University of Amsterdam

Nuke the NUKI

Research proposal

September 2019

Students:
M. Badias Simo

W. Bakker

T. Slokker

W. van Steenbergen

Tutor:
Peter Prjevara; Arno Bakker

Lecturer:
Jaap van Ginkel

Course:
Security of Systems and Networks

1 Introduction

Following the adoption of smart lights, such as Philips Hue and IKEA TRÅDFRI, smart door locks have become another widely available option for home automation. The ideology behind home automation is to improve the ease of use of these common devices. When it comes to smart locks, there is another concern. Namely, the smart lock has to be secure enough to protect your home, or at least be as secure as a traditional door lock. A smart lock adds new attack vectors to break into a home.
For this project we have selected the Nuki Smart Lock 2.0, a electronic door lock made by Nuki Home Solutions GmbH, based in Austria. This lock comes as an extension to traditional door locks, it is able to open the door on request by turning the key from inside the home. It does not replace the already installed traditional lock mechanism. We have chosen this lock specifically because it is recommended by AV-Test, an independent IT institute which certifies products based on a selection of criteria. Additionally, Nuki published an extensive blog post in which they made several claims about smart locks being safe to use. The claims are that using a smartphone to lock the door is not unsafe, and that smart locks are not easy to hack. We want to put these claims to the test.

2 Scope

This section describes the features of the product that are of interest, and what we will be basing our research questions on.
The smart lock has a feature that will from hereon be referred to as a hands-free unlock. This feature will send an unlock request to the lock when the user is in close proximity to the lock. We want to investigate how this feature determines whether the user is close to the lock, and what data it transmits while the user does not meet the criteria for hands-free unlock.

The Nuki data protection declaration Nuki (2018b) lists several types of information the service collects about the user, such as age, sex, languages, interests, and country of residence. Most notably there is no information about the lock access history, this history is described as a feature on the product page: "See exactly who locked and unlocked your door, and when. Wherever you are." Nuki (2018a). We want to look into this access history and how it is transferred between devices. In a more general sense we aim to look into all the data that is transferred between the devices and the central server.

Investigating the security protocol implementation between the app and lock has been set as a stretch goal. Nuki provides some transparency on the security concept Nuki (2015). The simplified encryption concept can be seen from Figure 1 and is a very basic description of a secure Bluetooth implementation. On top of this secure layer, Nuki specifies they implemented a challenge response type scheme which eliminates replay attacks.

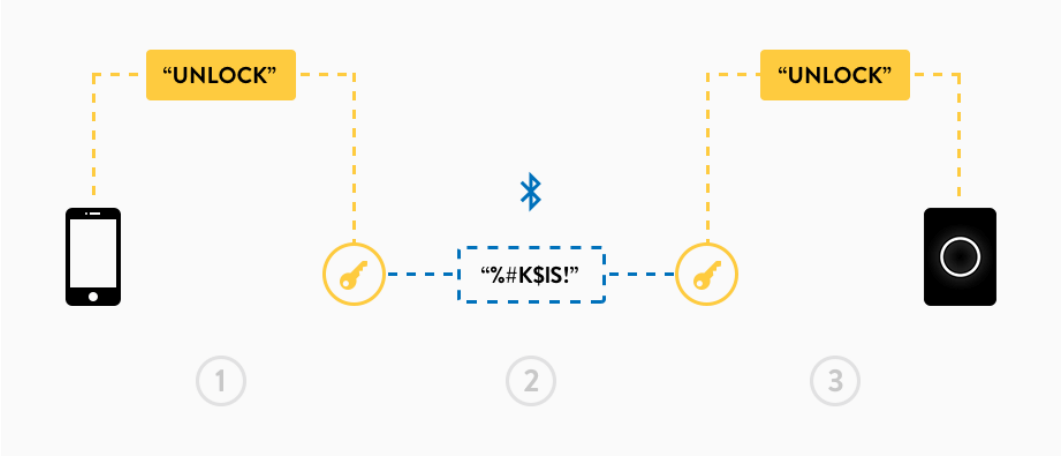

Figure 1: Nuki Encryption Concept

3 Research Question

The main research question is: *"Is the Nuki Smart Lock 2.0 as secure as the manufacturers claim it to be?"*
To formulate an answer to this question, the following sub questions need to be researched:

1. *What information is used in the hands-free unlock?*
2. *Can we trigger hands-free unlock, and unlock the door, remotely?*
3. *What data passes through the Nuki servers, and is it in an unreadable format?*
4. *Is the lock log information transferred in true end-to-end encryption between devices?*
5. *Stretch goal: Is the security protocol between app and lock properly implemented?*

4 Related Work

As mentioned before, AV-Test has recommended the Nuki Smart Lock 2.0. On their site Clausing (2019) they show what they tested the Smart Lock, and its components, on and what the results were. However, the presented results did not give a clear method to reproduce the tests. We contacted them to give us more insight into their testing method. We got a response in which they informed us about the testing criteria they used. They did not present us with their test results. Because the test performed by AV-Test are not scientifically reproducible this research will try to give a deeper insight in the security of the Nuki Smart Lock 2.0.

