How "Smart" is Your Smart Lock?

Kenneth Xue
COMP 116
Dec 13, 2019

Abstract

From toasters to fridges, every household item seems to be getting "smarter". One of the new trends of "smart" devices is the smart lock. The smart lock is growing industry still in its infancy. Smart locks allow users to more conveniently operate their locks via personal devices using technologies such as Bluetooth, Wifi, and Z-wave. However convenient, smart locks open up new vulnerabilities that allow for potential malicious attacks on one's home. These vulnerabilities all originate from poor implementation or bad security practices from smart lock manufacturers. While thinking about getting a smart lock, homeowners should think about the trade-off of price, security, and convenience between physical locks and smart locks. Presently, smart lock manufacturers do not prioritize the security of smart locks which causes many easy to exploit vulnerabilities.

Introduction

A smart lock is a lock designed to lock and unlock via electronic signals originated from an authorized device. Presently, the three main technologies used by smart locks are Bluetooth, Wi-Fi and Z-Wave. Much like regular locks, smart locks can be opened manually with a key, but the added "smart" features allow them to be opened with electronic signals originated from the user. As smart locks become more popular, the validity of their security comes into question: how does a smart lock compare to a physical lock? In this paper, I aim to discuss the technology in smart locks and analyze known vulnerabilities to present a holistic view of the purchasing choice of a smart lock.

To the community

Locks serve one and one purpose only: to secure. A smart lock brings convenience for its users at the cost of potential vulnerabilities. In the next 5 years, the smart lock industry is expected to have an 11% growth and a value of around 2 billion dollars[1]. There are a lot of reasons why a consumer might consider a smart lock. For starters, smart locks eliminate the need for hiding a spare key somewhere around your house, making your home more secure. A smart lock can also be opened without the owner being present, so the user can allow guests into their homes. Yet, the ultimate selling point of smart locks — their security — should be put into question.

[1]https://www.marketwatch.com/press-release/smart-lock-market-2019-global-trends-statistics-size-share-regional-analysis-by-key-players-emerging-technologies-growth-factors-and-future-plans-by-forecast-to-2023-2019-02-04

Technology involved

Before we dive into the potential vulunerblites of smart locks, we first must understand how smart locks work. Smart locks uses either Bluetooth, Wifi, or Z-Wave as their wireless protocol, and each one of these three technologies all have their own unique advantages and disadvantages.

1. **Bluetooth Low Energy**

Bluetooth Low Energy (BLE) is a special type of Bluetooth network designed specifically for small smart devices like Fitbit, wireless headphones, and keyboards. It is designed to behave like standard Bluetooth while consuming less power[2]. In terms of security, BLE uses the same protocols as standard Bluetooth to authenticate, authorize and encrypt data from source to destination. Smart lock companies also provide additional security in the form of smartphone apps. The user must first download an app on their device and pair the devices in order to start using the lock. The smart lock companies then ensure that once the lock is initially paired, it cannot be repaired with another device to ensure security.

The latest version of Bluetooth, Bluetooth 5.0, offers 2 security modes and 4 security levels that smart locks can use in order to provide security to its users. The lowest security level is level 1, which requires no pairing between the two devices and offers no encryption. Level 2 requires no pairing and offers 128-bit Advanced Encryption Standard (AES-128) as a method of encryption. AES is a Symmetric-key algorithm, meaning that the same key is used to decrypt and encrypt data. Level 3 requires pairing between the two devices and also uses AES-128 for encryptions. Level 4, the most secure level, requires pairing and uses Elliptic-curve Diffie–Hellman (ECDHE) as its method of encryption. ECDHE uses Elliptic-curve cryptography, which generates keys that are both shorter and more secure. The two security modes differ on the signing of the data, which is a way for a device to ensure that the data originates from the legitimate source and has not been tampered with. Security mode 1 does not have data signing while security mode 2 involves data signing between the source and destinate devices. While data signing makes the connection more secure, it takes more time, power, and computation power to execute. The level of total security is the combination of a security level and mode. For example, security mode 1, level 4 means that two devices must be paired, the data will be encrypted using ECDHE protocol, and the data will not be signed[3].

While seemingly secure, companies often neglect certain security features in favor of performance/cost or just because of pure incompetence. There is a history of Bluetooth hacks that exploit weakness and vulunterbies like the blueborne attack and the bleedingbit attack[4][5].

