Locking Down CNI:
An Evaluation of the Cyber Security of IoT Smart Locks for Integration into Critical National Infrastructure

by

Callum Giblin

September 2024

Abstract

This evaluation project investigates the security of various Internet of Things (IoT) smart locks, through comprehensive penetration testing methods to assess their suitability for securing Critical National Infrastructure (CNI) sites that house Operational Technology (OT) devices. The research aims to identify and evaluate potential vulnerabilities in smart lock systems, which could make them less suitable to their non-smart counterparts or could add further vulnerabilities to an OT network. The penetration tests employed include wireless network scanning & attacks, Radio Frequency Identification (RFID) based attacks, and Bluetooth attacks. These findings are documented with vulnerabilities categorised according to the Common Vulnerability Scoring System (CVSS) detailing severity and potential impact. Recommendations for mitigating identified risks are provided where appropriate. This project accentuates the necessity of hardened security measures for IoT devices in protecting CNI and identifies key areas for enhancement in current smart lock technologies.

Contents

Abstract.....i

Contents.....ii

List of Figures.....v

List of Tables.....vii

List of Acronyms and Abbreviations.....viii

Chapter 1 Introduction.....1

1.1 Problem Description.....1

1.2 Proposed Solution.....2

1.3 Methodology and Technology.....4

1.4 Ethical, Legal and Social Issues.....5

1.4.1 Ethical Considerations.....6

1.4.2 Legal Considerations.....6

1.4.3 Social Considerations.....6

1.5 Resources, Skills and Methods.....6

1.6 Project Planning.....9

Chapter 2 Ikea Rothult Penetration Test.....10

2.1 Engagement Contacts:.....10

2.2 Purpose & Scope.....10

2.3 Summary of Findings.....11

2.4 Detailed Findings.....12

2.4.1 1. Weak RFID Encryption.....12

2.4.2 2. Authentication Vulnerability.....13

2.4.3 3. Cooling-Off Period.....14

2.5 Detailed walkthrough.....14

2.5.1 RFID Attacks on Ikea E1777 RFID Keycard.....14

2.5.2 RFID Attacks on Ikea E1778 Rothult Lock.....17

Chapter 3 TTLock Padlock Penetration Test.....19

3.1 Engagement Contacts....19
3.2 Purpose and Scope....19
3.3 Summary of Findings....21
3.4 Detailed Findings....21
3.4.1 1. Default MIFARE Classic 1K Keys....21
3.4.2 2. Weak RFID Encryption....22
3.4.3 3. BLE Authentication Vulnerability....23
3.4.4 3. BLE Encryption Vulnerability....24
3.5 Detailed Walkthrough....25
3.5.1 RFID Attacks on TTLock RFID Key Fob....25
3.5.2 RFID Attacks on TTLock Padlock....30
3.5.3 BLE Attacks on the TTLock Padlock....31
Chapter 4 Yale Conexis L1 Penetration Test....35
4.1 Engagement Contacts....35
4.2 Purpose & Scope....35
4.3 Summary of Findings....37
4.4 Detailed Findings....38
4.4.1 1 Weak RFID Encryption....38
4.4.2 2. BLE Authentication Vulnerability....39
4.4.3 3. BLE Encryption Vulnerability....40
4.5 Detailed Walkthrough....41
4.5.1 RFID Attacks on Yale Smart Living Keycard....41
4.5.2 RFID Attacks on Yale Conexis L1 Lock....45
4.5.3 BLE Attacks on Yale Conexis L1 Lock....46
Chapter 5 eLinkSmart Padlock P5BF Penetration Test....51
5.1 Engagement Contacts....51
5.2 Purpose & Scope....51

5.3 Summary of Findings..... 52
5.4 Detailed Findings..... 53
5.4.1 1. BLE Authentication Vulnerability..... 53
5.5 Detailed Walkthrough..... 54
5.5.1 BLE Attacks on eLinkSmart Padlock P5BF..... 54
Chapter 6 Conclusion..... 57
6.1 Theme of Findings..... 57
6.2 Recommendations from Findings..... 57
6.3 Future Work..... 58
Chapter 7 Critical Evaluation..... 59
7.1 Strengths and Achievements..... 59
7.2 Project Limitations..... 59
Reference list / Bibliography..... 61
Appendix 1 Risk Severity Ratings..... I
Appendix 2 RFID Technology..... II
Appendix 3 BLE Technology..... IV
Appendix 4 Magic Cards..... V
Appendix 5 LEPSI Form..... VI

List of Figures

Figure 1.1 - Price of Copper 2019-2024 (Trading Economics, 2024) 1

Figure 1.2 Danger of Death Signage on an Electrical Substation (Giblin, C. 2024a) 2

Figure 1.3 Project Gantt Chart 9

Figure 2.1 Ikea E1778 Rothult Lock in Engaged (left) and Disengaged (right) states. 11

Figure 2.2 Ikea E1777 RFID Keycard Front (left) and Rear (right). 11

Figure 2.3 Proxmark3 “hf search” Command. 15

Figure 2.4 Proxmark3 "hf st info" Command. 16

Figure 2.5 Proxmark3 "hf st sim" Command. 17

Figure 2.6 Proxmark3 "hf st ndef" Command. 17

Figure 2.7 Proxmark3 "hf st sim" Command. 18

Figure 2.8 Flipper Zero GUI Showing the Fuzzer Tool Performing a Brute-Force Attack 18

Figure 3.1 TTLock Padlock 20

Figure 3.2 TTLock RFID Key Fob 20

Figure 3.3 Proxmark "hf search" command. 26

Figure 3.4 Proxmark3 "hf mf auto" Command. 27

Figure 3.5 Proxmark3 "hf mf csetuid" Command. 27

Figure 3.6 Proxmark3 "hf mf auto" Command to Verify Magic Card Keys 28

Figure 3.7 Flipper Zero Waiting for Key Fob 29

Figure 3.8 Flipper Zero TTLock RFID Key Fob Read Successfully. 29

Figure 3.9 Flipper Zero Emulating TTLock Key Fob 30

Figure 3.10 Flipper Zero Fuzzer Tool 31

Figure 3.11 Successful BLE Connection from the nRF52840 to the TTLock Padlock 32

Figure 3.12 Enumerated information from the TTLock via the nRF52840. 33

Figure 3.13 Wireshark Analysis of a SCAN_RSP from the TTLock Padlock 34

Figure 3.14 Enumerated Data from The Unencrypted BLE Data Packet 34

Figure 3.15 Wireshark Analysis of a CONNECT_IND Packet containing a Channel Map. 34

Figure 4.1 Yale Conexis L1 Lock Front (left) and Rear (right). 36

Figure 4.2 Yale Smart Access Module Side View (left) and Rear View (left). 36

Figure 4.3 Yale Smart Living Keycard 37

Figure 4.4 Proxmark3 “hf search” Command Performed on the Yale Smart Living Keycard 41

Figure 4.5 Proxmark 3 "hf search" Command Performed on the Magic Card 42

Figure 4.6 Magic MIFARE Classic 1K Keycard. 42

Figure 4.7 Proxmark 3 "hf mf auto" command on the Yale Smart Living Keycard 43

Figure 4.8 Proxmark3 "hf mf csetuid" Command. 43

Figure 4.9 Proxmark3 "hf mf restore" Command. 44

Figure 4.10 Block Dumps from the Magic Card and Yale Smart Living Keycard, Block 8 (Highlighted) shows a different block on each card. 45
Figure 4.11 Successful BLE Connection from the nRF52840 to the Yale Conexis L1 Lock 47
Figure 4.12 nRF Connect Application Logs 47
Figure 4.13 Device information Broadcast via BLE from the Yale Conexis L1 Lock 48
Figure 4.14 Commands Written Successfully to the Yale Conexis L1 via the nRF Connect Application 49
Figure 4.15 Identified Broadcasts from the Yale Conexis L1 50
Figure 4.16 Inspection of a SCAN_RSP Broadcast packet sent by the Yale Conexis L1 50
Figure 5.1 eLinkSmart Padlock P5BF 52
Figure 5.2 Successful BLE Connection from the nRF52840 to the eLinkSmart Padlock P5BF 55
Figure 5.3 nRF Connect Logs Showing the Connection and Subsequent Disconnection to the eLinkSmart Padlock P5BF 55
Figure 5.4 nRFConnect Sending Hexadecimal Codes via the 2ADF Service. 56
Figure 7.1 Bluetooth Enabled Device Shipments by Radio Version IV

List of Tables

Table 1.1 Smart Lock Technology Matrix 5
Table 1.2 Resources, Skills and Methods Required. 8
Table 2.1 Engagement Contacts for the Ikea Rothult Penetration Test 10
Table 2.2 In-Scope Assets. 10
Table 2.3 Ikea Rothult Finding Severity Summary 11
Table 2.4 Ikea Rothult Findings Summary 12
Table 3.1 Engagement Contacts for the TTLock Padlock Penetration Test 19
Table 3.2 In-Scope Assets. 19
Table 3.3 TTLock Padlock Finding Severity Summary 21
Table 3.4 TTLock Padlock Findings Summary 21
Table 4.1 Engagement Contacts for the Yale Conexis L1 Penetration Test 35
Table 4.2 In-Scope Assets. 35
Table 4.3 Yale Conexis L1 Finding Severity Summary 37
Table 4.4 Yale Conexis L1 Findings Summary 38
Table 5.1 Engagement Contacts for the eLinkSmart Padlock P5BF Penetration Test 51
Table 5.2 In-Scope Assets. 51
Table 5.3 eLinkSmart Padlock P5BF Finding Severity Summary 52
Table 5.4 eLinkSmart Padlock P5BF Findings Summary 53
Table 7.1 Likelihood and Impact Levels Matrix I
Table 7.2 Overall Risk Severity I

List of Acronyms and Abbreviations

AES	Advanced Encryption Standard
BLE	Bluetooth Low Energy
CAF	The Cyber Assessment Framework
CEH	Certified Ethical Hacker
CNI	Critical National Infrastructure
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DoS	Denial of Service
GDPR	General Data Protection Regulation
HTB	Hack The Box
HV	High Voltage
IoT	Internet of Things
IP	Internet Protocol
LAN	Local Area Network
LV	Low Voltage
MITM	Man-In-The-Middle
NCSC	National Cyber Security Centre
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NIS	Networks & Information Systems
OT	Operational Technology
OWASP	Open Web Application Security Project
PLC	Programmable Logic Controller
RFID	Radio Frequency Identification
RTU	Remote Terminal Unit
UID	Unique Identifier

Chapter 1 Introduction

1.1 Problem Description

Currently, UK Distribution Network Operators (DNO) that hold the licenses to supply electricity across various parts of the UK within Critical National Infrastructure (CNI) are at a high risk of cyber-attack. According to the NCSC Director of National Resilience, Jonathan Ellison (2024), the cyber threat to services on which we all rely, such as water, power and healthcare, is one which we must continue to urgently address. Recently in the Ukraine, there have been attacks on the country's power grid, with researchers believing that the Russian military group Sandworm is responsible (Tidy, 2022). The CNI of countries globally are of interest to various threat actors, from "State Sponsored Hackers" to "Hacktivists" who may wish to disrupt the flow of electricity or damage the key Operational Technology (OT) components that are vital in the distribution of energy.

The OT components, such as Remote Terminal Units (RTU), and Programmable Logic Controllers (PLC), are connected to the OT Network, often segregated in the Purdue model, the model used to define best practices for the relationship between industrial control systems and business networks (SANS, 2021). Some of these OT Components are geo-located in electrical substations across the licence area of a particular DNO, each DNO will have thousands of substations, each supplying electricity to the surrounding area. Substations can come in varying forms, from large High Voltage (HV) substations taking up on average 60 square meters, to Low Voltage (LV) substations, occupying around 4 square meters per substation.

