literature review and from this we expect to get an understanding of the security and convenience of smart locks to both evaluate them and based on the information we got from that we will create a questions for a survey for users about their perception of the security and convenience of smart locks. With the survey we expect to get data for how users perceive the security and convenience of smart locks and from there analyze the data to be able to answer our research questions.

2.2 Research methods

In this thesis we will use two different research methods, literature review and a survey. A literature review is a summarized set of relevant sources and the collective conclusion of the most relevant data to the interest of the review. A survey looks at a sample of a population in order to draw conclusions about that population. The group of world objects that the researcher is interested in is referred to as a population here.

In our work, the literature review is used to gather information about smart locks, with a focus mostly on security and some on convenience as well. This is to get a good understanding of smart locks today and their security, what work has already been done in this area, get information to base the survey on, and what the security and/or privacy trade offs of having a smart lock can be.

The survey is used to gather information about the user's perception of the security vs. convenience of smart locks. This is a Web-based survey, meaning that it is an online survey, It was created in Google Forms. This helped to create it in an easy way, and it makes it easy to analyze the data from it. The data will be analyzed, and with that, we will be able to answer the rest of our research questions.

The survey is composed of statements that participants should evaluate using a 5-point Likert scale, ranging from strongly disagree to strongly agree. Based on the answer to the initial statement, "I use a smart lock," participants will be presented with different statements in order to match their experience with smart locks. The Likert scale is

easy to understand for users and creates quantifiable data which is easy to statistically analyze[13]. All statements can be seen in Appendix 2.2

For data analysis in this research, Google Sheets was utilized. This tool offers ease of use and helpful built-in functions, such as the STDEV function. The STDEV function was used to calculate the standard deviation of the data. The standard deviation serves as a valuable statistic to understand the dispersion of data. By determining the standard deviation, it becomes possible to uncover patterns within survey responses. This information aids in drawing conclusions based on the findings of the research[14].

2.3 Reliability and Validity

Considering the reliability of this project, it should be quite dependable. The only factor that may influence the outcomes is the composition of the participants involved in the survey. All participants will first be asked if they have a smart lock and depending on their answer the following statements will be different. The literature review should get something that is very similar to our project and the survey is the only factor that should make any differences in the results if the work would be replicated. If the replication has the same survey questions the only thing that could change the results is the participants that answer it and this is why we will try to get as many to do the survey as possible this will help with the reliability and validity of this project.

2.4 Ethical considerations

In our survey it is required to login with an email to keep one answer to each person, but this email will not be saved and we will not take any other personal information like name, age, gender and so on. The survey is conducted by using google forms, this makes it so the data is stored in google drive but will not be shared with anyone outside of the project. All survey responses will be analyzed collectively. The data will only be used for the purpose of this project. The data will not be able to be linked back to the person that did the survey.

The results will only serve for increased awareness about smart lock vulnerabilities and no details on how locks can be exploited will be shared.

3 Theoretical Background

The literature review serves as the foundation for our research project as the theoretical background is built on it. It involves a limited literature review of existing research and reports on smart lock security, privacy, and convenience. The main objective of the literature review is to establish the current state of knowledge in the field, identify gaps in the existing research, and inform the design and implementation of our survey.

As cutting-edge technologies become more accessible and less expensive, the world is becoming more and more digital. This leads to many questions about if the convenience of connectivity is worth the risk it might add. These risks can include peoples security and privacy, especially when it's connected to their homes. The general lack of security thinking people have is also a problem. It has been shown that users are becoming more concerned with privacy and the security of their data. But some things have indicated that smart homes have improved security for users. This then leads to the question if security with smart home devices provide users with more benefits then threats [4]?

3.1 Smart locks today

There are many reasons to be using a smart lock. It offers many convenient features. For example there is no need to be carrying your keys with you. If you are unsure if you forgot to lock the door it can easily be checked in an app. If you have a delivery coming you can let the delivery man leave the package inside instead of leaving it on the porch. You can have temporary codes which friends and family can use or you can open the door remotely for them [15, 16].

Smart home devices are among the most popular IoT devices that have been developed to improve daily lives for users. Smartphones are used with these smart locks to make it easier for users to not have a physical key and not have to keep track if the door is closed or not, the security of these are very interesting for the security community. Because of this the security of smart locks are being investigated. IoT devices are being used more widely and have brought convenience into our lives. But even though these devices bring convenience there are also a wide range of security issues. There are a number of potential vulnerabilities in smart home appliances that is a threat to data privacy and personal security. With smart home systems the biggest vulnerability component is the mobile app. This is due to it being impossible for a human developer to implement a perfect interface for the smart home controlling app, also that there are always users that lack in the security skills and can easily be tricked by people with malicious intent. This is why smart home appliances should have an effective authentication to authorize and identify legitimate mobile apps and drop fake mobile apps [6].

The smart lock architecture typically involves integration with a smart hub and other microcontrollers, enabling seamless interaction with various smart devices [17]. However, this interconnectedness also introduces potential attack vectors that could be exploited by malicious actors.

3.2 Security, Privacy and Convenience

Introducing smart security devices to a home can provide greater security for a home but at the cost of giving up some privacy and cyber security. Data collected may be shared with third parties or be part of data breaches. How much security and privacy one is willing to give up for some convenience is of course individual [4].

Research in the field of cyber security has highlighted that there are multiple points of entry in appliances that "tech-savy" hackers can exploit. There has been a lot of focus on the privacy implications of appliances, but not as much has been focused on the sacrifices between privacy and other security. Privacy is a big challenge in smart homes since they are internet-connected, which makes private data more vulnerable. This then brings back the question of whether the convenience added is worth the trade-off in privacy. Technology firms have a big part to play in bettering the trade-offs between convenience and security [4].

Data collection from smart home devices may raise some concerns such as data collection and violation of privacy. A big factor in how much people care about their data privacy seems to depend on who may get access to the data. The biggest concern people seem to have is if the government gained access to their data. But if private corporations such as manufacturers were to have access to said data they would not be as concerned. They see it as a way in which the products could be improved. People also feel negative about if Internet Service Providers (ISP) were to collect data, they do not see any valid reason for them to gather data and some brought up the potential of compromising net neutrality. When it comes to advertisers the perception is more split, about 50/50. Some state that they like personalized advertisements and others feel they do not want them selling their data and making money off of it [18].

Smart home devices have become more mainstream due to tech companies have pushed these devices and technologies for multiple years now, but they are not completely adopted yet, the biggest factor to this is the privacy and security concerns. Smart home devices deliver convenience but for many consumers security and privacy are more important. Almost 70% of consumers are concerned about privacy and security risks, about 25% delay their purchases and about 20% even terminate their IoT devices or service. When adopting IoT devices and services, 37% of consumers have grown more wary. But there is a push to promote better security and privacy features [1].

With the many conveniences of IoT devices and technologies, many people and organizations are adopting and accepting the smart home or smart building applications they offer. Some of the biggest features of smart homes are remote control, safety from intruders, real-time monitoring, and more, but with this, they also manage security and privacy, which means that the solution for this is to protect the users. The data is usually sent via wireless communication and remotely transmitted to the users homes, this increases the risk of information leakage. Access to the user's smart home resources must be prevented and blocked from being accessed by unauthorized entities, by associating proper policies with the data. Smart homes still have several challenges in security and privacy, including data integrity, availability, access control, and confidentiality [5].

In the realm of smart home automation, smart locks serve as replacements for traditional deadbolt locks. These innovative devices operate on short-range network signals like Bluetooth Low Energy (BLE) and establish communication with the user's smartphone. Not only do smart locks substitute conventional locks, but they also offer additional functionalities such as automatic locking and unlocking of doors, as well as the ability to track individuals entering or leaving the home by detecting their smartphones. However, a concerning revelation emerged during DEFCON in 2015, indicating that approximately 75% of BLE smart locks are vulnerable to hacking.

The design of the lock and the applied mechanisms are the two main reasons why a smart lock's security can be compromised. The lock's physical design, overall architecture, and functionality are referred to as its design. It includes capabilities like wireless communication with the user's phone, the utilization of short-range network signals, and

extras like automated locking and tracking.

