Published in: Bravo, J., Ochoa, S., Favela, J. (eds) Proceedings of the International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2022). UCAmI 2022. Lecture Notes in Networks and Systems, vol 594. Springer, Cham. https://doi.org/10.1007/978-3-031-21333-5_98

Smart-lock attack through bluetooth communications replication

Cándido Caballero-Gil[1][0000−0002−6910−6538], Rafael Álvarez[2][0000−0002−8254−6255], Jezabel Molina-Gil[1][0000−0001−7702−9264], and Candelaria Hernández-Goya[1][0000−0002−9468−708X]

[1] Department of Computer Engineering and Systems, University of la Laguna, Tenerife, Spain,
{ccabgil,jmmolina,mhgoya}@ull.edu.es
[2] Department of Computer Science and Artificial Intelligence, University of Alicante, Spain.
ralvarez@ua.es

Abstract. The rise of smart locks has made them present in many homes and business in a large number of countries. This is due to their user-friendly design and the flexibility they offer. Smart-locks usually offer a convenient and secure way to unlock the door without the need for keys. However, as with any new technology, there are potential security risks that need to be considered. In particular, bluetooth security of smart-locks is very important because a leak can provide unauthorized access. Bluetooth is a wireless technology that allows devices to communicate with each other. It is used in a variety of devices, including smartphones, laptops, and now smart-locks. While Bluetooth offers many benefits, it also poses a security risk if it is not properly secured. To ensure the smart-lock is secure, one of the security factors must be considered is the Bluetooth security. This will ensure that only authorized users can access the home or business. In this work, the security of the Nuki smart-lock through bluetooth communications have been checked.

Keywords: Smart-Lock, Bluetooth, Cybersecurity, Cyber-Attack

1 Introduction

Technological advancements have allowed for the development of smart-locks, which provide an increased level of security for homes and businesses. With this kind of device, a door can be opened or unlocked using a mobile device, remote control, NFC card, or even a fingerprint or numeric code. In addition to this type of access, many of these locks can be considered smart as they can store and query an access log, communicate and synchronize with calendars to allow or withdraw access based on determined conditions, some of these locks even allow the access by entering a code when touching the door.

However, as with any new technology, there are always potential risks and vulnerabilities that must be considered. Here we will discuss some of the cybersecurity risks associated with smart-locks, and how to mitigate them. One of the

most common risks associated with smart-locks is that of hacking [7]. If a hacker is able to gain access to the lock's security, for example, capturing packets with the Wireshark tool [4] and a Bluetooth Sniffer, they could potentially unlock the door without the owner's permission. To mitigate this risk, it is important to ensure that the lock's security is enough, and only authorized users have access.

Another risk to consider is that of physical tampering. Smart-locks are typically installed on the exterior of doors, making them more susceptible to tampering. If someone were to physically tamper with the lock, they could potentially bypass the security measures and gain access to the property. To mitigate this risk, it is important to choose a smart-lock that is tamper-resistant and has a robust physical security design.

Finally, it is also important to consider the risk of human error. While smart-locks are designed to be user-friendly, there is always the potential for user error. For example, if a user forgets to lock the door, or fails to properly secure the lock, this could lead to a security breach. To mitigate this risk, it is important to educate users on the proper use of smart-locks, and to ensure that they are aware of the importance of security.

In the state of art, the paper [9] demonstrate several practical attacks based on the threat models toward August smart-lock including handshake key leakage, owner account leakage, personal information leakage, and denial-of-service (DoS) attacks. Authors in paper [3] propose several defenses that mitigate different attacks. One of these defenses is a novel approach to securely and usably communicate a user's intended actions to smart locks, which was prototyped and evaluated.

1.1 Nuki smart-lock

The Nuki lock is a motorized lock, that is, there is a motor that turns the key automatically. Its installation is very simple. It adapts to the cylinder that the user have in the door and one of the keys is used inserted in the smart-lock to open the door, the key could also be used to open if the door has a double clutch cylinder. It is not necessary to disassemble the original lock because it is adhered to the door by a very strong 3M adhesive or screws.

The Nuki Smart Lock [8] has been gaining considerable popularity in recent years. Nuki stands out for its security and easy installation. The Nuki lock is the first smart lock in Europe that opens doors with the help of a smartphone. The lock has also a remote control, a numeric keypad. The Nuki lock provides great convenience when it comes to use as the door can be opened from a cell phone, smartwatch or Tablet. In addition, temporary or permanent access can be given to other people, such as family, friends or cleaning services for a specific schedule. Furthermore, thanks to its hands-free system, the door will open when it detects the cell phone, providing great convenience to the user when it comes loaded or simply for greater speed. In case it is a company or tourist accommodation like Airbnb, a temporary code can be provided to users to prevent the loss and copying of keys. This lock allows to have several users registered at the same time, sending them an invitation code, which can be withdrawn as soon as desired.

The reason to choose this smart-lock was that this device is one of the most famous in the European market.

2 Hardware and software for the bluetooth attack

Adafruit bluefruit LE Sniffer Adafruit bluefruit LE Sniffer [1] is programmed with a firmware image that makes it an easy-to-use firmware image that makes it an easy-to-use Bluetooth Low Energy (BLE) sniffer.