DNOs have seen a concerning trend of unauthorised break-ins into these substations. For 2016, DNO SP Energy Networks reported a 607% increase in unauthorised access and theft from electrical substations (Fitzsimmons, 2016). According to statistics provided by Trading Economics, in the past 5 years, the price of copper has steadily increased (see Figure 1.1. below), indicating a direct correlation between the cost of copper and the unauthorised break-ins at electrical substations.

Figure 1.1 - Price of Copper 2019-2024 (Trading Economics, 2024)

Break-in through “forced entry,” for example cutting off a padlock is possible, however, the locks used on substations are usually accredited by BS-EN-12320, a standard set by the British Standards Institution and are tested for resistance against a variety of known manual attacks. This means that locks that are certified and graded to withstand attacks such as the use of an angle grinder for a specific amount of time that would likely warrant unwanted attention to the crime taking place. If there is no damage to the door or the locking mechanism, this would suggest that the criminal has a physical key or are gaining entry through lock picking.

The most common crime that is seen when unauthorised access is gained into these substations is the theft of copper earthing cables, which can then be sold. However, as these substations contain sensitive OT technology, there is a concern that cyber criminals could break into the substations and have direct access to the OT network. They could, for instance, plug directly into a PLC via an RJ45 cable and perform in-depth network scanning, DOS attacks and more.
There are also more general concerns about protecting these geophysical locations, such as:

- Theft of raw materials, such as copper, that can be sold for a profit by criminals.
- Risk of injury or death to the public. (See Figure 1.2 below)
- Risk of disruption to infrastructure due to damaged equipment.

Figure 1.2 Danger of Death Signage on an Electrical Substation (Giblin, C. 2024a)

1.2 Proposed Solution

One potential solution to this problem is the implementation of smart Internet of Things (IoT) locks, as an alternative to traditional (non-smart) locking mechanisms. With smart locks being connected through the Internet of Things, they can add features such as remote access control, real-time monitoring and logging capabilities. Unlike traditional locking mechanisms, which rely on physical keys that could be lost, copied or stolen, smart locks can utilise features such as encrypted digital keys and multi-factor authentication,

enhancing the lock's security. It is important to note, however, that not all manufacturers offer the same features within their smart locks, necessitating careful selection based on the specific security needs of the substation, the organisation that owns the substation, and any regulatory bodies.

Whilst implementing smart IoT locks does provide substantial benefits in additional features added over traditional locks and can help counter the issue of unauthorised access of the locks by countering traditional attack vectors such as lock-picking and cloning keys, they are not without potential drawbacks. Their reliance on network connectivity (such as Bluetooth Low Energy (BLE) and Wi-Fi networks) and power can make them vulnerable to outages and cyber-attacks. Therefore, a robust implementation of the technology is required to ensure they both physically strengthen the perimeter of the geophysical location and do not add any additional vulnerabilities to the IT/OT network of an organisation. For this reason, penetration tests, a form of security testing that allows ethical hackers to perform planned attacks on IT and OT infrastructure and software within the agreed scope of a test, to identify exploitable vulnerabilities with the intention to report and remediate these vulnerabilities, should be run against smart locks before they are implemented. Tests should include, but not be limited to:

- RFID key encryption cracking,
- RFID reader fuzzing/brute-forcing,
- Bluetooth/BLE penetration testing,
- Other network connectivity penetration testing (i.e. Zigbee, Z-Wave)
- Authentication bypass methods.

These tests have been chosen as they are penetration tests for technologies commonly found in IoT smart locks currently found in the market at the time of writing. The RFID attacks test for vulnerabilities in the RFID reader found in locks, and attacks on the encrypted keys used to operate the lock. The attacks on networks such as Bluetooth, BLE, Wi-Fi, Zigbee and Z-Wave aim to manipulate the data being transferred over the air to perform Man-in-the-middle (MITM) attacks, replay attacks and Denial of Service (DoS) to cause the lock to actuate without being authenticated. In 2016 at a DEFCON conference, security researchers Anthony Rose & Ben Ramsey identified and demonstrated vulnerabilities that could be found in some smart locks that utilise BLE in their presentation “Picking Bluetooth Low Energy Locks from a Quarter Mile Away”, this kind of vulnerability is an example of what manufacturers of the devices should be aware of, so they can mitigate it and provide the most secure product for their customers.

The problem that needs to be solved is to implement a secure solution at these geophysical locations, ensuring there is an increase in the level of security at the locations, whilst guaranteeing that the solutions provided do not introduce new vulnerabilities, in the past, there have been concerns over the cyber security of IoT Smart Locks and the potential risks and vulnerabilities that must be considered (Caballero-Gil et al., 2023).

Some companies within the electricity distribution industry already have some smart locks in use, for example, French DNO Enedis utilises the ISEO lock system and platform, minimising the risk of intrusion through a tailor-made access control solution, the solution ISEO offered was smart lock technology, using Bluetooth as the main technological components with Locken Smart Access (LSA) as a web-based software used to manage access and configure the access control system (ISEO, no date).

In this report, an evaluation project will be produced, focusing on performing penetration tests against various potential solutions in the form of IoT smart locks. This project will consider how the data is stored and secured, and the process of implementation to ensure an overall improvement in security without the

addition of any unwanted vulnerabilities, thereby averting the expansion of potential attack vectors within the organisation.

This report will produce, as an output, recommendations to both DNO companies for what technologies they could invest in to improve their security posture, and to vendors, as any vulnerabilities found within the products tested within this report will be shared with the vendors of the products so that they may patch and fix these. The tests will not be fully comprehensive, and will test for known vulnerabilities only, and will only be tested against a select number of products.

The benefits of this evaluation project will empower DNOs to enhance their cybersecurity posture through the addition of a secure physical layer to their OT equipment, facilitated by the integration of a smart lock that has been tested through this project to evidence how secure it is. The addition of locks not only strengthens the overarching cybersecurity stance of the organisation but will also add tangible benefits, such as facilitating logging and monitoring of who has accessed the physical sites (something not possible with current non-smart lock technology), which will also aid in defending against insider threats.

Furthermore, the inclusion of this supplementary cybersecurity feature will facilitate DNOs in attaining compliance with the NIS and CAF standards, as mandated by the National Cyber Security Centre (NCSC). Specifically, in the CAF “Principle B2 Identity and Access Control” when in order to achieve this CAF profile, the organisation needs to ensure *only authorised and individually authenticated users can physically access and logically connect to your network or information systems on which your essential function(s) depends* (NCSC, 2024).

DNOs are under the regulatory body OFGEM (The Office of Gas and Electricity Markets), which oversees the activities of energy companies ensuring they act in the interest of consumers, it enforces standards and regulations, in their price control “RIIO-ED2”, OFGEM details out the outputs that the 14 electricity DNOs that operate within the UK must deliver for their consumers (OFGEM, 2024). As part of RIIO-ED2, OFGEM has set out “Cyber Resilience Guidelines” that DNOs should aim to meet to mature the cyber security and resilience of their network and information systems (Okin, 2020).

The expected outcome of the project should be an extensive report, consisting of penetration tests, details of the findings in the penetration tests, executive summaries of the penetration tests, and recommendations for lock systems, security controls and processes. This report should be made available to all DNOs (and other CNI organisations) to allow for a secure implementation of the technology across the UK, strengthening the cybersecurity posture of the entire CNI network within the UK.

1.3 Methodology and Technology

This evaluation project will utilise a range of dedicated hardware hacking tools, hacking software tools, and other technologies to conduct penetration testing on a range of IoT smart locks. The primary hardware tools that will be used include:

- A Flipper Zero,
- A Proxmark 3,
- An Alfa USB AWUS036ACH-C, (henceforth, this will be referred to as an *External Wi-Fi Card)*,
- A Nordic Semiconductors nRF52840,
- A Samsung Galaxy A03s running Android with “Developer options” enabled.

These tools have capabilities that allow for the testing and exploitation of vulnerabilities in various wireless and RFID systems. These tools will be used to assess the security of the smart lock's communication protocols and access controls.

The testing environment that the tests are to be conducted in will be set up on a private Local Area Network (LAN), isolated from the internet to ensure complete control and security during the testing process. A dedicated router will facilitate the connection of the devices within this network, to mitigate potential external interference.

The operating systems that will be used to perform these penetration tests are Windows 10, Android XXX and Kali Linux, a distribution of Linux developed primarily to be used for cyber security purposes such as penetration testing.

The hardware used in the penetration tests will be accompanied by their appropriate software counterparts, to enable interaction between the operating systems and the hardware tools, this is where evidence for the penetration test in the form of screenshots will be gathered.

The Flipper Zero and Proxmark 3 will be used to analyse and attempt to bypass RFID security measures, whilst the external Wi-Fi card, NRF52840 and the Samsung A03s will be used to probe wireless communication protocols for weaknesses and perform the attacks. Each step of the penetration test will be documented, with a focus on identifying known potential vulnerabilities and evaluating the effectiveness of each lock's security measures.

The smart locks that will be used in this project are:

- eLinkSmart Padlock P5BF
- Ikea Rothult
- TTLock Padlock
- Yale Conexis L1

These locks have been chosen as they all contain a variety of technologies that can be tested against, such as RFID, Wi-Fi, Bluetooth and BLE (See *Table 1.1 Smart Lock Technology Matrix* for specific technologies found in each lock.) It should be noted that the Yale Conexis L1 has the capability to add additional IoT technologies in the form of plug-in "modules" that can provide additional functionality such as Z-Wave connectivity, however, only the Yale Access module that provides Bluetooth connectivity to smartphones will be tested.

Lock Manufacturer/Name	**RFID**	**Wi-Fi**	**Bluetooth/BLE**	**Magstripe**
eLinkSmart Padlock P5BF	No	No	Yes	No
Ikea Rothult	Yes	No	No	No
TTLock Padlock	Yes	No	Yes	No
Yale Conexis L1	Yes	No	Yes	No

Table 1.1 Smart Lock Technology Matrix

1.4 Ethical, Legal and Social Issues

Within this project, there are ethical, legal and social issues that must be considered to ensure that the work is conducted responsibly, lawfully and with an awareness of its potential impacts.

1.4.1 Ethical Considerations

The ethical aspects of this project primarily revolve around responsible testing and the potential impacts of exposing known vulnerabilities to products that are available to consumers. Conducting penetration tests, even in a controlled environment requires a commitment to ethical guidelines to responsibly disclose any discovered vulnerabilities, weaknesses or flaws in software, hardware, or systems and report them to the affected organisation or vendor (HackerOne, no date). Adhering to ethical standards helps ensure that the testing process does not create new risks to organisations and vendors through the exploitation of found vulnerabilities. Moreover, responsible disclosure of vulnerabilities is vital to prevent malicious actors from exploiting them before they are patched, thereby protecting users.

1.4.2 Legal Considerations

Legal considerations are required to ensure the project complies with relevant laws and regulations. Using hacking tools and techniques without proper authorisation can lead to legal consequences. In the UK, where this project is being undertaken, the applicable law that must be adhered to throughout this project is the Computer Misuse Act 1990, according to Section 3 it is illegal to perform “Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.” (Computer Misuse Act 1990 s.3).

Ensuring that all testing is conducted in controlled environments and on systems that are owned and controlled by the tester, this project avoids legal liabilities.

1.4.3 Social Considerations

Social considerations address the project's broader impact on public safety, trust and the perception of “smart” technologies, such as IoT devices. The findings in this project could influence the consumer's perception of how IoT smart locks are perceived and used. If vulnerabilities are not correctly disclosed and addressed by manufacturers, it could lead to the public’s loss of trust in this type of device.