The precise protocols, algorithms, and software elements that make up a smart lock's implementation, on the other hand, are referred to as its mechanisms. These systems are in charge of handling access control, encryption, and authentication procedures to ensure safe communication. Security breaches may also be caused by flaws or weaknesses in the established mechanisms [19].

3.3 Attacks

Smart locks, like any other digital security system, can be vulnerable to various types of attacks. Through the literature review, numerous attack methods have been identified. The following list presents some of the key methods in which a smart lock can be compromised:

Man-in-the-Middle (MITM) attack: During the communication between a smart lock and the user's device, such as a smartphone, an attacker has the capability to intercept this communication. By doing so, the attacker can capture, manipulate, or inject data into the communication process. This unauthorized interference poses a significant risk as it may grant the attacker unauthorized access to the smart lock or prevent the legitimate user from accessing it [20].

Brute-force attack: An attacker systematically attempts every possible combination of characters for the lock's password or PIN until the correct one is found. This method can be time-consuming but may eventually result in unauthorized access if the password or PIN is weak or easily guessable [21].

Dictionary attack: Instead of trying every possible character combination like a brute-force attack, a dictionary attack uses a list of common or likely passwords, often derived from previously leaked data breaches. If the smart lock's password is a common one or found on this list, the attacker can gain access more quickly than through brute force [21].

Social engineering: Attackers can use social engineering tactics, such as posing as a service technician, to gain physical access to the smart lock or trick users into revealing their login credentials [22].

Relay attack: In this method, an attacker captures and relays the signal from the user's device (e.g. a smartphone or key fob) to the smart lock, tricking it into thinking the device is nearby and granting access. This attack can be carried out using specialized hardware or even smartphone apps designed for this purpose [23].

Skimming keytags: An attacker can intercept and clone a key tag or RFID card used for authentication purposes, allowing them to gain unauthorized access to the smart lock. This can be accomplished using specialized hardware or even a smartphone app [24].

Cloning keytags: An attacker can clone a key tag or RFID card by physically stealing it and creating a duplicate. This can be carried out using simple hardware and does not require specialized skills or knowledge [25].

To summarize, we have analyzed various aspects of smart lock technology, including the convenience features, smart lock architecture, and potential security vulnerabilities.

Furthermore, we have identified different types of attacks that could compromise smart locks and the implications of such breaches for privacy and security.

This research shows that smart locks offer various convenience features, such as keyless entry, remote access, temporary codes for friends and family, and the ability to grant access to delivery personnel. These features are seen as major benefits by users and contribute to the growing popularity of smart home devices.

Smart homes typically integrate with smart hubs and other microcontrollers, allowing for seamless interaction with various smart devices. However, this interconnectedness introduces potential attack vectors that could be exploited by malicious actors. The mobile app, which serves as the primary interface for a smart lock. is often the biggest vulnerability component due to human errors and the potential for the app to be exploited.

Various attack methods that could compromise smart locks have been identified. This includes, Man-in-the-Middle (MITM) attacks, brute-force attacks, dictionary attacks, social engineering, relay attacks, skimming key tags and cloning key tags.

While smart locks may introduce some additional security features they also introduce potential security and privacy risks. Data collected by smart locks may be shared with third parties or be part of data breaches. The level of concern varies depending on who may gain access to the data, with the government being the most concerning for many users.

The convenience features offered by smart locks can be seen as both a benefit and a drawback, as they require users to weigh the trade-offs between convenience and security. Some users may be willing to accept certain risks for the added convenience, while others prioritize security and privacy over convenience. As technology firms continue to develop and promote smart home devices, addressing these security and privacy concerns will be crucial for widespread adoption.

The insights gained from our literature review have been a crucial part of the development of the survey. It has provided a comprehensive understanding of smart lock technology, potential vulnerabilities, and the various attack methods that could compromise smart locks. These findings showed that there are potential risks and security vulnerabilities. Knowing this, the survey statements could be shaped around them to find out if users are aware and how they feel.

4 Research project – Implementation

In this chapter, we introduce, describe, and explain all activities carried out to collect data for our study, focusing on the design and implementation aspects of our research project. The goal is to describe in great detail how we collect data, which will form the basis for answering the remaining research questions.

4.1 Research Approach

Our research project involves a combination of a literature review, the design and implementation of a survey, and a comparative analysis of the security and convenience of smart locks. This approach allows us to gather relevant information on the current state of smart lock security, as well as user perceptions and trade-offs between security and convenience.

4.2 Survey Design and Implementation

Based on the insights gained from the literature review, we designed a web-based survey to gather user perceptions on the security and convenience of smart locks. The survey consists of several statements that participants evaluate using a 5-point Likert scale, ranging from strongly disagree to strongly agree. The statements are designed to capture both the perspectives of smart lock users and non-users.

To ensure a broad and diverse pool of participants, the survey was publicized on the school's general Slack channel as well as on LinkedIn. This means that because of the distribution platforms used the participants are most likely quite highly educated and have or are currently studying for a university degree. The data collected from the survey was then analyzed to answer our research questions related to user perceptions, security risks, and trade-offs associated with smart locks.

4.3 Comparative Analysis

Using the data collected from the literature review and the survey, we conducted a comparative analysis of the security and convenience aspects of smart locks. This analysis aims to determine whether the convenience offered by smart locks justifies the associated security and privacy risks. The comparative analysis involves assessing various attack vectors, user perceptions, and potential trade-offs.

5 Results & Analysis

In this chapter the results gathered from the survey will be presented and analyzed. The survey was publicized on the Linnaeus University (LNU) general Slack channel as well as on Oliver Berglöf's Linkedin. The survey was open from the 5th of April until the 18th of April. The data collected from this was then analyzed and will be presented in this section.

The survey aimed to gather insight on peoples perception on the security and convenience of smart locks among Swedish homeowners. All the information about the users are self claimed.

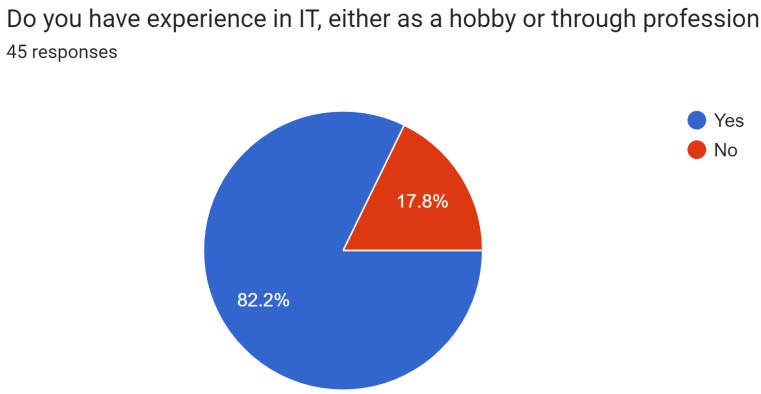


Figure 5.1: Users IT experience

As shown in Figure 5 it can be seen that out of the 45 survey participants 37 (82.2%) have experience in IT either as a hobby or through work, while eight (17.8%) have no experience in IT.

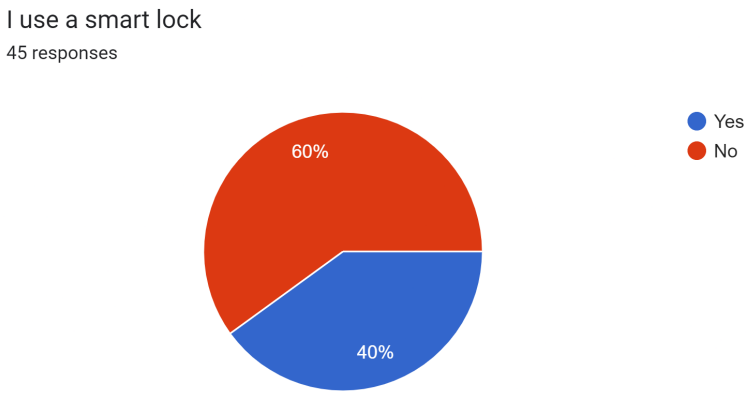


Figure 5.2: Uses a smart lock

With these 45 participants 18 (40%) are using smart a lock and 27 (60%) are not using smart a lock, shown in Figure 5.2

Out of the 18 that are using smart locks, 14 (78%) have IT experience while four (12%) do not. And out of the 27 that are not using smart locks 24 (89%) have IT experience and three (11%) have no IT experience.