Antena Bluetooth CBT40NANO The CBT40NANO Bluetooth Nanoadapter [14] is used to create a wireless connection to other Bluetooth devices. In this project it is used to create a connection through a virtual machine, running the Linux operating system, to the lock. In this way, the traffic necessary to unlock the lock can be replicated.

Wireshark Wireshark is the most widely known and used packet analyzer in the world and is the program used in this project to analyze the packets sent between the mobile device and the lock. Thanks to this program, you can capture and analyze in detail all network traffic entering and leaving your PC. This free program allows you to perform a deep inspection of hundreds of protocols, as it supports physical layer protocols, link protocols, network protocols, transport layer and also application layer.

Gatttool Gatttool [2] is a tool that allows obtaining information or manipulating attributes of a BLE device. In this project we have implemented the writing of keys in the lock thanks to this tool.

3 Bluetooth replication attack for the smart-lock

The process of locking and unlocking the lock is very simple. The user must enter the app with the username used to register previously. Then the app will take him to the main menu of the application, where if there is already a lock associated, it will appear with the options to unlock, sliding the finger to the right, or lock, sliding the finger to the left.

In order to study the security of the smart-lock, we will check how the sending of information between the application and the lock works. The objective of this process is to be able to capture the traffic when the lock connects with the smartphone and sends it the key to unlock the door, and then try to replicate that traffic. For this purpose, we use a tool to make the connection between our computer, the application and the lock. In this project we use the Adafruit bluefruit LE sniffer, which allows us to capture and analyze the packets in transit between the devices. To analyze the traffic captured in the Wireshark application, we first need to link the information received by the sniffer. The nRF Sniffer for Bluetooth LE program is used for it. This tool allows us to see in real time all the devices that are being captured by the sniffer in order to capture the data to later filter that content in Wireshark and check the information in detail. Thanks to this tool we can see all the available nearby Bluetooth devices

with their respective MAC addresses. In addition to this, it presents a guide of all the useful commands that we can use with this tool.

3.1 Nuki lock bluetooth attack

Nuki lock has been studied in this project. Next, some technical concepts about it and its operation will be shown, and then proceed to the analysis of its security. It is especially noteworthy that the Nuki lock operates at the highest level of security encryption, as it uses AES with 256-bit keys. AES is a symmetric block cipher, which means that it encrypts and decrypts data in blocks of 128 bits each. To do this, it uses a specific cryptographic key, which is effectively a set of protocols for manipulating information. This key can be 128, 192 or 256 bits in size. AES-256, the 256-bit key version of AES, is the encryption standard used by LE VPN. It is the most advanced form of encryption and consists of 14 rounds of substitution, transposition and mixing for an exceptionally high level of security. Its larger key size makes it essentially unbreakable, meaning that even if hacked, the data would be impossible to decrypt.

The Nuki lock stands out in Europe for its good reviews regarding its security, therefore, it has been analyzed if a package replication would hack it.

With the Adafruit bluefruit LE sniffer and its nRF Sniffer for Bluetooth program to detect nearby BLE devices, we connect to the Nuki lock to later analyze the packets sent and received in Wireshark. Once Wireshark has been started and the 'btatt' filter has been introduced to acquire only Bluetooth traffic, we can unlock the lock and check what information is reaching us and if it will be possible to hack it. In Figure 1 we can appreciate the communication between the Nuki lock and our Samsung mobile device.

The protocol used for the connection is also ATT where the attributes sent are stored, but in the column indicating the packet information, slight formatting changes can be observed, which will be discussed later. In this case, we can see that several write requests are made to the lock to send the keys with Handle 0x0092 with the command:

Sent Write Request, Handle 0x0092

Therefore, we must collect all the values that are sent in order to later perform their replication. In order to see these values, we are interested in the information provided by the ATT protocol. Once we have all the keys that are sent, we can replicate the traffic again from our virtual machine. First, we check that we are receiving connection from the Nuki lock with the hcitool tool and, since we get a signal, we can run our bash script, previously modified with the values found in Wireshark. However, even though the values are correctly written to the lock, it fails to unlock it. This is because, when unlocking the door, Nuki instantly changes the key for the next opening, being unfeasible to hack the lock with this method, since the previously collected keys would be automatically obsolete.

In the following, we will explain in detail how the encryption works in the Nuki lock [6]. This lock uses the principle of end-to-end encryption, i.e., it applies a cipher to the key in such a way that only the receiving device can decrypt it. To establish communication between the Nuki app and the Smart Lock, a