1.5 Resources, Skills and Methods

What needed	Why needed	When needed	Problems if not available	How to ensure available

Wireshark (Software)	For conducting sniffing attacks	Throughout penetration testing	Unable to carry out some portions of the penetration testing	Already downloaded and installed
nRFConnect for Desktop (Software)	Required for interacting with nRF52840 dongle, including installing firmware and performing BLE communications	Throughout penetration testing	Unable to carry out some portions of the penetration testing	Already downloaded and installed
An Android Smartphone (Hardware)	For communications between the smart locks and the associated smartphone application	Throughout penetration testing	Unable to carry out some portions of the penetration testing	Already downloaded and installed
qFlipper (Software)	Desktop application for gathering screenshot and other evidence from the Flipper Zero device	Throughout penetration testing	Unable to capture evidence for penetration tests	Already downloaded and installed
4 IoT Smart Locks (Hardware)	For targets within the penetration test	Throughout penetration testing	Unable to carry out penetration tests	Already purchased.
Nordic Semiconductor nRF52840 (Hardware)	For communicating between the computer and Bluetooth functionality of the locks	Throughout penetration testing	Unable to carry out some portions of the penetration testing	Already purchased.
Flipper Zero (Hardware)	For performing a variety of attacks such as RFID attacks.	Throughout penetration testing	Unable to carry out some portions of the penetration testing	Already purchased.
Wi-Fi Router (Hardware)	For creating an offline segmented Wi-Fi network as to not disrupt any live networks during the penetration tests	Throughout penetration testing	Unable to carry out some portions of the penetration testing	Already purchased
Proxmark 3 (Hardware)	For communicating between the computer and	Throughout penetration testing	Unable to carry out some portions of the	Already purchased.

	RFID functionality of the locks		penetration testing	
CEH Platform (Information/ Software)	For Bluetooth/IoT Hacking training	For training and knowledge before the penetration tests	N/A	Should be available, if not other platforms are available for this (for example Hack The Box)

Table 1.2 Resources, Skills and Methods Required.

1.6 Project Planning

Before beginning the project, a Gantt chart was created to illustrate planned work to be completed throughout the project's life cycle. Whilst this acted as a guide for the project planning, it was not followed accurately, as many of the tasks, such as the "Penetration Testing" task had some time float due to its lack of dependencies on other tasks.

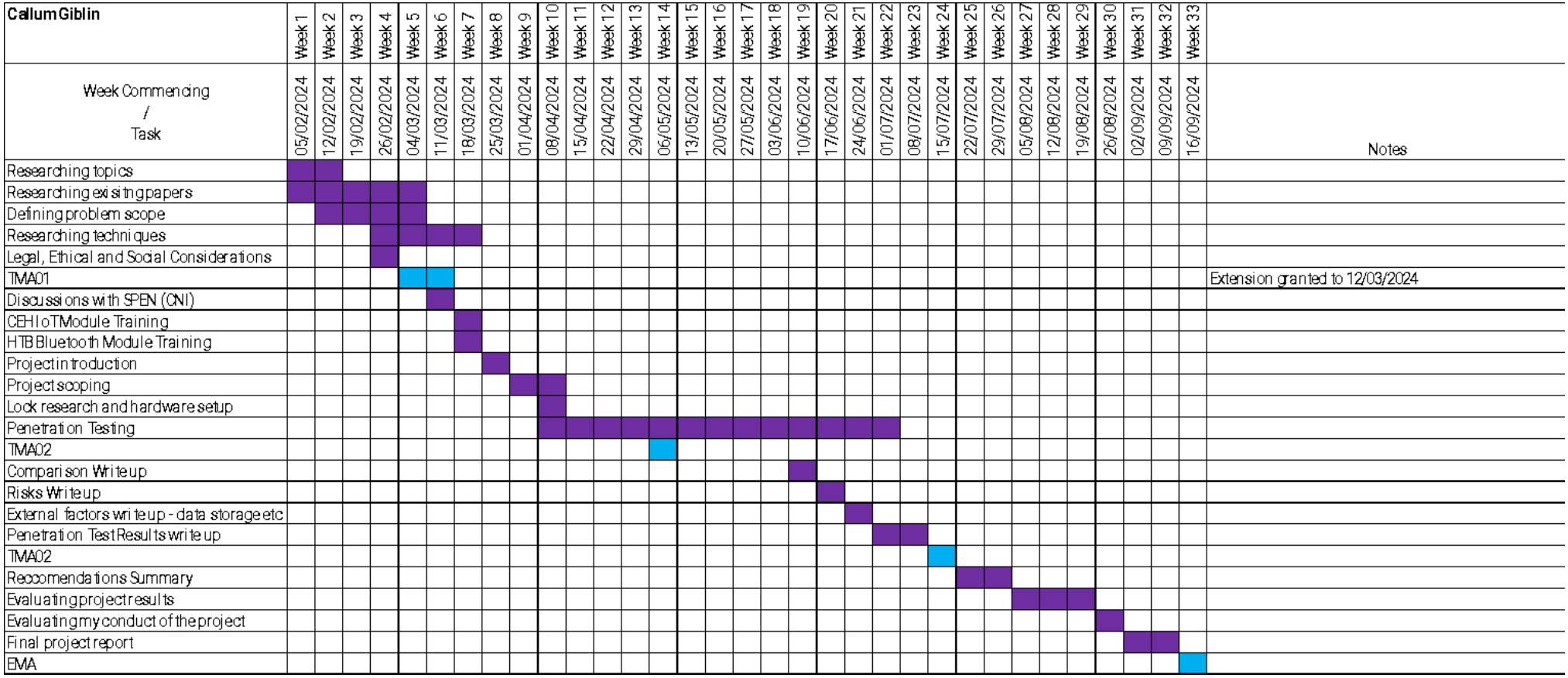


Figure 1.3 Project Gantt Chart

Chapter 2 Ikea Rothult Penetration Test

2.1 Engagement Contacts:

Contact Name	Title	Contact Email
Callum Giblin	Primary Tester	cllmgbln@gmail.com

Table 2.1 Engagement Contacts for the Ikea Rothult Penetration Test

2.2 Purpose & Scope

The purpose of this penetration test is to evaluate the security of the Ikea Rothult smart lock, with a specific focus on its RFID (Radio Frequency Identification) technology, which serves as the primary smart component of this device. This assessment aims to identify potential known vulnerabilities within the lock, which could be exploited by malicious actors to gain unauthorised access.

This test will examine the RFID communication protocols, and the data encryption used by the device, documenting attack methods used and providing scoring and recommendations for any vulnerabilities found.

The scope of the testing is limited to the RFID functionality of the device and the RFID keys used to operate the lock, these in-scope assets can be found in Table 2.2 In-Scope Assets, below.

Asset (Device/Module/Unit)	Description
Ikea E1778 Rothult Lock	Physical lock device, a white plastic box with a metal actuating lock.
Ikea E1777 RFID Keycard	A white plastic RFID keycard with black printed text & imaging.

Table 2.2 In-Scope Assets.

Figures 2.1 and 2.2, show the assets outlined in Table 2.2 In-Scope-Assets.

Figure 2.1 Ikea E1778 Rothult Lock in Engaged (left) and Disengaged (right) states.

Figure 2.2 Ikea E1777 RFID Keycard Front (left) and Rear (right).

2.3 Summary of Findings

During the penetration test of the Ikea Rothult lock system, the tester found a total of two findings that highlight potential risks associated with this smart lock. The tester also identified one informational finding from an observation from a test. Table 2.3 below, details the finding count and severity measurements.

Findings & Severity					
Critical	**High**	**Medium**	**Low**	**Informational**	**TOTAL**
0	2	0	0	1	3

Table 2.3 Ikea Rothult Finding Severity Summary

Table 2.4 shows a high-level overview of the findings discovered during the testing process. The details of these findings are further examined in section 2.4 Detailed Findings.

Finding	Severity Level	Title	Description
1	High	Weak RFID Encryption	Weak encryption on the E1777 Keycards, allowing for cloning & replay attacks
2	High	Authentication vulnerability	No requirement to authenticate before adding an additional keycard to actuate the lock
3	Informational	Cooling-off period	No cool-off period security measures on the device.

Table 2.4 Ikea Rothult Findings Summary

2.4 Detailed Findings

2.4.1 1. Weak RFID Encryption

2.4.1.1 Common Vulnerabilities and Exposures

While there are no known specific CVEs directly associated with the ST25 series of RFID chipsets, there are existing vulnerabilities related to RFID & NFC technologies, such as replay attacks, brute-force attacks and weak encryption which are still relevant.

2.4.1.2 Description

Through manipulation of the Ikea 1777 RFID keycard, it was discovered that the chipset being used was the ST25 series, manufactured by ST Microelectronics, it was also revealed that this keycard had been developed for use specifically for the Ikea Rothult smart lock, which gives a malicious actor a clear indication of what the card is used for. Using a Proxmark3 on the keycard and the reader within the Ikea 1778 Rothult lock, the tester was able to break the encryption on the keycard, retrieving the passwords and payload of the keycard that is read by the reader to authenticate a user to operate the lock. With this information, a malicious actor could emulate the keycard or clone it to a new keycard.

Whilst the manufacturer has implemented a counter on the keycard, that should mitigate a replay attack, this countermeasure was not observed in testing.

2.4.1.3 Impact and Likelihood

The potential impact of this attack could allow a malicious actor to authenticate the lock, with a replay attack if they have access to an existing lock and keycard.

It is unlikely that a malicious actor would have access to both a lock and a keycard unless an authorised user had lost or had their keycard stolen. However, the attack is relatively simple to execute and could be performed by a malicious actor who had the knowledge and tooling to do so.

As per *Appendix 1 Risk Severity Ratings*, this finding has been rated as follows:
Impact: HIGH
Likelihood: MEDIUM
Overall Risk Severity: High.

2.4.1.4 Remediation & Mitigation Techniques

- Implement an alternative RFID chipset that uses strengthened encryption methods, such as AES-128.
- Do not allow the reader to pass plain-text data back to the RFID chipset that could be intercepted, this traffic should be encrypted.

2.4.2 2. Authentication Vulnerability

2.4.2.1 Common Vulnerabilities and Exposures

CVE – N/A

There are no known specific CVEs associated with this finding.

2.4.2.2 Description

The tester found that if the Ikea Rothult E1778 Lock was in an unlocked position, it was possible to actuate the lock using multiple keycard UIDs (Unique Identifiers), that were not already associated with being authenticated keys to the lock. Not all UID combinations worked, this would highlight the potential for a malicious actor to attack the lock with a brute-force attack. This attack only worked whilst the lock was attacked in an unlocked state, in practice, this could allow a malicious actor to create a backdoor (a means of bypassing authentication at a later date or time).

2.4.2.3 Impact and Likelihood

The potential impact of this attack would allow a malicious actor to self-authenticate any number of keycards UIDs to a lock, allowing them to actuate the lock.

The likelihood that this attack could happen is low, as the malicious actor would need to access a lock that has been left unattended in an unlocked state, however, a user may have left a lock unlocked accidentally or may leave a lock unlocked whilst inside a secure area.

As per *Appendix 1 Risk Severity Ratings*, this finding has been rated as follows:
Impact – HIGH
Likelihood – MEDIUM
Overall Risk Severity – High.

2.4.2.4 Remediation & Mitigation Techniques

- The Ikea E1778 should implement a more secure authentication process when adding additional keycards as keys.
- The installer of the smart lock should implement a process to ensure that the lock is not left unattended whilst unlocked. However, it should be noted that this mitigation technique will not help defend against insider threats.

2.4.3 3. Cooling-Off Period

2.4.3.1 Common Vulnerabilities and Exposures

There is no CVE associated with this informational observation, however, it is considered good cyber security practice to have mitigation techniques to limit failed authentication techniques in an attempt to mitigate brute-force attacks.