5.0.1 Do not use smart locks

Out of the 45 responses on the survey 27 responded that they do not use a smart lock and only their responses will be considered in this section.

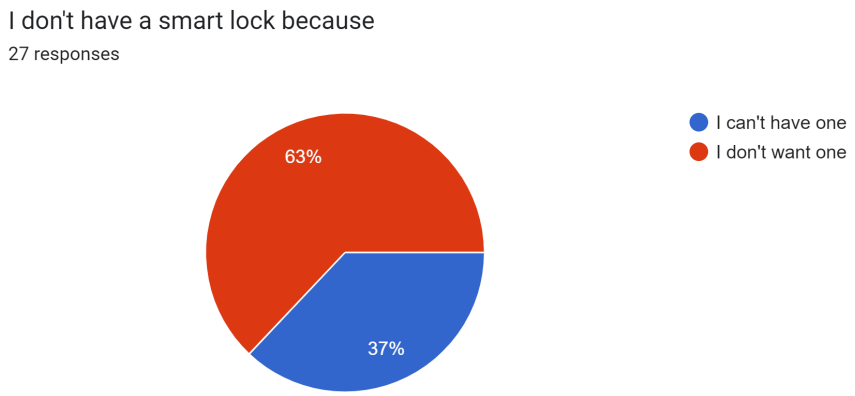


Figure 5.3: Why they don't use a smart lock

As shown in Figure 5.3 it can be seen that out of these 27, 17 (63%) don't have one because they don't want one and ten (37%) don't have one because they can't have one.

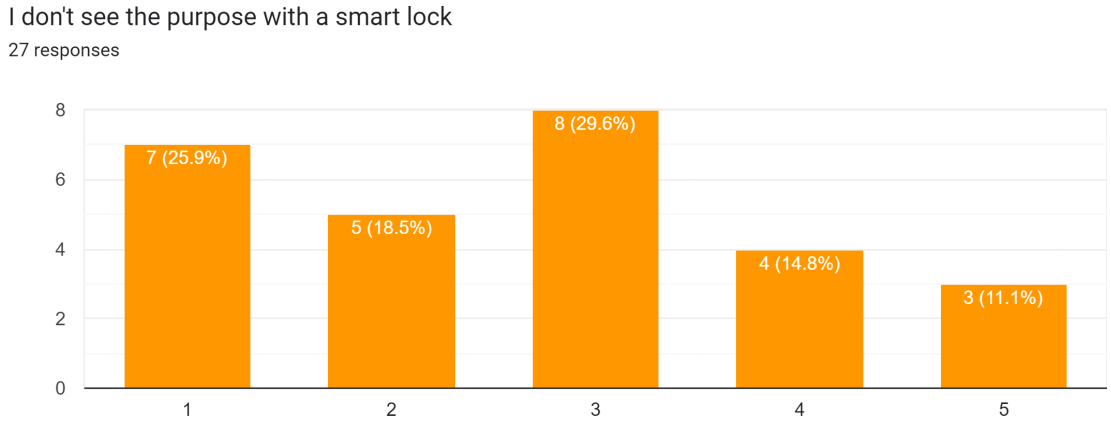


Figure 5.4: See the purpose of smart lock

In question about the purpose of smart locks seven (25.9%) don't see the purpose while three (11.1%) do see the purpose and the rest are somewhere in between some see the purpose less and some more but most seem to be neutral, this can be seen in Figure 5.4.

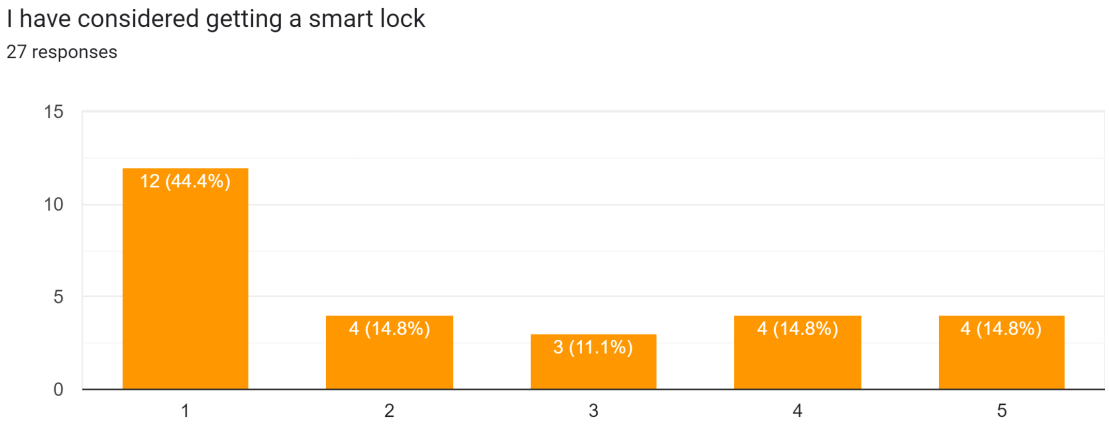


Figure 5.5: Considerd getting a smart lock

As shown in Figure 5.5, 12 (44.4%) have not considered getting a smart lock while four (14.8) have considered it and the others have somewhat considered it some more and some less.

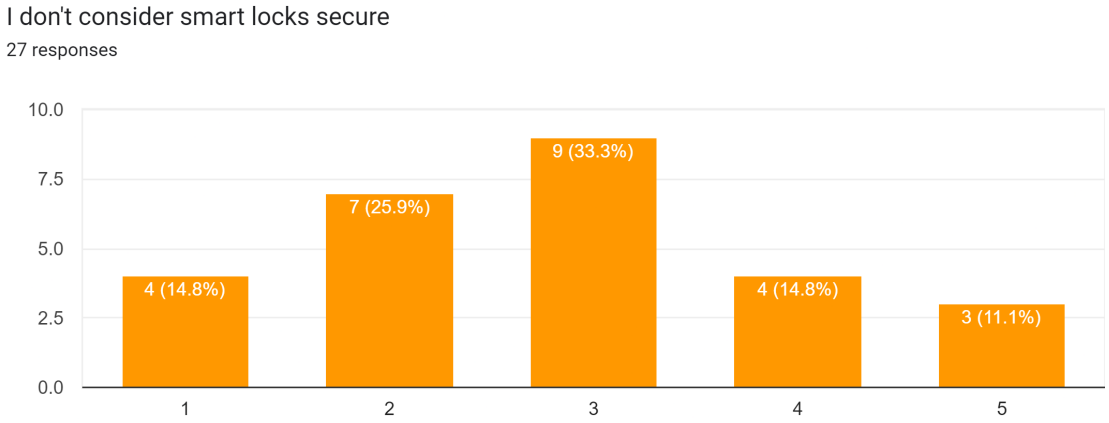


Figure 5.6: Consider smart locks secure

In Figure 5.6 it can be seen that four (14.8%) do not consider smart locks secure, and three (11.1%) do consider them secure and the rest in between where some feel more secure with them and some more.

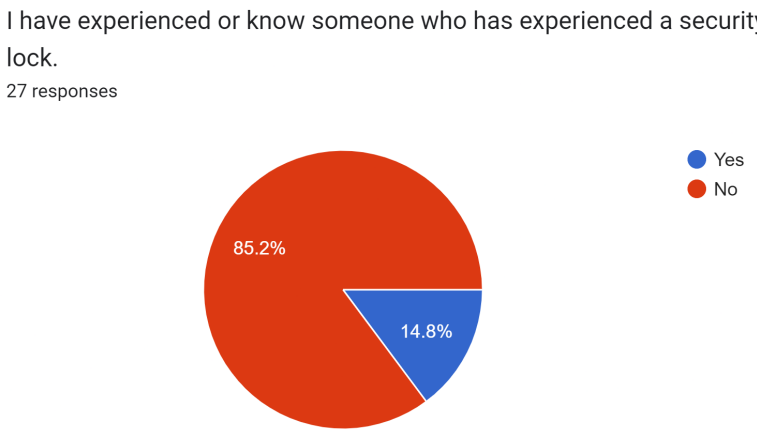


Figure 5.7: Security breach

In Figure 5.7 it is shown that, 23 (85.2%) do not have experience or know someone who has experienced a security breach related to a smart lock. While four (14.8%) do have experience or know someone who has experience a security breach related to a smart lock.