[2] https://www.keynie.com/blog/ble-technology-the-technology-behind-bluetooth-smart-locks
[3] https://duo.com/decipher/understanding-bluetooth-security
[4] https://www.armis.com/blueborne/
[5] https://www.armis.com/bleedingbit/

When it comes to hardware, bluetooth also has the limitations. As with all bluetooth devices, it has a small range, so the owner can only access when the lock is near. Bluetooth smart locks also requires an additional hub to access the internet, making the installation more complex and expensive.

2. **Wi-Fi**

The second and the least popular technology that smart locks use is Wi-Fi. The smart lock connects to the user's home Wi-Fi and become a part of the local network. One advantage of Wi-Fi smart locks is that it does not require any additional hubs or add-ons to be used to its fullest potential, as it will have full internet access via the user's home network. Wi-Fi smart locks also provide the longest range and the most data throughput out of the three technologies. However, these advantages also come at a cost — Wi-Fi smart locks take the most amount of power to operate, making it not as sustainable as the other options[6].

Wi-Fi smart locks are the most vulnerable to attack as they are directly connected to a home's router: one of the most vulnerable items in a home[7]. Even if the locks themselves are built to perfection, Wi-Fi smart locks are exposed directly from attacks on a home's router, making it unsafe

3. **Z-Wave**

Z-Wave is a wireless protocol consisting of low-energy radio waves designed for home appliances and gadgets. Z-Wave devices form a mesh network, a network in which the devices connect directly with one another. There is usually a central hub that all devices connect to that enable them to connect to the internet. Compared to BLE, Z-Wave uses similar power and has a larger range.

In terms of security, Z-Waves uses the same AES-128 encryption as Bluetooth security level 2. Z-wave protocols also require the user to follow a special procedure when pairing with their devices to provide further security. The technology is still at its infancy, and not much research has been done on its security and potential flaws.[8]

In summary, there are three wireless technology standards that power smart locks: Bluetooth, Wi-Fi and Z-Wave, each with their pros and cons. Bluetooth has robust security protocols and low power usage but requires a hub and has a limited range. Wi-Fi has the longest range and is stand-alone but has high power usage and vulnerability. Z-Wave provides a long-range with small power usage but also requires a hub.

---

[6] https://www.keymitt.com/blogs/wi-fi-and-bluetooth-in-iot-smart-lock-systems-and-why-do-we-need-both

[7] https://www.darkreading.com/network-and-perimeter-security/most-home-routers-are-full-of-vulnerabilities/d/d-id/1332987

[8] https://www.the-ambient.com/guides/zwave-z-wave-smart-home-guide-281

Historical Vulnerabilities

Much like other IoT devices, smart locks often contain vulnerabilities that can be exploited to various degrees. But before we discuss these vulnerabilities and exploits, it is important to know that almost always, **the vulnerabilities originate from faulty/careless implementations by the manufacturers.** These vulnerabilities don't come from Bluetooth or Z-Wave but the lack of security awareness from the makers of the locks. A research presented in DEFCON 2016 found that a large majority of smart locks are easily exploited, and yet **no manufacturers wanted to fix these vulnerabilities**[9]. Almost all smart lock-related vulnerabilities can be categorized into two sections: flaws with the hub and flaws with the lock/lock's app.

As Bluetooth and Z-wave smart locks need to connect to a hub to function, the hub itself becomes a potential vulnerability. In general, a vulnerability of the hub means that a hacker could break into the hub and access the devices it is connected to. With this access, a hacker can then easily unlock the smart lock. This vulnerability was found in July 2019 with Zipato's smart hubs. Researchers found that Zipato used the same private SSH key for every single hub, meaning that anyone on the same Wi-Fi network as the hub can assess the hub itself with root privilege and thus having the ability to directly control the lock. This is dangerous for home users but even more dangerous for complexes. In a private home, a hacker would first need to break into the Wi-Fi in order to access the lock; though very achievable due to the vulnerable nature of most routers, this requires multiple steps and can take time. However, apartment complexes and hotels connect their hubs on the same shared Wi-Fi. That means that anyone with access to the shared Wi-Fi can directly access the hub and unlock any door of their wanting in the whole building.[10]

The other, more common, area of vulnerability are the smart locks themselves. These vulnerabilities come in all varieties, ranging from credentials sent over plaintext to design flaws within guest systems. In the research presented at DEFCON 2016, the researchers successfully broke into 12 out of the 16 BLE smart locks remotely using a Bluetooth sniffer. Out of these 12, 4 smart locks sent passwords in plaintext. Other smart locks contained various encryption implementation issues that allowed the researchers to bypass the encryption without ever having to decrypt the keys[11].