2.4.3.2 Description

In a brute-force attack, the tester observed there was no cooling-off period implemented by the Ikea Rothult E1778 lock, allowing the tester to repeatedly test various UIDs against the lock that were not authenticating. Whilst this brute-force attack was not successful, the lock should implement a failsafe mechanism to prevent brute-force attacks.

2.4.3.3 Remediation & Mitigation Techniques

- The Ikea Rothult E1778 Lock should implement a mitigation technique in the form of a cool-off period, for example, after 5 failed attempts to authenticate a lock, the lock should be un-operable for a period of time, this would thwart a malicious actor's brute-force attempts significantly.

2.5 Detailed walkthrough

2.5.1 RFID Attacks on Ikea E1777 RFID Keycard

2.5.1.1 Proxmark3 Password Encryption Attack

1. Using the Proxmark3 tooling and associated terminal, the tester was able to use the **hf search** command to obtain the keycards UID (Unique Identifier), **02 E2 00 7C 7F 6D C0**, and the associated manufacturer of the keycard, **ST Microelectronics SA France**. This also unveiled the use of the ISO/IEC 1443-1:2018 ISO standard for contactless proximity objects.

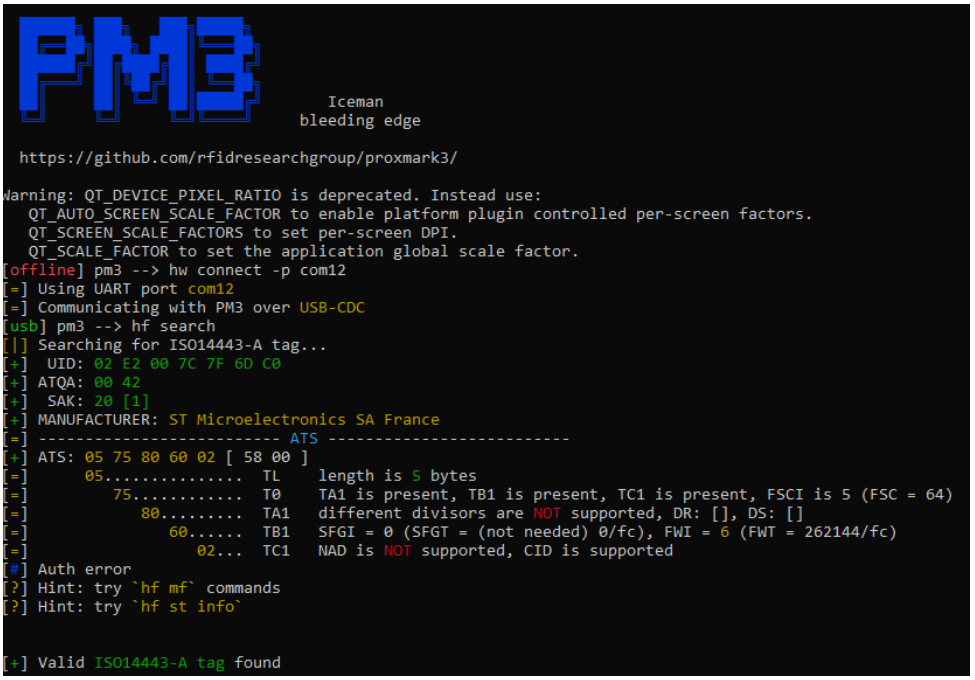


Figure 2.3 Proxmark3 “hf search” Command.

2. Knowing the manufacturer, the tester was then able to use the command **hf st info** to further gather details of the keycard, this unveiled that the product code (chipset type) was an “ST25???” (here a ? represents an unknown subtype of the ST25 card), and that it was produced specifically for the purpose of being used as an IKEA Rothult card.

   This command also unveiled the use of a counter being used by the card, a security feature used to track and limit operations or events, such as being read successfully or unsuccessfully, the counter could be used to increment or decrement each time the card is read by the reader, this is an

attempt to stop the cloning of a card.

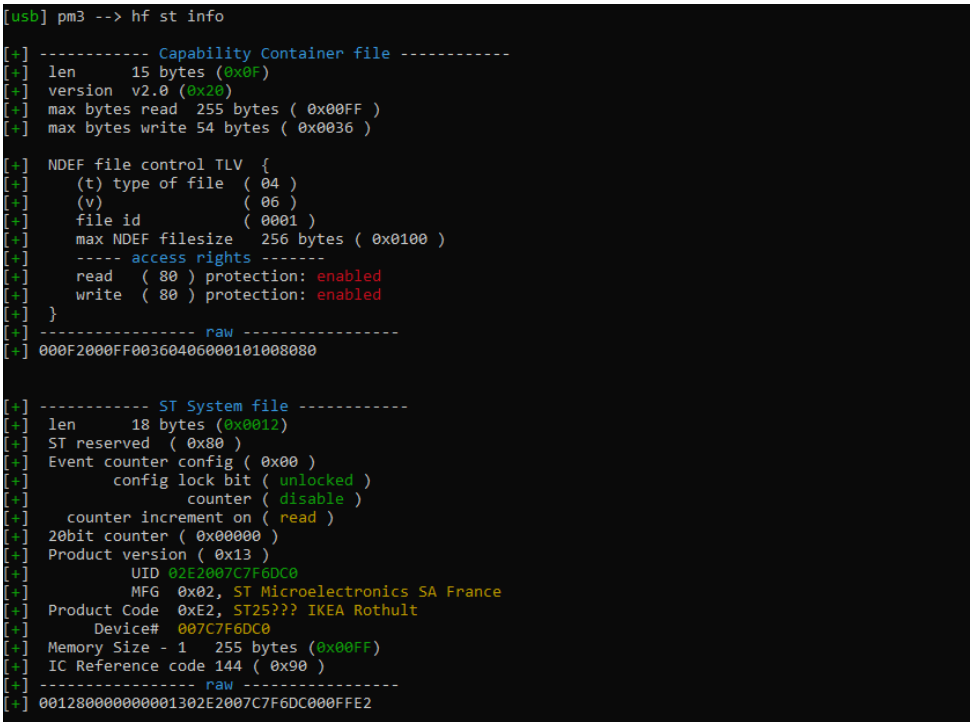


Figure 2.4 Proxmark3 "hf st info" Command.

3. Then, using the command **hf st sim -u 02E2007C7F6DC0**, the tester was able to use the Proxmark3 hardware to emulate the key card with the previously discovered UID to send to the RFID reader inside the Ikea E1778 lock, this does not allow the operation of the lock, however, the reader sends back a 16-bit password; **CE05A5A6BE8873CBA42B40051735EDCE**, to the Proxmark3 terminal, unencrypted.

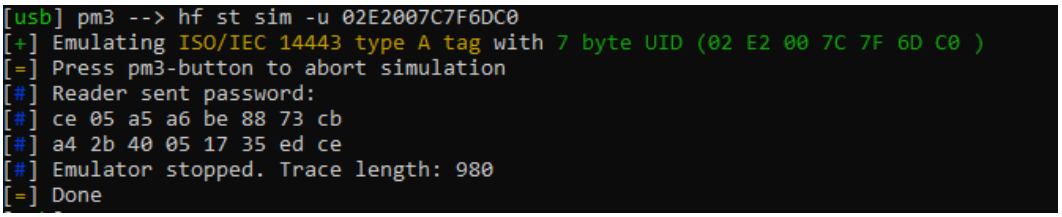


Figure 2.5 Proxmark3 "hf st sim" Command.

4. Using the password previously uncovered, the tester was then able to read the NDEF file stored on the keycard with the command **hf st ndef -p CE05A5A6BE8873CBA42B40051735EDCE**, showing the payload data contained on the card that is used as the key.

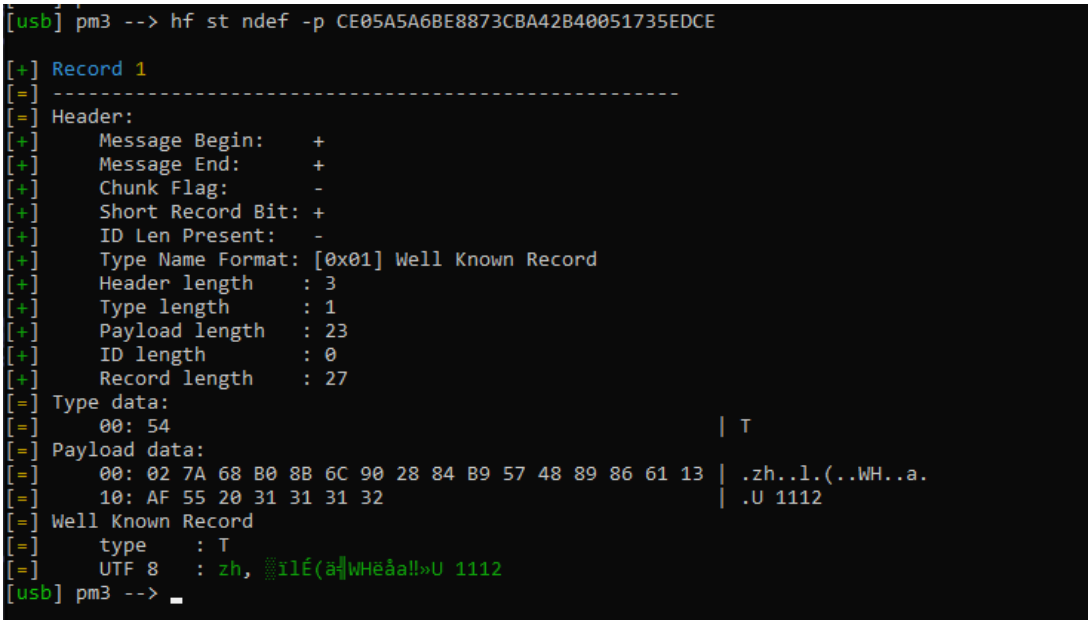


Figure 2.6 Proxmark3 "hf st ndef" Command.

2.5.2 RFID Attacks on Ikea E1778 Rothult Lock

2.5.2.1 Proxmark3 Emulating a Randomly Assigned UID.

1. Using the Proxmark3 tooling and associated terminal, the tester was able to use the command **hf st sim -u 02E2007C7FABCD**, to emulate a UID that is not associated with the lock, using this emulated UID (and other UIDs that were not associated with the lock), allowed for the lock to be engaged, and then to be unlocked using the same UID. It is unknown whether this is a feature or a flaw in the design.

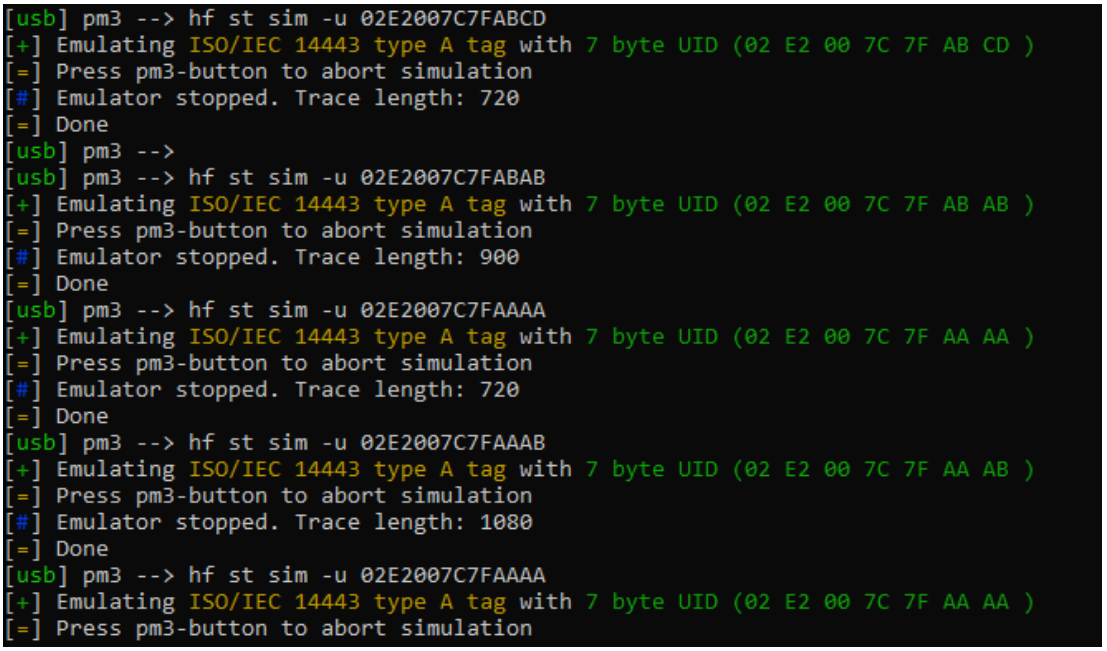


Figure 2.7 Proxmark3 "hf st sim" Command.