The 17 that don't have a smart lock because they don't want one have an average of 3 on the question about the purpose of smart locks and average of 3.2 on the question if they consider smart locks secure. The ten that don't have a smart lock because they can't have a smart lock had an average of 2.1 on the question about purpose and an average of 2.2 on the question if they consider smart locks secure.

5.0.2 Do use smart locks

In this section only the responses from the 18 participant that state that they do use a smart lock are considered.

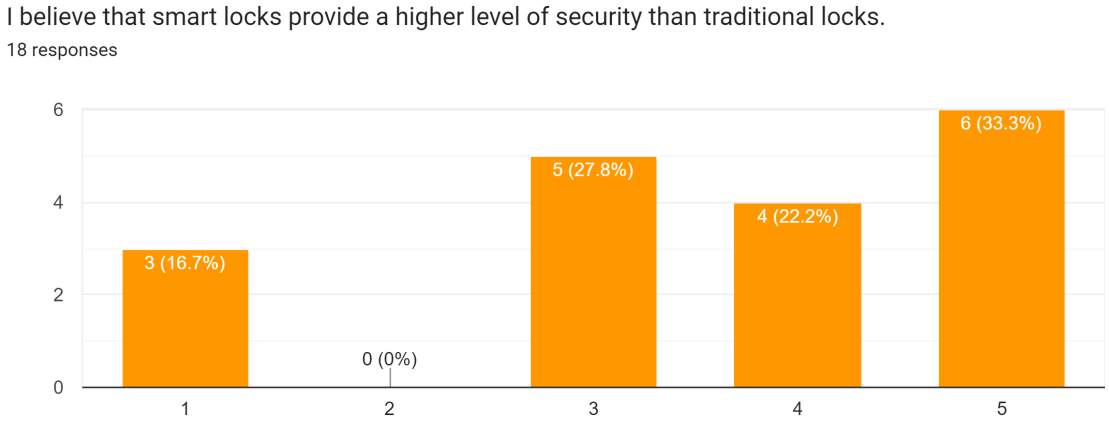


Figure 5.8: Smart locks security

As shown in 5.8 Three (16.7%) strongly disagree that smart locks provide a higher security than traditional locks, while six (33.3%) strongly agree that they provide a higher security and the rest are mostly neutral with some leaning more towards strongly agree.

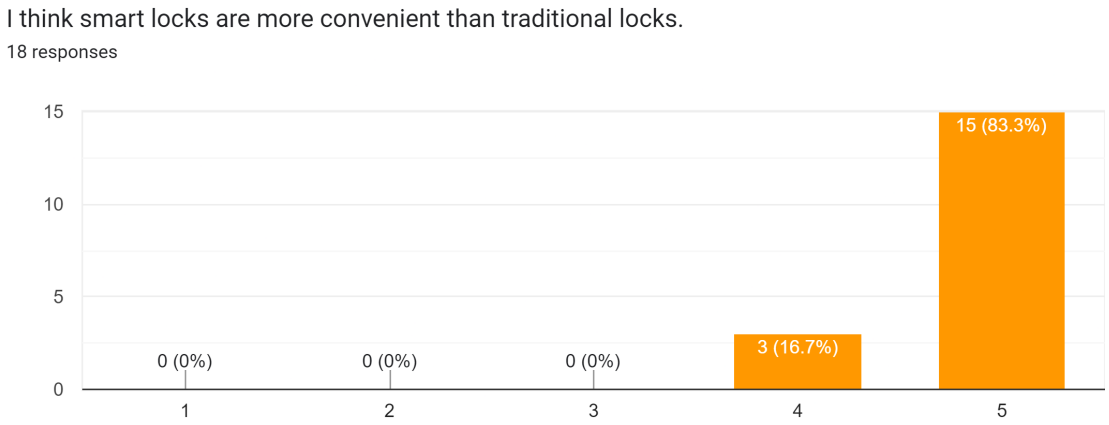


Figure 5.9: Smart locks convenience

In the Figure 5.9 it can be seen that when it comes to the convenience of smart locks 15 (83.3%) strongly agree that they are more convenient then traditional locks and three (16.7%) are between neutral and strongly agree.

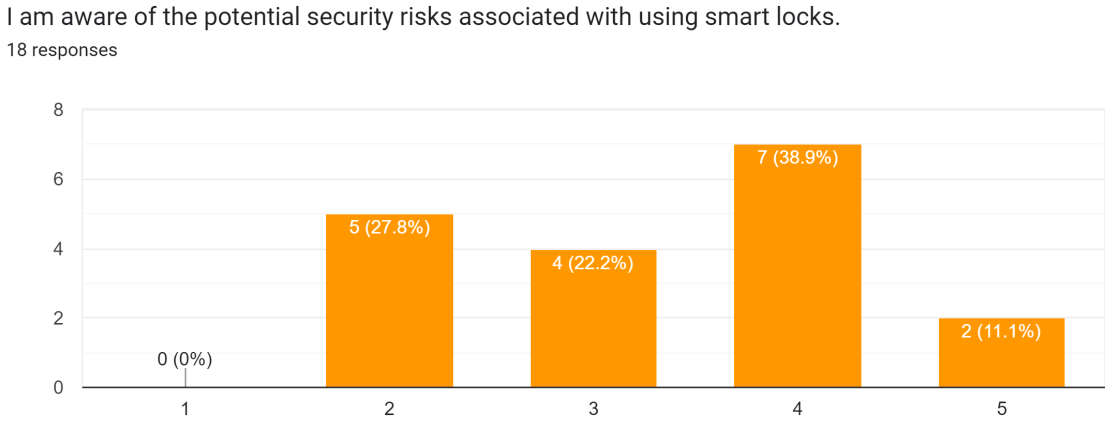


Figure 5.10: Aware of potential security risks

About awareness of the security risks associated with using smart locks, as shown in Figure 5.10 two (11.1%) strongly agree, seven (38.9%) are between neutral and strongly agree while, four (22.2%) are neutral and five (27.8%) are between neutral and strongly disagree and no one strongly disagrees.

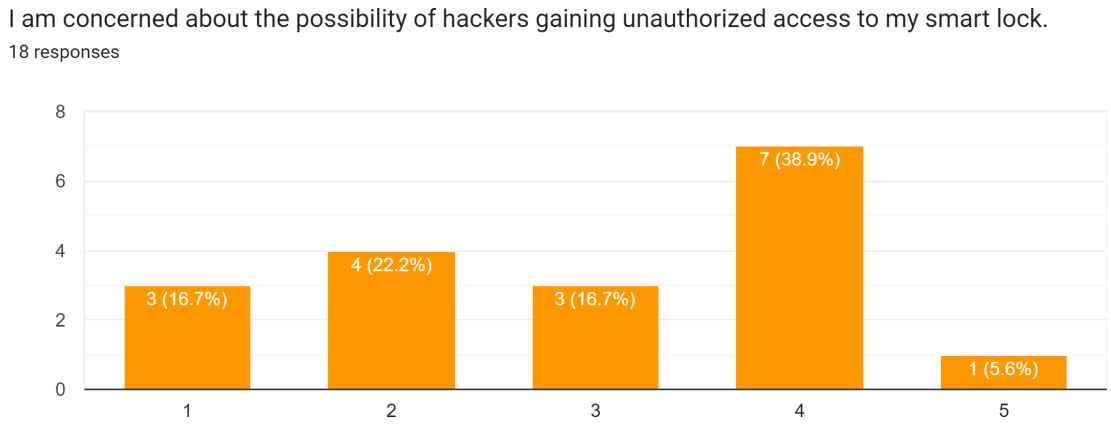


Figure 5.11: Concerned about hackers

As it can be seen in Figure 5.11, when it comes to users concerned about the possibility of hackers gaining unauthorized access to their smart lock. three (16.7%) strongly disagree and one (5.6%) strongly agree but seven (38.9%) are in between neutral and strongly agree.