In August 2016, the smart lock maker August was found to have a vulnerability regarding its guest access system. The lock had a feature that granted temporary access to other users, useful for visiting guests and Airbnb owners. However, instead of sending a temporary key to the guest, the lock would send a permanent key to the guest but with a time restriction on the app. That means that the guest can access and save the key and use the same key to operate the lock after their intended stay.

---

[9] https://www.cnet.com/how-to/procrastinators-heres-your-last-day-to-ship-holiday-gifts-from-amazon-walmart-and-best-buy/

[10] https://techcrunch.com/2019/07/02/smart-home-hub-flaws-unlock-doors/

[11] https://www.tomsguide.com/us/bluetooth-lock-hacks-defcon2016,news-23129.html

This poses a great danger to Airbnb users as they experience a lot of guest traffic[12]. In May 2019, this exact same flaw and more were discovered in locks made by Hickory. Researchers at Rapid7 found that Hickory locks granted guests full API access during their stay, which allowed guests to retain these privileges after their allotted time. Furthermore, the locks also transmitted credentials in cleartext as well as had insecure storage vulnerabilities.[13]

Action Item: Should I Get A Smart Lock?

The smart lock is a fast-growing industry still in its infancy. As more and more homeowners look towards "smart" home solutions, it is important to know the trade-offs between physical and smart locks. The general trade-off between physical and smart locks lies in their price, security, and convenience[14].

Price is perhaps the largest difference-maker to most consumers. An average physical lock costs around $20-$30 while an average smart lock costs around $200-$300.

The trade-off of security between the two is a gray area. While smart locks are plagued with various vulnerabilities, it could also help with security. Many smart locks have additional security features such as cameras that help a homeowner better protect their homes. When looking at the secutiy of smart locks, it is important to keep in mind that security flaws within the locks come from bad implementation/code from the manufactures. So in theory, there could exist a product that is secure. On the topic of smart lock security, experts seem to have a consensus: as of now, smart locks should not be trusted. Quoting Jeremiah Grossman, Chief of Security Strategy at cybersecurity firm SentinelOne, "Would I personally entrust the security of my home to such a device? Not at the moment, but in the future as the devices get better and more secure I might trust them more.[15]"

When it comes to convenience, smart locks take the edge. Having a smart lock means that one would never have to leave a spare key as there are multiple ways of opening the lock. A smart lock allows the user to control the lock remotely and grant guests temporarily control, saving time and effort. While these features might not be important for a home user, it can be greatly helpful for special circumstances such as Airbnb and complexes.[16]

Personally, I see the smart lock as an industry that still has a long way to go. While smart locks are functionally developed, it still suffers basic security flaws like transmitting credentials in plaintext or hardcoded keys. I believe that this issue speaks more about the attitude of smart lock companies. Currently, most of the smart lock companies don't have the right focus and attitude about the

[12] https://www.cnet.com/how-to/procrastinators-heres-your-last-day-to-ship-holiday-gifts-from-amazon-walmart-and-best-buy/

[13] https://blog.rapid7.com/2019/08/01/r7-2019-18-multiple-hickory-smart-lock-vulnerabilities/

[14] https://www.scmp.com/native/lifestyle/topics/premier-living/article/3006243/are-smart-locks-safe-hear-what-security

[15] https://lifehacker.com/we-asked-five-security-experts-if-smart-locks-are-ever-1797910643

[16] https://www.lifewire.com/smart-locks-4159894

security of their products. When researchers contacted the 12 companies with vulnerable locks, **not a single one responded.** I believe that while smart locks are beneficial to certain demographics, it should not be recommended to the average homeowner as both the widespread security flaws and the companies' nonresponsive attitude towards these flaws project a bad trend for the industry.

Conclusion

The bottom line of all this is that no lock, smart nor physical, is safe. While having a smart lock adds additional vulnerabilities to a home's security, it is important to keep in mind that having a hacker break into a home via a vulnerable smart lock is extremely rare. In the present day, a home break-in is much more likely through lock picking or simply breaking a window. Ultimately, the decision of getting a smart lock should be the added utility to the consumer's life. The potential risk of having a smart lock should not drive off any potential consumers that would benefit from its convenience. Having said this, the industry as a whole is growing rapidly economically but is stagnant in its security. We are seeing flaws in 2016 locks being repeated in 2019 locks due to manufacturing negligence and disinterest in security. If this trend of negligence continues as more homes install smart locks, it could cause a major security issue.