2.5.2.2 Flipper Zero Brute Force Attack

1. Using the Flipper Zero, the tester attempted to launch a brute-force attack using the fuzzer tool on the RFID reader in the lock, whilst unsuccessful, the lock did not have a countermeasure to stop the brute-force attempt, for example, a cool-off period after three failed attempts to actuate the locking mechanism.

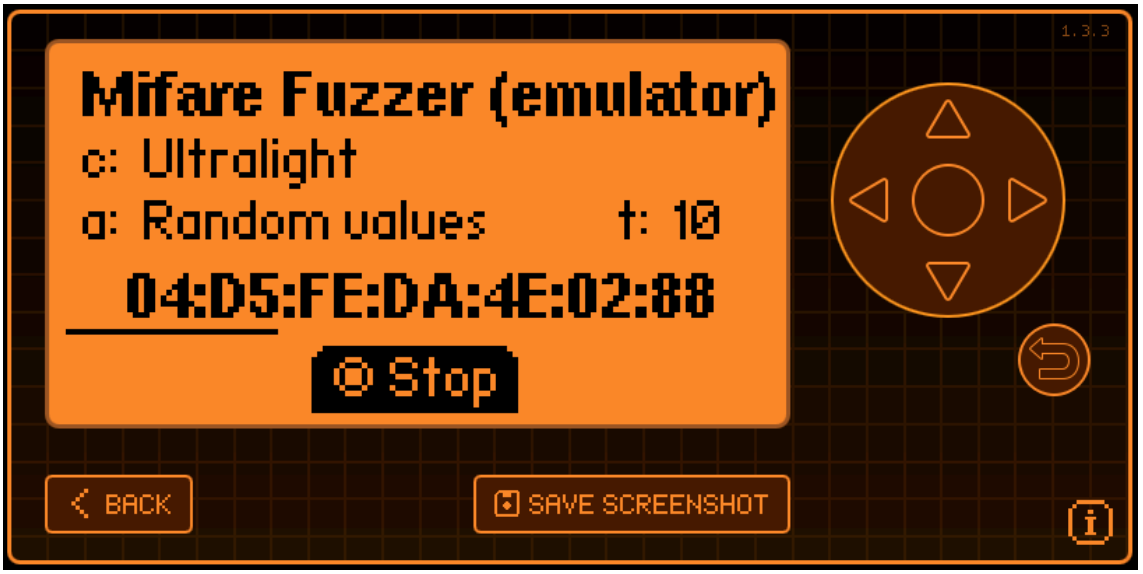


Figure 2.8 Flipper Zero GUI Showing the Fuzzer Tool Performing a Brute-Force Attack

Chapter 3 TTLock Padlock Penetration Test

3.1 Engagement Contacts

Contact Name	Title	Contact Email
Callum Giblin	Primary Tester	cllmgbln@gmail.com

Table 3.1 Engagement Contacts for the TTLock Padlock Penetration Test

3.2 Purpose and Scope

The purpose of this penetration test is to evaluate the security of the TTLock Padlock smart lock, with a specific focus on its RFID and BLE (Bluetooth Low Energy) technology, both of which serve as the smart components of this device. This assessment aims to identify potential known vulnerabilities within the lock, which could be exploited by malicious actors to gain unauthorised access.

This test will examine the RFID & BLE communication protocols, and the data encryption used by the device, documenting attack methods used and providing scoring and recommendations for any vulnerabilities found.

The scope of the testing is limited to the RFID and BLE functionality of the device and the RFID keys used to operate the lock, these in-scope assets can be found in Table 3.2 In-Scope Assets, below.

Asset (Device/Module/Unit)	Description
TTLock Padlock	Physical lock device, an aluminium black/gunmetal cube featuring touch-sensitive buttons, with a metal shackle.
TTLock RFID Key Fob	A thin, plastic oblong RFID key fob with an image printed on it, with an elasticated cord attached.

Table 3.2 In-Scope Assets.

Figures 3.1 and 3.2, show the assets outlined in Table 3.2 In-Scope-Assets.

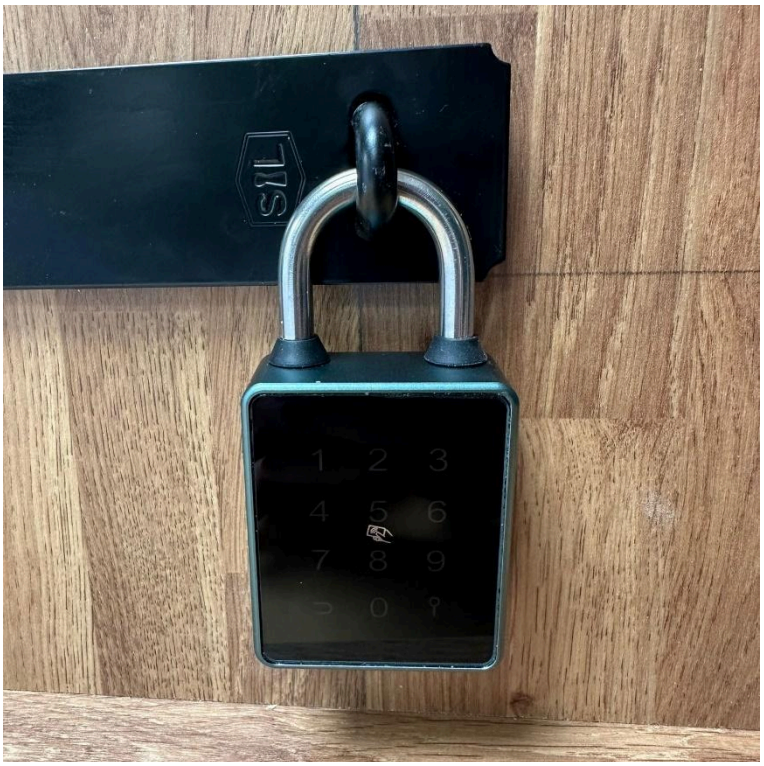


Figure 3.1 TTLock Padlock

Figure 3.2 TTLock RFID Key Fob

3.3 Summary of Findings

During the penetration test of the Ikea Rothult lock system, the tester found a total of four findings that highlight potential risks associated with this smart lock. Table 3.3 below, details the finding count and severity measurements.

Findings & Severity					
Critical	**High**	**Medium**	**Low**	**Informational**	**TOTAL**
3	**0**	1	0	0	4

Table 3.3 TTLock Padlock Finding Severity Summary

Table 3.4 shows a high-level overview of the findings discovered during the testing process. The details of these findings are further examined in section 3.4 Detailed Findings.

Finding	Severity Level	Title	Description
1	Critical	Default MIFARE Classic 1K Keys	The TTLock Key Fob comes with default MIFARE Classic Keys, allowing for dictionary attacks.
2	Critical	Weak RFID Encryption	Weak encryption on the MIFARE Classic 1K Keycards, allowing for cloning & replay attacks
3	Medium	BLE Authentication Vulnerability	No requirement to authenticate a BLE connection to connect to the device and gather details regarding the lock.
4	Critical	BLE Encryption Vulnerability	BLE Broadcast traffic is not encrypted, allowing for sniffing of clear text data sent via BLE.

Table 3.4 TTLock Padlock Findings Summary

3.4 Detailed Findings

3.4.1 1. Default MIFARE Classic 1K Keys

3.4.1.1 Common Vulnerabilities and Exposures

CWE: CWE-1394 Use of Default Cryptographic Key

The TTLock Key Fob, which employs the MIFARE Classic 1K RFID chipset, provided with the lock had been issued with the default key of **ffffffffffff** across all sectors in both blocks (Key A and Key B), this would allow an malicious actor to use the knowledge of default keys to perform a dictionary attack on the key fob, giving them access to bypass authentication quickly. According to MITRE's CWE-1394, it is the system administrators' task as part of the installation or deployment of the product (2022).

3.4.1.2 Description

Using the Proxmark3 and associated terminal, the tester was able to break the encryption of the MIFARE Classic 1K using a dictionary attack that took a total of three seconds to perform, this unveiled that all keys were set to the default MIFARE 1K Classic cryptographic key.

Whilst CWE-1394 advises mitigation for this task should be the responsibility of the system administrator, it is not good cyber hygiene for a manufacturer to provide a product with weak protections.

3.4.1.3 Impact and Likelihood

The impact of this weakness, would allow for a malicious actor to break the encryption of the TTLock Key Fob in seconds, meaning they would only need to have close proximity access to the key fob for a brief amount of time to perform an attack on it.

Unless the malicious actor was an insider threat, it is not very likely that a malicious actor would have access to a keycard, unless it had been stolen or lost. However, this attack is very simple to execute using tools such as the Proxmark3 or Flipper Zero and can be performed by malicious actors who have low level RFID hacking skills.

As per *Appendix 1 Risk Severity Ratings,* this finding has been rated as follows:
Impact: High
Likelihood: High
Overall Risk Severity: Critical.

3.4.1.4 Remediation & Mitigation Techniques

- The manufacturer should supply the TTLock Key Fob with preset, random cryptographic keys on the MIFARE Classic 1K RFID chipset.
- Before deployment of the TTLock Key Fob, the system administrator should change the cryptographic keys on the MIFARE Classic 1K RFID chipset to ensure they were not tampered with before deployment, for example in a supply chain attack.

3.4.2 2. Weak RFID Encryption

3.4.2.1 Common Vulnerabilities and Exposures

Weak encryption on the MIFARE Classic 1K RFID chipset used in the TTLock Key Fobs, enables malicious actors to create a cloned keycard if in physical proximity to the original keycard.

3.4.2.2 Description

Using the Proxmark3 and associated terminal, the tester was able to identify the UID of the authorised TTLock Key Fob and was able break the weak encryption deployed on the MIFARE 1K Classic, revealing all blocks and sectors for key A and key B used to authenticate the lock. The tester was able to upload the decrypted keys and UID onto a blank Magic MIFARE 1K Classic card (which has the ability to alter its associated UID, See Appendix 4) that was then able to authenticate when presented to the TTLock Padlock.

3.4.2.3 Impact and Likelihood

The potential impact of this attack could allow a malicious actor to authenticate the lock, with a replay attack if they had access to an authorised keycard and were able to break the encryption of it.

Unless the malicious actor was an insider threat, it is not very likely that a malicious actor would have access to a keycard, unless it had been stolen or lost. However, this attack is very simple to execute using tools such as the Proxmark3 or Flipper Zero and can be performed by malicious actors who have low level RFID hacking skills.

As per *Appendix 1 Risk Severity Ratings,* this finding has been rated as follows:
Impact: High
Likelihood: High
Overall Risk Severity: Critical.