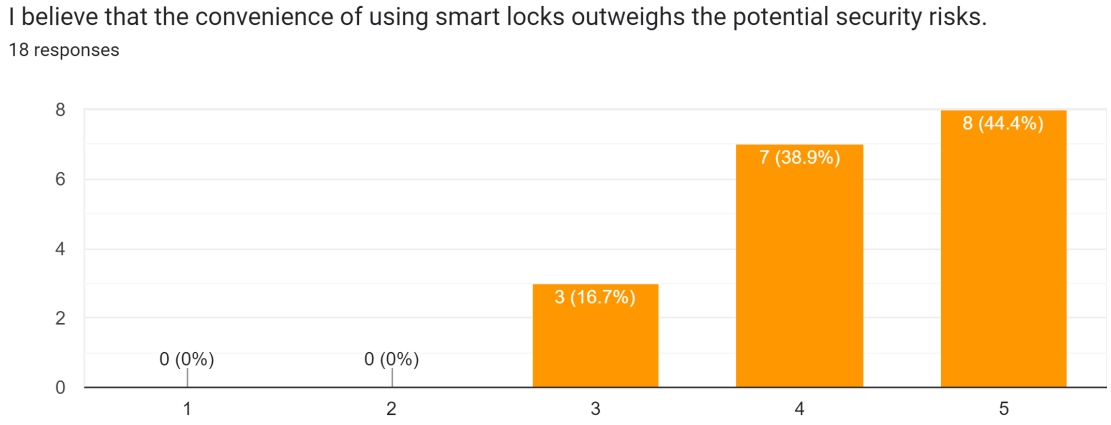


Figure 5.12: Convenience outweighs security risks

In Figure 5.12 it shows that eight (44.4%) strongly agree and no one strongly disagrees and three (16.7%) are neutral and the seven (38.0%) others are in between neutral and strongly agree.

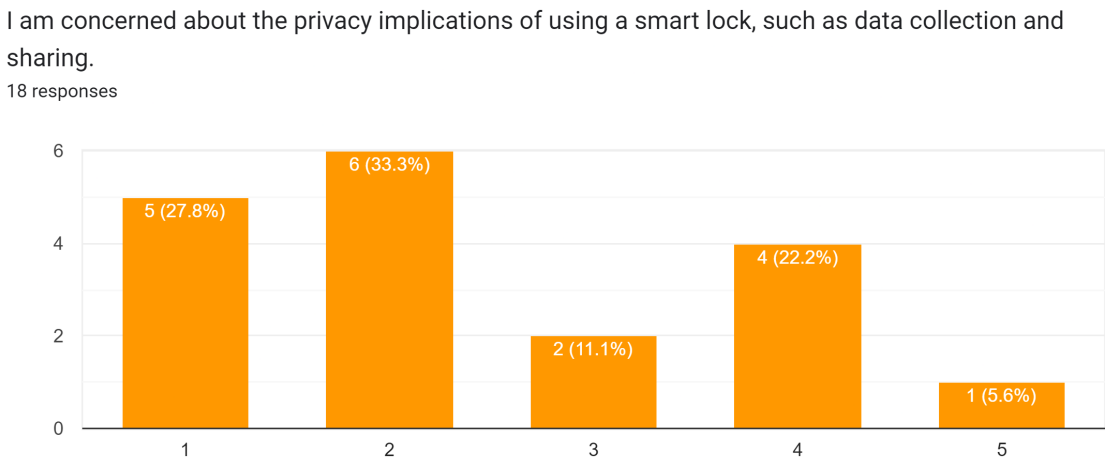


Figure 5.13: Privacy concerns

When it comes to users being concerned about the privacy implications of using a smart lock, five (27.8%) strongly disagree that they are concerned and one (5.6%) strongly agree, but 6 (33.3%) are in between strongly disagree and neutral, this can be seen in Figure 5.13.

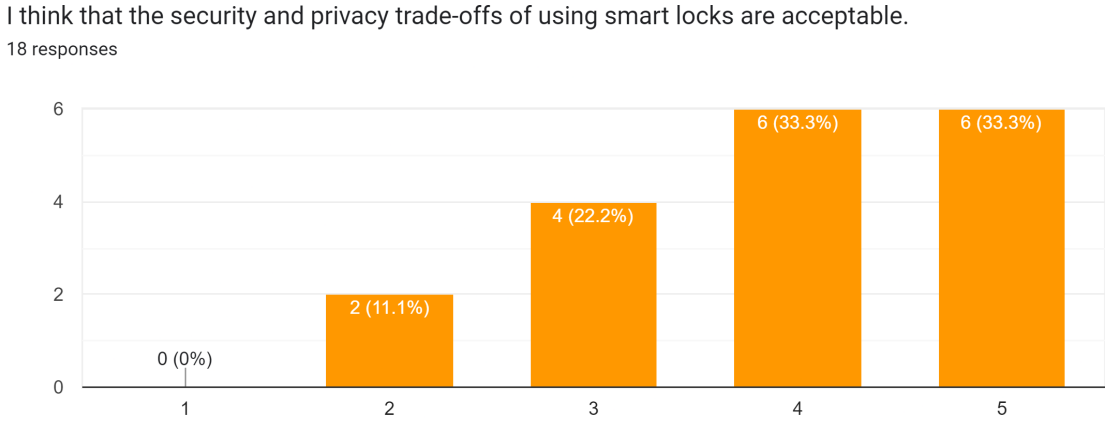


Figure 5.14: Trade-off acceptable

In Figure 5.14 it is shown what users think if the security and privacy trade-offs are acceptable, it can be seen that zero strongly disagree and that six (33.3%) strongly agree and another six (33.3%) are in between neutral and strongly agree.

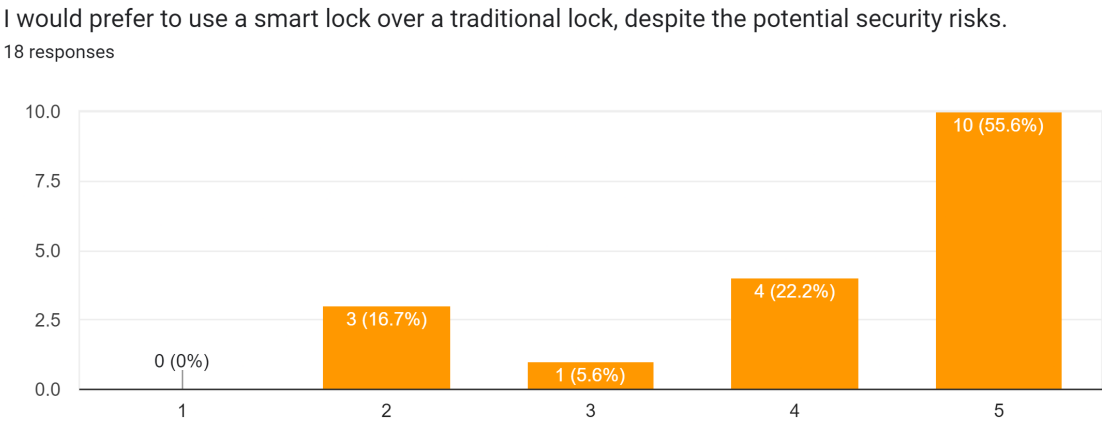


Figure 5.15: Prefer smart lock

In Figure 5.15 it can be seen that when it comes to users prefer smart lock, even that it has potential security risks ten (55.6%) strongly agree and zero strongly disagree.