White-hat hackers extensively researched smart door locks. In many cases these researchers found security flaws to open the lock without authentication. This could be done because of development errors, weak- data security and passwords. Almost all of these experiments are based on Man-In-The-Middle (MITM) attacks. After the communication was intercepted there were pre-written scripts. These scripts would exploit previously mentioned security flaws or brute force the password on the device. Security (2016)

5 Approach & Methods

To carry out the project, a controlled test environment will have to be set up. Two similar devices running Android will be used to install the Nuki App. Also, both devices are going to be connected to the Nuki Smart Lock. Each one will consult the lock access history of the other in order to check if the data is end-to-end encrypted between the two devices or if it is consulted, modified or stored by the Nuki central server.

Within this environment the network traffic of the application will be captured and analyzed. The capture will be done within the device itself or with a secondary machine that will run a wireshark-type of application. With the obtained information the network packets will be scanned for user sensitive data.

6 Requirements

This Research will require some items to be able to succeed. The following things are needed:

- **Two Nuki Android Apps** - In order to test the data transmission to the Nuki central server.
- **Two similar devices running Android** - Where we are going to install and test the Nuki Apps.
- **Nuki Smart lock 2.0** - To set up a test environment, connect the lock to the app and generating the needed data.

7 Planning

The official research will take 5 weeks. It starts on Monday 23 September 2019 and will end on Friday 25 October 2019. in Table 1 the planned activities/tasks are stated.

Weeknumber	Starting Date	Tasks
3	16 September	Final project proposal (20 September)
4	23 September	Setting up test setup
5	30 September	Performing tests and processing results
6	07 October	Performing tests and processing results
7	14 October	Writing report
8	21 October	Project presentations 21 October & Definitive version report 25 October

Table 1: Project Planning

8 Ethics

The focus of our work can be considered an attack to the integrity of the Nuki lock and its Android mobile application as well as to the privacy and security of their users. Also, our attempts at collecting the data between the Nuki App and the Central Server could compromise third parties information. However, it is well known that an offence research is needed in order to improve the defense of a technology and for being prepared for real criminal attacks.

Moreover, Nuki promises to their clients that their system has no weakness and nothing is been said about the activity lock information. We believe that, as tech researchers, it is our responsibility to corroborate that what business claims are honest and accurate. As it has been seen, there is not a perfectly secure system because it's hard to get everything right Morrissey (2019). Also, a lot of companies collect data (legally or not) to improve their products or to simply sell it. BBC (2018)

To avoid compromising third parties data, our test will be conducted under an experimental environment using our personal devices. The analysis on physical Nuki devices will be performed only using devices acquired for the experiments. Also, at the end of the project, any detected weakness on the application or to its connection with the lock, as well as any irregularity with the collected data, will be reported to Nuki. This way, the security problems might be fixed.

References

BBC. (2018). *Facebook's data-sharing deals exposed.* Retrieved from `https://www.bbc.com/news/technology-46618582`

Clausing, E. (2019, May). *Certified! nuki smart lock 2.0.* AV-Test. Retrieved from `https://www.iot-tests.org/2019/05/certified-nuki-smart-lock-2-0/`

Morrissey, J. (2019). *In the rush to join the smart home crowd, buyers should beware.* Retrieved from `https://www.nytimes.com/2019/01/22/business/smart-home-buyers-security-risks.html`

Nuki. (2015). *Nuki encryption concept.* Retrieved from `https://nuki.io/en/blog/nuki-news/nuki-encryption-concept/`

Nuki. (2018a). *The nuki activity log.* Retrieved from `https://nuki.io/en/blog/nuki-news/the-nuki-activity-log/`

Nuki. (2018b). *Nuki data protection declaration.* Retrieved from `https://nuki.io/en/service/privacy/`

Security, M. (2016). *Picking bluetooth low energy locks from a quarter mile away.* Retrieved from `https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20Rose-Ramsey-Picking-Bluetooth-Low-Energy-Locks-UPDATED.pdf`