3.4.2.4 Remediation & Mitigation Techniques

- Implementation of an alternative RFID chipset that uses strengthened encryption methods, such as AES-128, used by MIFARE DESFire cards that currently do not have any known vulnerabilities and cannot be cloned.
- Implementation of detection methods in the reader to identify Magic cards, to ensure that cloned cards are not able to authenticate the lock.
- Implementation of a counter so that each time the TTLock Key Fob is read, a value is written to one of its blocks or sectors to mitigate the use of cloned Magic cards.

3.4.3 3. BLE Authentication Vulnerability

Without the requirement to authenticate before a connection, BLE often allows a peripheral (such as a Smart lock) to be connected to a client and will display its characteristics.

3.4.3.1 Description

The tester was able to briefly connect to the TTLock Padlock using the nRF52480 and the nRF Connect application, this connection did not require authentication, and the tester was able to enumerate the characteristics of the TTLock, such as the services the lock can perform and the name, manufacturer and the Bluetooth device address.

In this test the tester was not able to actuate the lock through sending commands (actioning services), however, the details provided by the enumeration of the TTLock Padlock, provided plenty of detail that a malicious actor could utilise as reconnaissance to build a more advanced attack.

The TTLock Padlock would only allow a BLE connection for 1 second, before forcing a disconnect, whilst this could be a firmware bug, this works as a good mitigation to stop malicious actors from being able to

connect to the device without authentication for long periods of time, reducing the scope of attacks via BLE significantly.

3.4.3.2 Impact and Likelihood

The impact of this attack is relatively low, all that a malicious actor would gain from this attack is reconnaissance, however, it must be noted that the reconnaissance provided may lead to further attacks.

The likelihood of this attack is fairly high, this attack is easily performed using both specialist equipment, and also on free applications available on smartphones.

As per *Appendix 1 Risk Severity Rating*, this finding has been rated as follows:

Impact: Low

Likelihood: High

Overall risk: Medium.

3.4.3.3 Remediation & Mitigation Techniques

- Where possible, BLE advertising channels should display a minimum amount of information regarding the device, and its services, to limit enumeration techniques from a malicious actor.
- The manufacturer should implement a physical button on the device to turn BLE communications on when required, and this should be set to be off when not required.

3.4.4 3. BLE Encryption Vulnerability

3.4.4.1 Common Vulnerabilities and Exposures

BLE Communications broadcast from both the host (TTLock Padlock) and the client (Smartphone using the TTLock application), are unencrypted.

3.4.4.2 Description

Through sniffing using the Wireshark, the tester was able to find unencrypted BLE packets being broadcast both from the host (TTLock Padlock) and the client (Smartphone). This unencrypted data contains details such as UUIDS (Universal Unique Identifiers), Scan Response Data, and advertising addresses and channel maps, which could be used by a malicious actor to develop further attacks to calculate authentication keys, which in turn could be used in a replay attack.

3.4.4.3 Likelihood and Impact

The impact of this attack could allow for a malicious actor to capture unencrypted BLE packets and use them to craft a replay attack to authenticate the lock remotely at any point in time.

Given that the packets are communicated over a BLE channel that is unencrypted, this attack could be performed by anyone covertly within the range of the BLE broadcast signal. This makes the attack easy to perform by a malicious actor, with little risk associated when compared to RFID attacks where the malicious actor must be in a close physical proximity to the device.

As per *Appendix 1 Risk Severity Rating*, this finding has been rated as follows:

Impact: High

Likelihood: High

Overall risk: Critical.

3.4.4.4 Remediation & Mitigation Techniques

As per Finding 2. BLE Authentication Vulnerability.

- The manufacturer should implement a physical button on the device to turn BLE communications on when required, and this should be set to be off when not required.

The manufacturer should also ensure that sensitive data, such as Scan Response Data that can contain cryptographic keys should be encrypted whilst in transit via BLE.

3.5 Detailed Walkthrough

3.5.1 RFID Attacks on TTLock RFID Key Fob

3.5.1.1 Proxmark3 TTLock Key Fob Cloning Attack

1. Using the **hf search** command in the terminal for the Proxmark3, the tester was able to identify the Key Fob UID as **FF C1 4E 13**, and the chipset type as a MIFARE Classic 1K.

Figure 3.3 Proxmark "hf search" command.

2. Using the **hf mf auto** command, the tester then attacked the card's encryption to enumerate the sectors of both key A and key B, this was successful and unveiled all sectors for both keys to be

ffffffffffff. The attack was fast as the **hf mf auto** command was able to use a dictionary attack on the sectors, as **ffffffffffff** is often the default hexadecimal key set for MIFARE Classic 1K, this highlights concern as the default key fob for the lock should not be set to this, as it can be easily guessed. Implementing default passwords or keys in a real-world application is considered poor cyber hygiene.

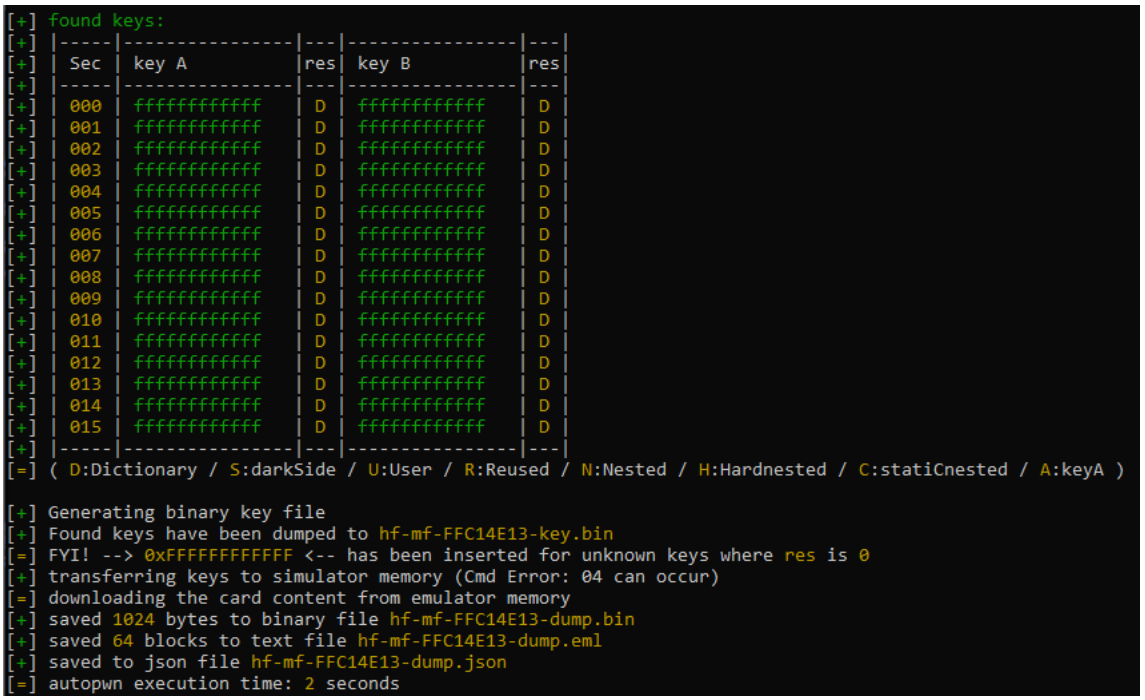


Figure 3.4 Proxmark3 "hf mf auto" Command.

3. Using the Proxmark3 command **hf mf csetuid** on a MIFARE 1K Classic Magic card (henceforth referred to as a Magic card), the tester was able to alter the UID of the Magic card to match the TTLock key fob.

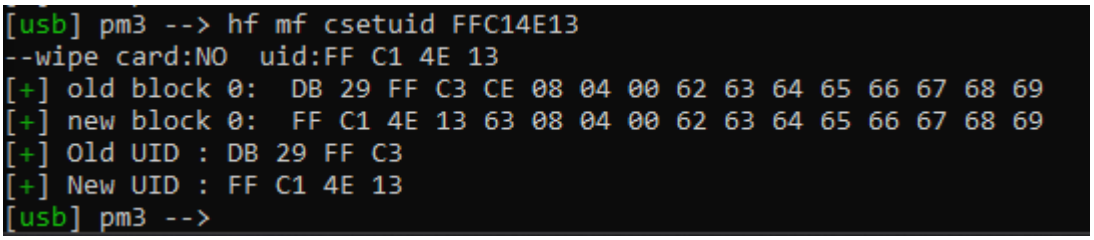


Figure 3.5 Proxmark3 "hf mf csetuid" Command.

4. The tester then used the command **hf mf restore** to upload the dumped keys from the TTLock key fob onto the Magic card, then verified the restore, viewing sectors of both keys using the **hf mf auto** command to display the key blocks.

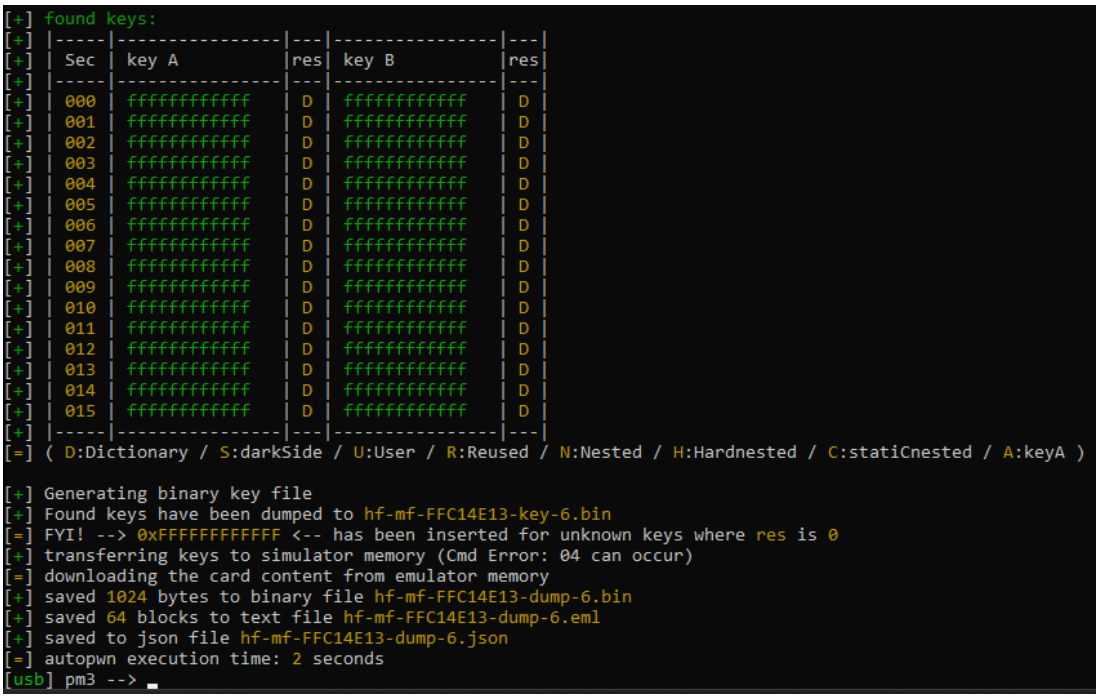


Figure 3.6 Proxmark3 "hf mf auto" Command to Verify Magic Card Keys

5. The tester then was able to authenticate the TTLock padlock using the Magic card which had been cloned from the TTLock key fob.

3.5.1.2 Flipper Zero TTLock Key Fob Emulation Attack

1. Using the Flipper Zero, the tester was able to read the TTLock Key Fob, capturing the key fob's chipset type, UID, and all keys.