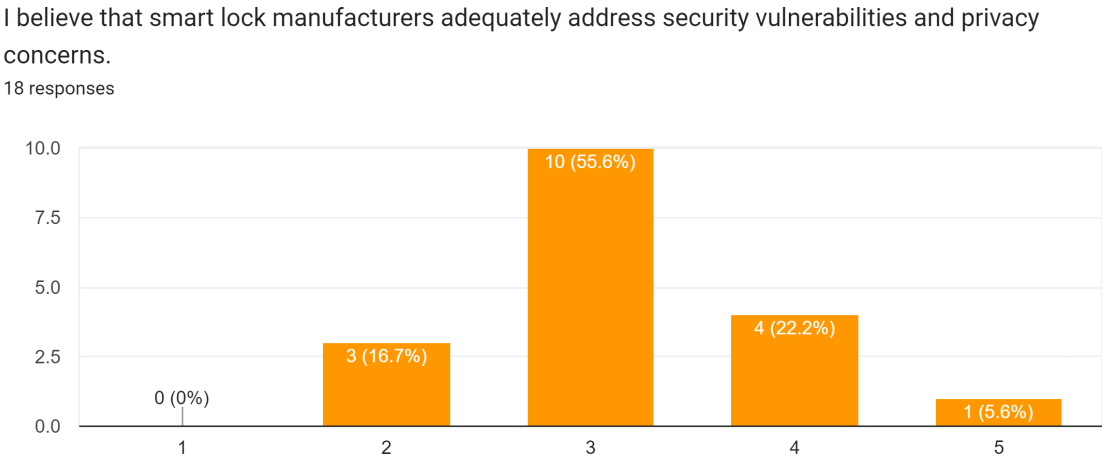


Figure 5.16: Manufactures on privacy

Figure 5.16 shows the results from a question about if users think that manufacturers address there security vulnerabilities, it can be seen that one (5.6%) strongly agree, zero strongly disagree but ten (55.6%) are neutral.

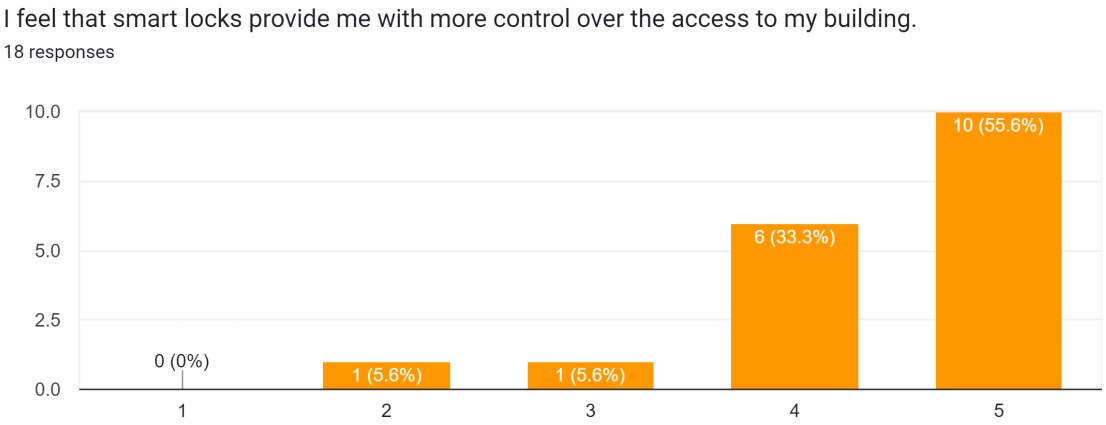


Figure 5.17: Smart locks control

On the question about if users feel more in control with smart locks, ten (55.6%) strongly agree, zero strongly disagree, this can be seen in Figure 5.17.

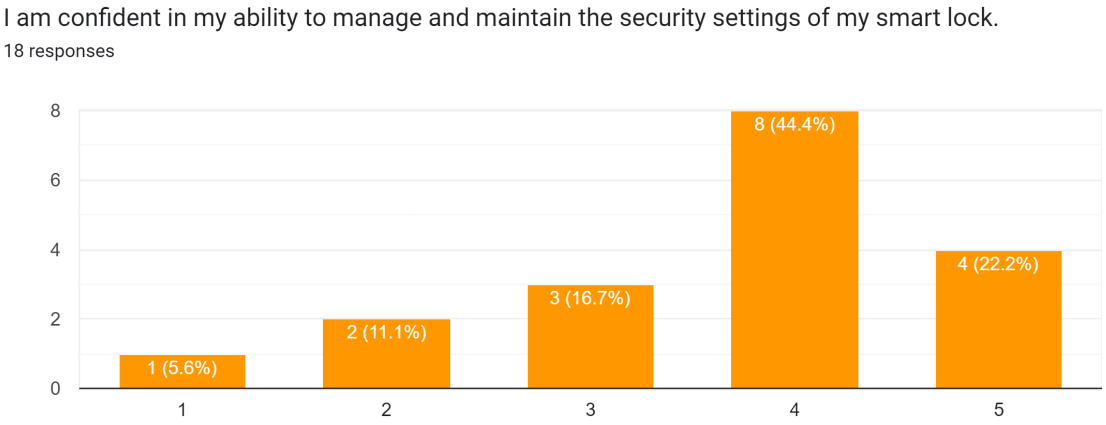


Figure 5.18: Manage security settings

In Figure 5.18 it can be seen if users feel confident in being able to manage the security settings of their smart lock. Eight (44.4%) are in between neutral and strongly agree, one (5.6%) strongly disagree and four (22.2%) strongly agree.

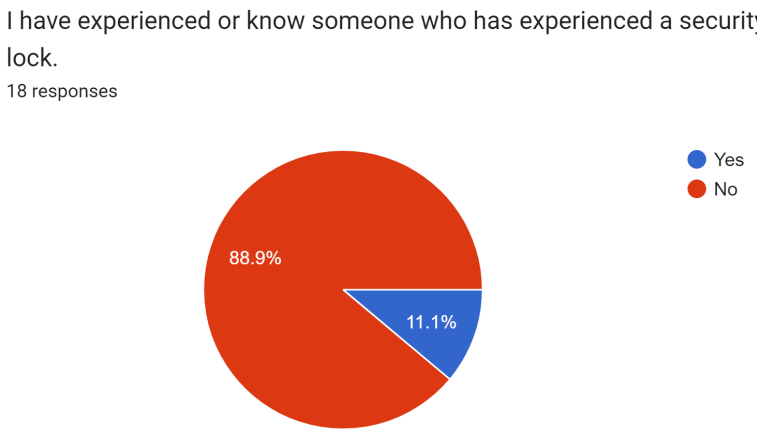


Figure 5.19: Experience with security breach

When it comes to if the users have experienced or know someone who has experienced a security breach, 16 (88.9%) have not and two (11.1%) have, this can be seen in figure 5.19

	Survey Question	**Mean**	**SD**
Non smart lock users answers			
	I don't see the purpose with a smart lock	2.67	1.33
	I have considered getting a smart lock	2.41	1.55
	I don't consider smart locks secure	2.81	1.21
Smart lock users answers			
	I believe that smart locks provide a higher level of security than traditional locks.	3.56	1.42
	I think smart locks are more convenient than traditional locks.	4.83	0.38
	I am aware of the potential security risks associated with using smart locks.	3.33	1.03
	I am concerned about the possibility of hackers gaining unauthorized access to my smart lock.	2.94	1.26
	I believe that the convenience of using smart locks outweighs the potential security risks.	4.28	0.75
	I am concerned about the privacy implications of using a smart lock, such as data collection and sharing.	2.44	1.29
	I think that the security and privacy trade-offs of using smart locks are acceptable.	3.89	1.02
	I would prefer to use a smart lock over a traditional lock, despite the potential security risks.	4.17	1.15
	I believe that smart lock manufacturers adequately address security vulnerabilities and privacy concerns.	3.17	0.79
	I feel that smart locks provide me with more control over the access to my building.	4.39	0.85
	I am confident in my ability to manage and maintain the security settings of my smart lock.	3.53	1.14

Table 5.1: Average scores (Mean) and standard deviations (SD) for the survey statements

When examining the survey results the standard deviation plays a significant role. It offers a measure of the variation of the answers, which allows for a better understanding of the consensus among the participants.