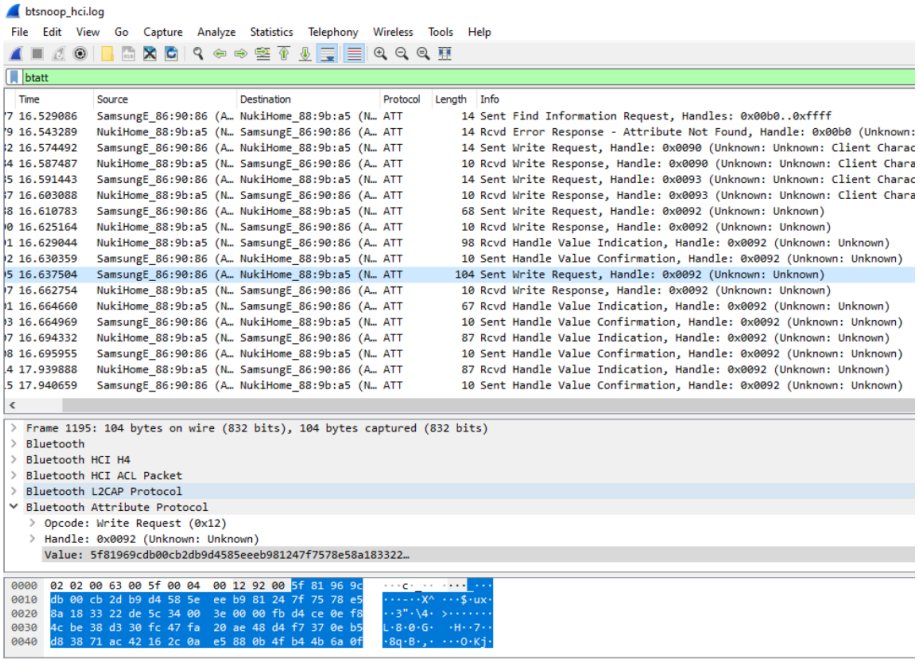

Fig. 1. Capturing packets traffic of Nuki Smart-Lock using Wireshark

proprietary key is used that is known only to both devices. To protect against attackers, the data is encrypted before it is transmitted by the sender (the Nuki app). This is done using the NaCl (Networking and Cryptography library) process [5]. In this process, unique combinations of numbers and letters are used only once. This data is transferred via Bluetooth and decoded again when received by the receiver (Nuki Smart Lock).

1. The Nuki app sends the "unlock" instruction and encrypts it in such a way that only the app and Nuki Smart Lock know the key.
2. The Nuki app transfers the encrypted message via Bluetooth to the lock.
3. Nuki Smart Lock knows the key and therefore can decrypt the contained message and execute the "unlock" command.
4. In the unlocking process, the Nuki app receives a random number. The "unlock" instruction can only be sent to the lock when it necessarily contains an identical random number.

If another unlock instruction with the same random number is subsequently sent to the door lock, Nuki Smart Lock rejects the instruction. This analysis shows us that the security level of Nuki is high, as reported by the manufacturers, and that overall it is a lock that the market can currently rely on. However, since the packet replication method used in this project is only one of the options for hacking, this research does not imply that there may not be another procedure for unlocking the lock and that this lock may end up being vulnerable to attack.

4 Conclusions and future work

This paper tests the security of the *Nuki Smart-lock* though bluetooth communications. Detailed research has been carried out on how the door opening process works and what information is sent through the devices involved. In addition to this, the replication of packets obtained with the intention of unlocking the lock from our computer has been tested. Throughout the research, it has been verified that Nuki lock has a good level of security in this aspect.

However, new methods could be found to perform the attack and it is possible that the security of the Nuki lock could be broken. The current work is quite flexible and could be expanded much further in the future.

In addition, in this work only one method to unlock the lock is contemplated, however, many more procedures may exist or be created to unlock the lock from other information or by attacking another point of the connection. Considering the advancement of technology and market competition, manufacturers will strengthen the security of their smart-locks in upcoming releases. Even so, there is a wide variety of brands on the market that can be analyzed for vulnerabilities.

Acknowledgements Research supported by the Spanish Ministry of Science, Innovation y Universities (MCIU), the State Research Agency (AEI) and the European Regional Development Fund (ERDF) under project RTI2018-097263-B-I00.

References

[1] Adafruit. *Bluefruit LE Sniffer - Bluetooth Low Energy (BLE 4.0) - nRF51822*. `https://www.adafruit.com/product/2269`. (Visited on 2022).

[2] Gatttool. *Gatttool*. `http://manpages.ubuntu.com/manpages/cosmic/man1/gatttool.1.html`. (Visited on 2015).

[3] Grant Ho et al. "Smart locks: Lessons for securing commodity internet of things devices". In: *Proceedings of the 11th ACM on Asia conference on computer and communications security*. 2016, pp. 461–472.

[4] Ulf Lamping and Ed Warnicke. "Wireshark user's guide". In: *Interface* 4.6 (2004), p. 1.

[5] *NaCl*. `https://en.wikipedia.org/wiki/NaCl_(software)`. (Visited on 2022).

[6] *Nuki Encryption*. `https://nuki.io/es/blog/sientete-seguro/seguridad-en-primer-plano-concepto-de-cifrado-de-nuki-explicado-de-forma-sencilla/`. (Visited on 2022).

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

[8] Nuki Home Solutions. *Nuki Smart Lock*. `https://nuki.io/es/smart-lock/`. 2013. (Visited on 2022).

[9] Mengmei Ye et al. "Security analysis of Internet-of-Things: A case study of august smart lock". In: *2017 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*. IEEE. 2017, pp. 499–504.