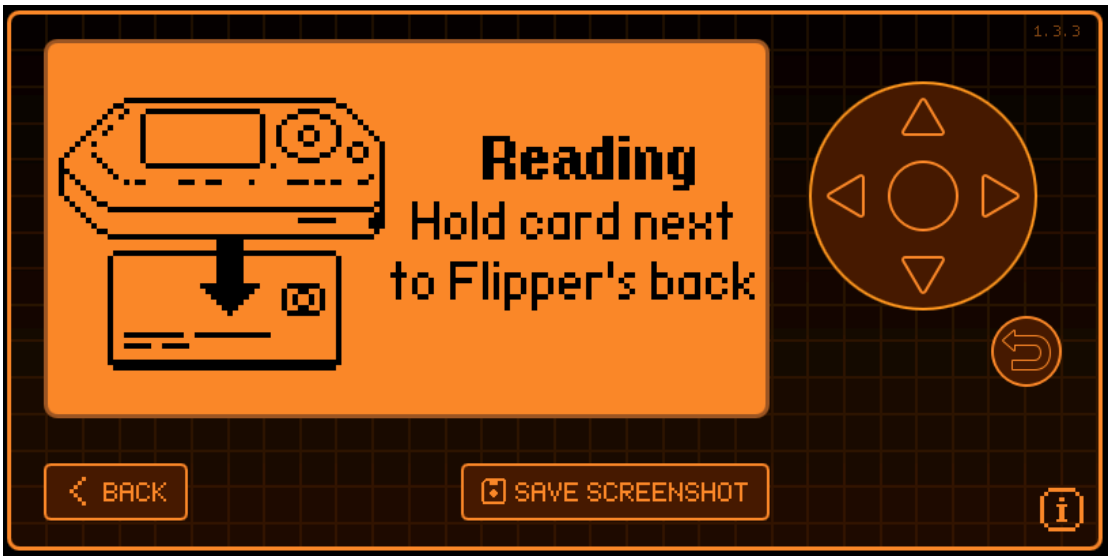


Figure 3.7 Flipper Zero Waiting for Key Fob

Figure 3.8 Flipper Zero TTLock RFID Key Fob Read Successfully.

2. Using the Flipper Zero, the tester was then able to emulate the TTLock Key Fob, which was able to authenticate the lock.

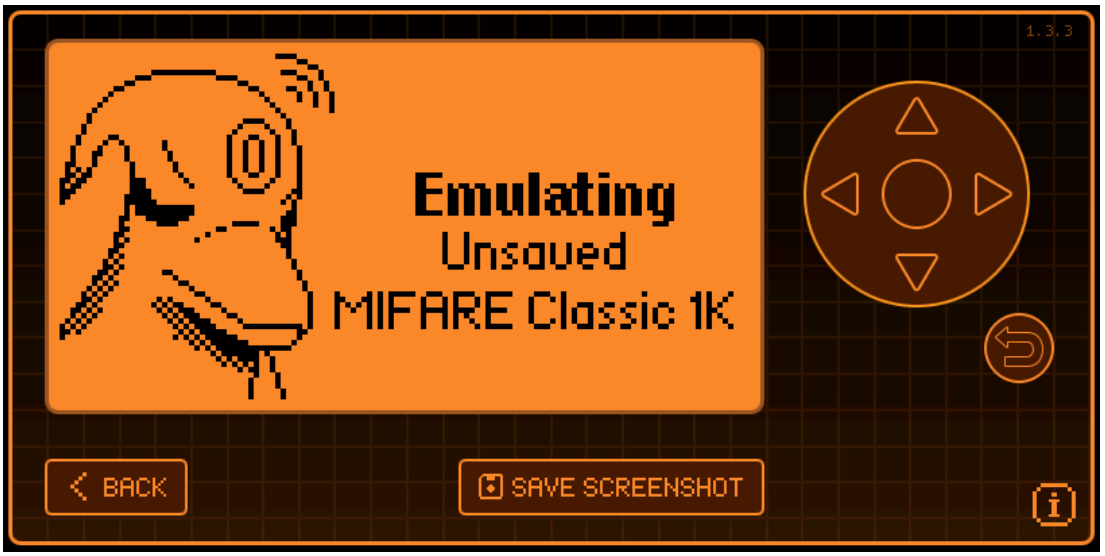


Figure 3.9 Flipper Zero Emulating TTLock Key Fob

3.5.2 RFID Attacks on TTLock Padlock

3.5.2.1 Flipper Zero Brute-Force Attack

1. Using the Flipper Zero, the tester attempted to launch a brute-force attack using the fuzzer tool on the RFID reader in the TTLock Padlock, the first four randomly generated MIFARE Classic 1K UIDS were read but authentication was rejected by the lock, as indicated by visual and audio indicators, on the fifth randomly generated UID the lock displayed a different visual and audio indicator, and disabled authentication via RFID, even when the authorised TTLock key card was presented, this cool-off period lasted for two minutes, before the lock reenabled RFID authentication methods.

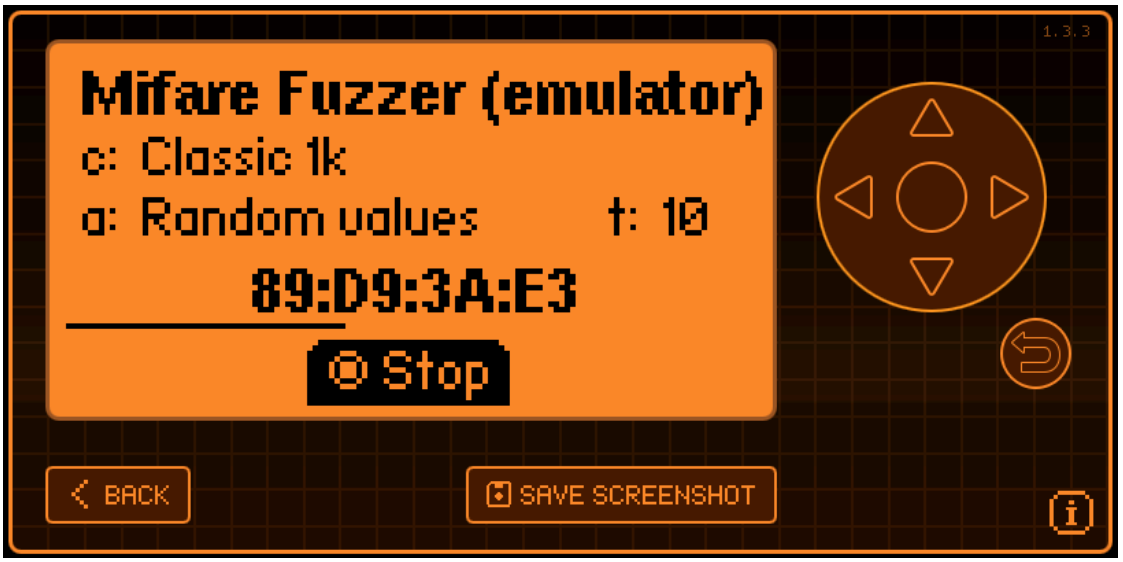


Figure 3.10 Flipper Zero Fuzzer Tool

3.5.3 BLE Attacks on the TTLock Padlock

3.5.3.1 nRF52480 Authentication Bypass Attack

1. Using the nRF52840, and the nRF Connect for Desktop application, the tester attempted to scan and interact with the TTLock padlock through its BLE communications protocol without being authenticated through the TTLock smartphone application. The tester was able to identify the device which had the name broadcast over BLE as “T55C_e0c0b1” and the Bluetooth device address as “88:06:99:b1:C0:E0”.

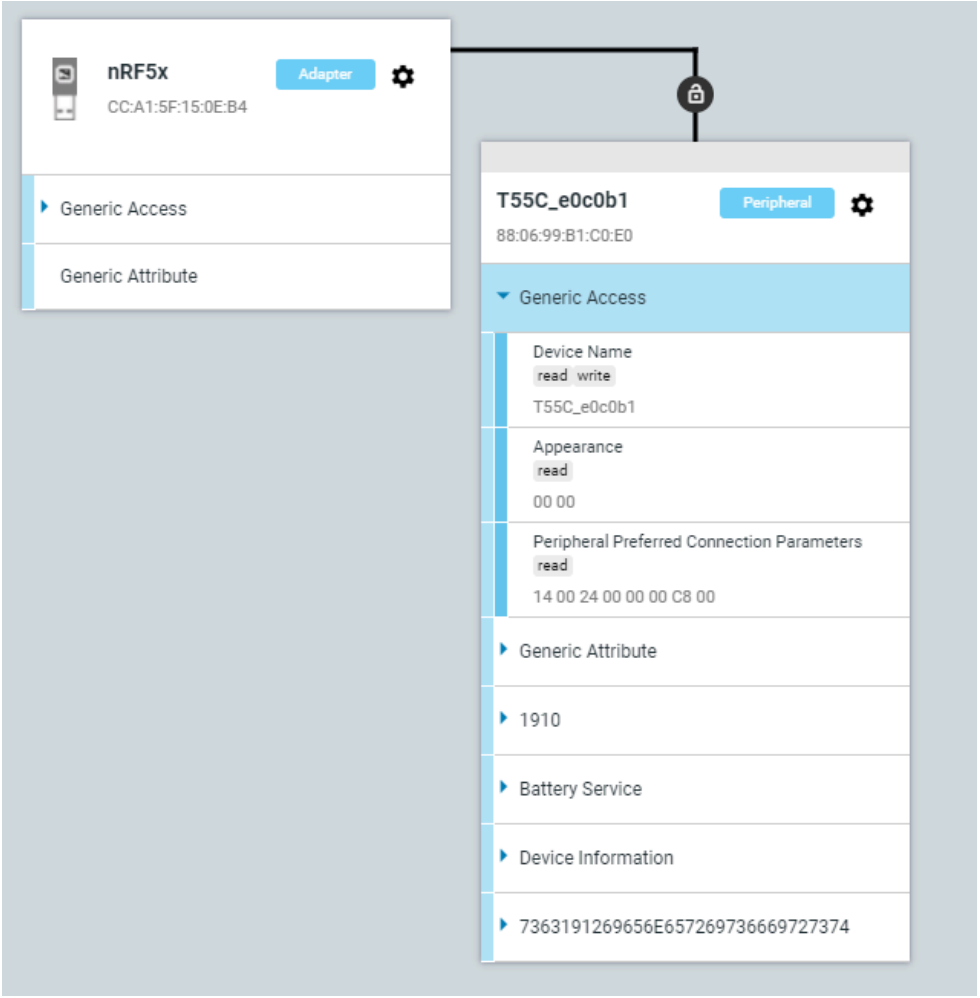


Figure 3.11 Successful BLE Connection from the nRF52840 to the TTLock Padlock

2. The TTLock connection only lasted for 1 second each time, before disconnecting from the nRF52840, this could be a security measure implemented by the manufacturer, therefore the tester was unable to authenticate the lock this way, however, the tester was able to enumerate information from the TTLOCK such as the Firmware installed, the current battery level, the Manufacturer name and Model number.

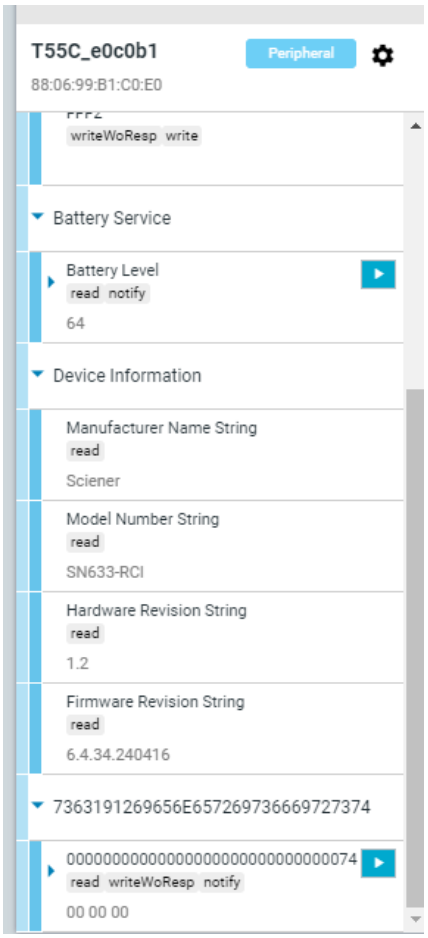


Figure 3.12 Enumerated information from the TTLock via the nRF52840.