A low standard deviation shows that the participants had similar opinions or thoughts on the topic. For example, the low standard deviation (0.38) and mean answer of 4.83 for the statement "I think smart locks are more convenient than traditional locks" suggests that (all) the participants may be using smart locks because they are very convenient and thus draw the conclusion that they are most likely more convenient than traditional locks.

On the other hand, a high standard deviation signifies a more varied response, which makes it more difficult to draw definite conclusions. For example, the statement "I believe that smart locks provide a higher level of security than traditional locks." for smart lock users has a high standard deviation (1.42) and a mean answer of 3.56, which indicates that the answers are very spread out. This can then mean many things, the dispersion could be caused by differences in IT knowledge or varying security and privacy concerns.

In summary, standard deviation serves as a crucial tool for assessing the reliability and strength of the conclusions drawn from the responses. It helps pinpoint areas where respondents exhibit strong agreement or disagreement, and reveals nuanced differences in opinions that can guide future research or inform product enhancements. By analyzing the standard deviation in conjunction with the mean scores, we can gain a deeper understanding of the participants' perspectives on smart lock usage, security and convenience.

Continuing our analysis of the survey results, it appears that individuals with IT knowledge tend to be somewhat more concerned about privacy and security issues related to smart locks. For instance, when asked about concerns regarding hackers potentially gaining unauthorized access to their smart locks, participants with IT knowledge had a mean score of 3.2, indicating a neutral stance. In contrast, participants without IT knowledge had a mean score of 2.2, leaning slightly towards not being concerned about this potential security risk. The trend is similar when participants were asked about data collection and sharing concerns related to smart locks. However, both groups are not very concerned in general. The group with IT knowledge appears to be somewhat more concerned, with a mean score of 2.7, compared to the group with IT knowledge, which has a mean score of 1.8. Interestingly, this does not really match the statement about whether they are aware of potential security risks. Here the difference is much smaller, at 3.5 for the group with IT knowledge and 3.0 for the other. This might be caused by people without IT knowledge who believe they are aware but don't really understand all the potential risks associated with smart locks.

6 Discussion

In the literature review that was conducted we found that with smart locks comes both convenience features and security and privacy risks. The conveniences features can be key-less entry, remote access/control to the lock and temporary codes for guests. Methods that have been identified that can compromise smart locks are MITM, brute-force attacks, dictionary attacks, social engineering, relay attacks, skimming key tags and cloning key tags. And privacy can also be compromised with both data breaches and what data is shared with third parties.

In our survey, we found that out of the participants that use smart locks they all seem to think that the convenience of using smart locks is worth the potential security risks. And that all seems to know some security risk associate but some seems to know more and some less.

With these findings we can answer our research questions with the literature review pointing out all the trade-offs with smart locks, and the survey we got the users perception on the security and convenience of smart locks, as well as getting knowledge of users knowing about the security risks associated with smart locks.

During our work, we had some challenges, such as getting enough participants for our survey and finding enough previous work in the area. We believe that getting more participants would help make a better analysis of the results and draw more conclusions from a broader group of people. For future research, it would be advantageous to allocate more time for survey distribution and promote the survey in more locations and for longer durations. This approach would help us reach a larger number of potential participants and collect more data to enhance the validity of our findings.

Considering the implications of our study for the larger smart lock industry is crucial after taking these realizations into account. Our research emphasizes how crucial it is to address security and privacy issues while educating users about the potential dangers associated with smart locks. To allay user concerns and promote wider use of smart locks, producers and developers should place a high priority on enhancing security features and offering clear information about data handling procedures.

Users may also benefit from educational initiatives that are aimed at them because they will be better able to decide whether to use smart lock technology and maintain their security and privacy. Users can make better decisions about whether to use smart locks in their homes by being provided with the resources and tools they need to better understand the benefits and drawbacks of this technology.

In conclusion, our research emphasizes the necessity of a well-balanced strategy for the advancement and uptake of smart lock technology. While the convenience features of these devices are unquestionably appealing, it is important to address the security and privacy concerns raised by them. We can contribute to the creation of a safer and more secure environment for users who choose to adopt smart lock technology by enhancing security features, offering transparent information on data handling practices, and increasing awareness of potential risks.

7 Conclusions and Future Work

This section will conclude a conclusion of our results to our research questions and future work.

7.1 What are the security, privacy, and convenience trade-offs associated with using a smart lock?

Using smart locks gives trades-offs in terms of security, privacy and convenience. Smart locks offer conveniences but with these comes risks.

When it comes to the conveniences of smart locks, they may vary between different locks. The benefits found in the literature review were key-less entry, remote access/control, and temporary codes.

In terms of security risks, the literature review identified multiple compromising methods associated with smart locks, including MITM, brute-force attacks, dictionary attacks, social engineering, relay attacks, skimming key tags, and cloning key tags. These risks may, of course, be different depending on the lock and its security features.

Privacy risks associated with smart locks were also identified in the literature review. The risks found were data breaches and how the data is shared with third parties. It is important that the user is aware of the data collection and how it's being used to try to avoid these risks.

7.2 How do users perceive the security and convenience of smart locks?

A survey was done to get the users perception on smart locks security and convenience. And in general, it appears that participants were conscious of the potential risks associated with using a smart lock. Nevertheless, they seem to believe that the benefits of convenience outweigh any eventual risks.

The perception of convenience and security varies across users, and the results of the survey show that the participants understand that there are potential security and privacy risks with using smart locks, but they also know about the convenience it offers and that this can be valuable.

Everyone's perception can vary depending on their experience and knowledge of smart locks. Users who have less experience and knowledge may have a different perception of convenience and security than those with more.

These survey results do not provide insight into the specific risks users are aware of or how to deal with them. Therefore, further research is needed to know how users can be educated about the risks associated with smart locks, how to be more secure, and how to use their convenience.

In conclusion, users seem to perceive that in the trade-offs between security, privacy, and convenience, the convenience is worth the potential security and privacy risks.

7.3 Do users know the security risks associated with smart locks?

The survey that was conducted showed that users generally have awareness about the potential security risks associated with smart locks. All of the respondents indicated that they were aware of the existence of security risks, while some were more knowledgeable than others.

The survey does not provide any specific risks that users are aware of or how much they know about them. The users may be aware of these risks, but it's unclear how much they know about them and how to prevent them.

These results are relevant for society since the growing popularity of smart locks today gives the manufacturers a view of their users' perceptions of security and convenience and gives the users a point of view on what others think as well as the security risks associated with smart locks.

7.4 Future Work

Further research is needed to investigate users' perceptions in greater detail, particularly focusing on different demographics. While this thesis did not specifically target any particular demographic, it ended up primarily involving university students. A larger sample size could be beneficial in order to more clearly observe differences and patterns. This would also help identify how to improve users' knowledge about the risks of smart locks and ways to mitigate them. Other future research could be done on how to better educate users about how to use smart locks securely.

References

[1] A. Johannson. (2020, Apr) Security in the smart home. ISACA Now Blog. [Online]. Available: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/security-in-the-smart-home

[2] "Smart home market size, share, growth trends report 2022-2030," 2022. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/smart-homes-industry

[3] D. Celestine, "Smart lock systems: An overview," *International Journal of Computer Applications*, vol. 177, no. 37, p. 40–43, Feb 2020.

[4] T. Westbrook, "Home security and emergency response: The convenience vs security trade-off," *Salus Journal*, vol. 9, no. 1, p. 66–74, Feb. 2021. [Online]. Available: https://salusjournal.com/wp-content/uploads/2021/04/Westbrook_Salus_Journal_Volume_9_Number_1_2021_pp_66_74.pdf

[5] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, "Securing the smart home: a real case study," *Internet Technology Letters*, vol. 1, p. e22, 12 2017.

[6] M. Ye, N. Jiang, H. Yang, and Q. Yan, "Security analysis of internet-of-things: A case study of august smart lock," in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2017, pp. 499–504.

[7] S. Veijalainen and T. Karlsson, "Evaluating the security of a smart door lock system kth thesis report," *DEGREE PROJECT IN TECHNOLOGY*, 2021. [Online]. Available: https://kth.diva-portal.org/smash/get/diva2:1602711/FULLTEXT01.pdf.

[8] R. Hassani, "Security evaluation of a smart lock system raihana hassani kth royal institute of technology school of electrical engineering and computer science," 2021. [Online]. Available: https://kth.diva-portal.org/smash/get/diva2:1533957/FULLTEXT01.pdf.

[9] A. Viderberg, "Security evaluation of smart door locks arvid viderberg kth skolan fÖr elektroteknik och datavetenskap," 2019. [Online]. Available: http://www.diva-portal.org/smash/get/diva2:1336796/FULLTEXT01.pdf.

[10] A. Fung, "Smart homes and policy: Cybersecurity risks and tradeoffs | bipartisan policy center," 2022. [Online]. Available: https://bipartisanpolicy.org/blog/smart-homes-policy-cybersecurity-risks/

[11] Khanacademy.org, "The scientific method," 2023. [Online]. Available: https://www.khanacademy.org/science/biology/intro-to-biology/science-of-biology/a/the-science-of-biology

[12] K. J. Jansen, K. G. Corley, and B. J. Jansen, *E-Survey Methodology*, 2006. [Online]. Available: https://faculty.ist.psu.edu/jjansen/academic/pubs/esurvey_chapter_jansen.pdf

[13] J. Losby and A. Wetmore, *CDC Coffee Break: Using Likert Scales in Evaluation Survey Work*, 2012. [Online]. Available: https://www.cdc.gov/dhdsp/pubs/docs/CB_February_14_2012.pdf

[14] "Stdev - google docs editors help," 2019. [Online]. Available: https://support.google.com/docs/answer/3094054?hl=en

[15] Elon, "Därför ska du ha ett smart lås," Sep 2020. [Online]. Available: https://www.elon.se/smart-las-till-din-ytterdorr

[16] Yale, "Smarta låset yale doorman och allt för din hemsäkerhet," 2021. [Online]. Available: https://www.yalehome.com/se/sv

[17] Verisure, "Yale doorman | doorman l3 uppkopplat till hemlarm | verisure," (Accessed on 03/20/2023). [Online]. Available: https://www.verisure.se/hemlarm/produkter--tjanster/digitalt-dorrlas/yale-doorman

[18] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home iot privacy," *Proceedings of the ACM on human-computer interaction*, vol. 2, no. CSCW, pp. 1–20, 2018.

[19] P. Saiprasanna, *SMART LOCKS: EXPLORING SECURITY BREACHES AND ACCESS EXTENSIONS*, 2017. [Online]. Available: https://shareok.org/bitstream/handle/11244/300035/Palle_okstate_0664M_15335.pdf?sequence=1

[20] NordVPN, "What is a man in the middle attack?" Jan 2020. [Online]. Available: https://nordvpn.com/blog/man-in-the-middle-attack/

[21] ——, "What is a brute force attack?" Nov 2019. [Online]. Available: https://nordvpn.com/blog/brute-force-attack/

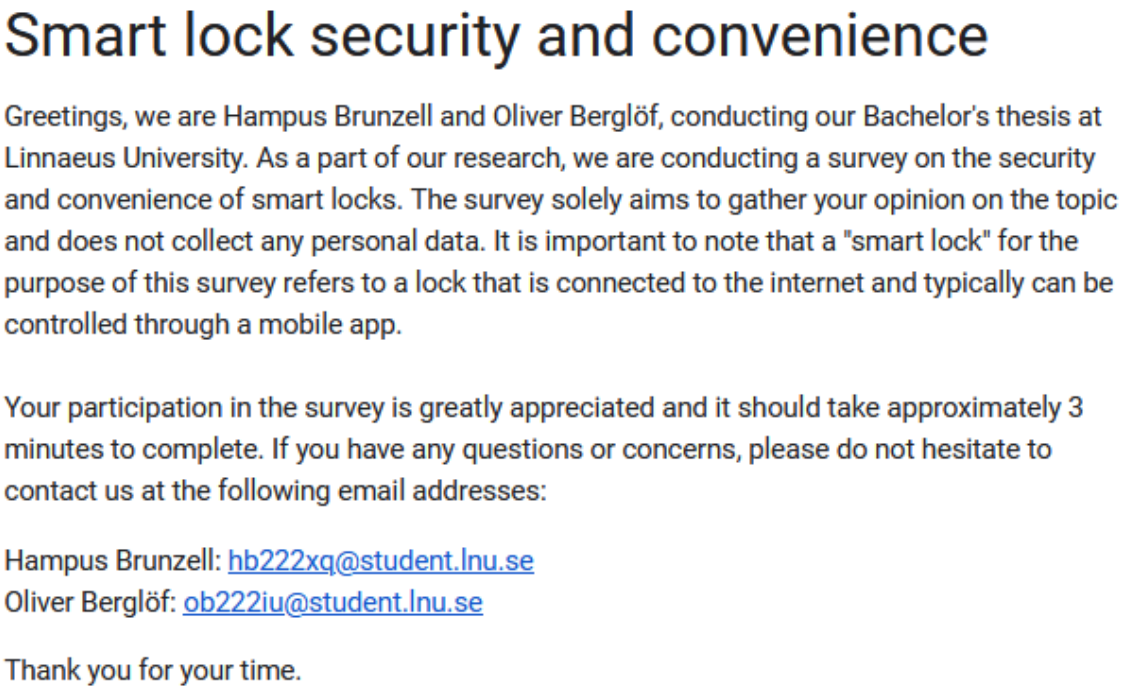
[22] ——, "Social engineering definition - glossary," Oct 2022. [Online]. Available: https://nordvpn.com/cybersecurity/glossary/social-engineering/

[23] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS '16*, 2016.

[24] NordVPN, "Skimming attack definition," May 2022. [Online]. Available: https://nordvpn.com/cybersecurity/glossary/skimming-attack/

[25] W. Huang, Y. Zhang, and Y. Feng, "Acd: An adaptable approach for rfid cloning attack detection," *Sensors*, vol. 20, no. 8, p. 2378, 2020.

A Appendix 1: Survey Description



Smart lock security and convenience

Greetings, we are Hampus Brunzell and Oliver Berglöf, conducting our Bachelor's thesis at Linnaeus University. As a part of our research, we are conducting a survey on the security and convenience of smart locks. The survey solely aims to gather your opinion on the topic and does not collect any personal data. It is important to note that a "smart lock" for the purpose of this survey refers to a lock that is connected to the internet and typically can be controlled through a mobile app.

Your participation in the survey is greatly appreciated and it should take approximately 3 minutes to complete. If you have any questions or concerns, please do not hesitate to contact us at the following email addresses:

Hampus Brunzell: hb222xq@student.lnu.se
Oliver Berglöf: ob222iu@student.lnu.se

Thank you for your time.

Figure 1.20: Description of the survey for the participants

B Appendix 2: Survey Statements

Table 2.2: Smart Lock Survey Statements

No.	Statements
1	I use a smart lock.
2	Do you have experience in IT, either as a hobby or through professional work?
	Statements to people who do not use a smart lock
3	I don't see the purpose with a smart lock.
4	I have considered getting a smart lock.
5	I don't consider smart locks secure.
6	Any other thoughts you would like to share?
	Statements to people who use a smart lock
7	I believe that smart locks provide a higher level of security than traditional locks.
8	I think smart locks are more convenient than traditional locks.
9	I am aware of the potential security risks associated with using smart locks.
10	I am concerned about the possibility of hackers gaining unauthorized access to my smart lock.
11	I believe that the convenience of using smart locks outweighs the potential security risks.
12	I am concerned about the privacy implications of using a smart lock, such as data collection and sharing.
13	I think that the security and privacy trade-offs of using smart locks are acceptable.
14	I would prefer to use a smart lock over a traditional lock, despite the potential security risks.
15	I believe that smart lock manufacturers adequately address security vulnerabilities and privacy concerns.
16	I feel that smart locks provide me with more control over the access to my building.
17	I am confident in my ability to manage and maintain the security settings of my smart lock.
18	I have experienced or know someone who has experienced a security breach related to a smart lock.
19	Do you have any other thoughts or experiences you would like to share?