3.5.3.2 Wireshark Sniffing for Unencrypted BLE Data

1. Using Wireshark and the nRF52840, the tester was able to sniff Broadcast packets from the TTLock Padlock, coming from the advertising channel identified in test 3.5.3.1, “88:06:99:b1:c0:e0”

   These broadcasts from TTLock Padlock show two packet types;

   - **ADV_IND** which is “Advertising Indication”, advertising itself with basic information about the device, such as its address.

   - **SCAN_RSP** which is “Scan Response”, an answer to a “Scan Request” (or **SCAN_REQ)** packet, which can contain additional device information, such as local names and service UUIDs (Universally Unique Identifiers).

   Furthermore, the tester was able to sniff **SCAN_REQ** packets being sent from another Bluetooth device address with the destination of the TTLock padlock.

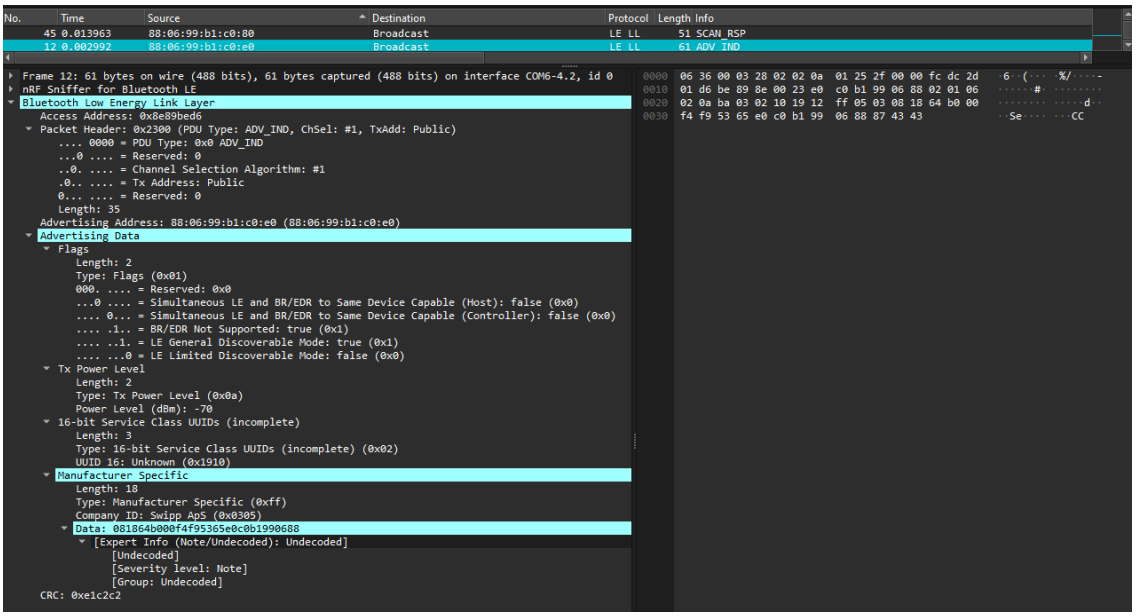


Figure 3.13 Wireshark Analysis of a SCAN_RSP from the TTLock Padlock

2. The details enumerated by the tester in this sniffing test, include details of the device name, and the scan response data.

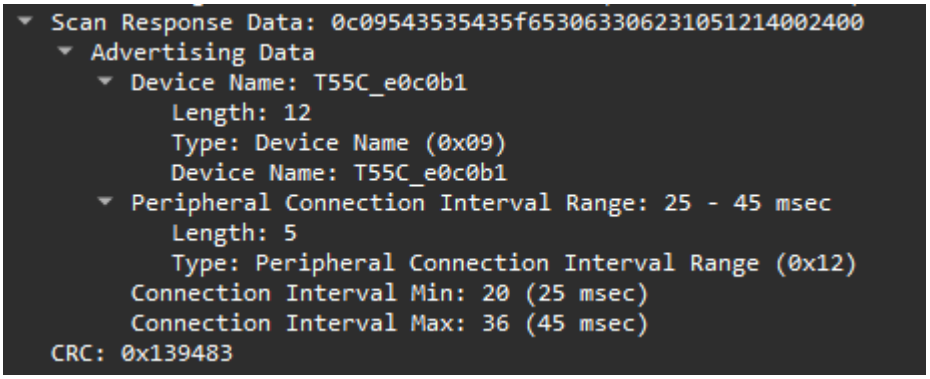


Figure 3.14 Enumerated Data from The Unencrypted BLE Data Packet

3. The tester was also able to identify a Connect Indication (**CONNECT_IND)** packet being sent to the TTLock, which a malicious actor may be able to use as part of a replay attack to authenticate a BLE connection to the TTLock Padlock.

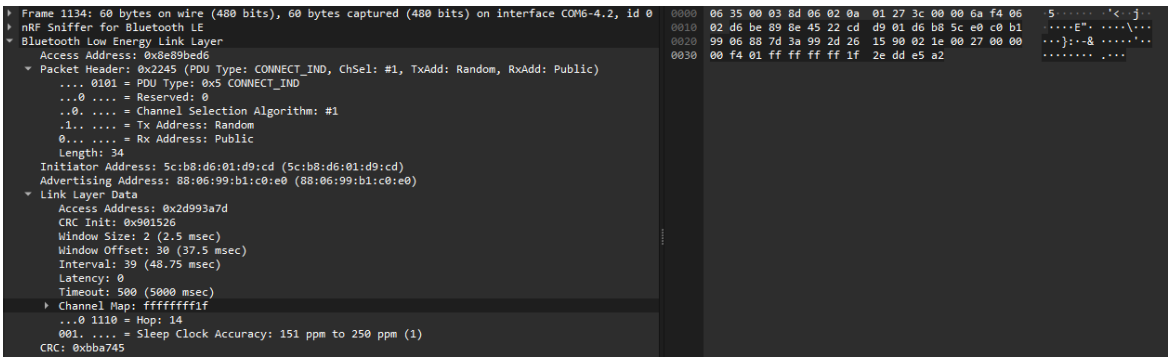


Figure 3.15 Wireshark Analysis of a CONNECT_IND Packet containing a Channel Map.

Chapter 4 Yale Conexis L1 Penetration Test

4.1 Engagement Contacts

Contact Name	Title	Contact Email
Callum Giblin	Primary Tester	cllmgbln@gmail.com

Table 4.1 Engagement Contacts for the Yale Conexis L1 Penetration Test

4.2 Purpose & Scope

The purpose of this penetration test is to evaluate the security of the Yale Conexis L1 smart lock, with a specific focus on its RFID and BLE (Bluetooth Low Energy) technology, both of which serve as the smart components of this device. This assessment aims to identify potential known vulnerabilities within the lock, which could be exploited by malicious actors to gain unauthorised access.

This test will examine the RFID & BLE communication protocols, and the data encryption used by the device, documenting attack methods used and providing scoring and recommendations for any vulnerabilities found.

The scope of the testing is limited to the RFID and BLE functionality of the device and the RFID keys used to operate the lock, these in-scope assets can be found in Table 3.2 In-Scope Assets, below.

Asset (Device/Module/Unit)	Description
Yale Conexis L1 Lock	Physical lock device, a plastic black/gunmetal cube featuring touch-sensitive buttons, with a metal shackle.
Yale Smart Access Module	A yellow access module inserted into the handle of the door lock that adds Bluetooth functionality through the Yale Access App on a smartphone.
Yale Smart Living Keycard	A thin, plastic RFID key card with the Yale logo printed on both sides.

Table 4.2 In-Scope Assets.

Figures 4.1, 4.2 and 4.3, show the assets outlined in Table 4.2 In-Scope Assets.

Figure 4.1 Yale Conexis L1 Lock Front (left) and Rear (right).

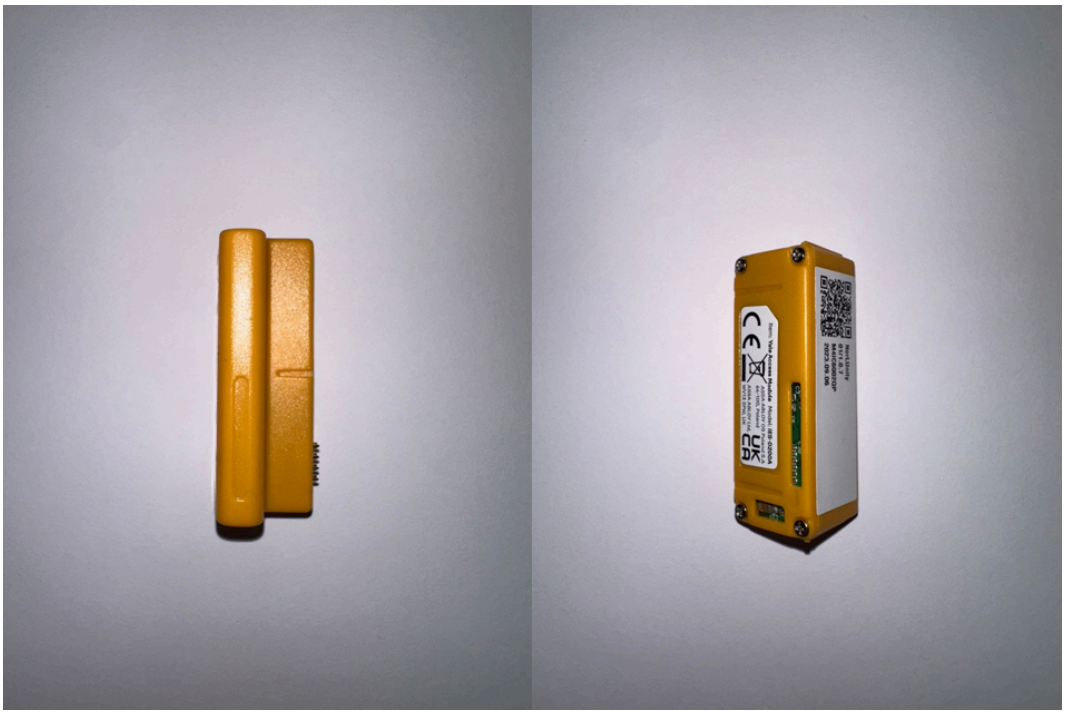


Figure 4.2 Yale Smart Access Module Side View (left) and Rear View (left).

Figure 4.3 Yale Smart Living Keycard

4.3 Summary of Findings

During the penetration test of the Yale Conexis L1 Lock, the tester found a total of three findings that highlight potential risks associated with this smart lock. Table 4.3 below, details the finding count and severity measurements.

Findings & Severity					
Critical	**High**	**Medium**	**Low**	**Informational**	**TOTAL**
2	0	1	0	0	3

Table 4.3 Yale Conexis L1 Finding Severity Summary

Table 4.4 shows a high-level overview of the findings discovered during the testing process. The details of these findings are further examined in section 4.4 Detailed Findings.

Finding	Severity Level	Title	Description
1	Critical	Weak RFID Encryption	Weak encryption on the MIFARE Classic 1K Keycards, allowing for cloning & replay attacks
2	Medium	BLE Authentication Vulnerability	No requirement to authenticate a BLE connection to connect to the device and gather details regarding the lock.
3	Critical	BLE Encryption Vulnerability	BLE Broadcast traffic is not encrypted, allowing for sniffing of clear text data sent via BLE.

Table 4.4 Yale Conexis L1 Findings Summary

4.4 Detailed Findings

4.4.1 1 Weak RFID Encryption

4.4.1.1 Common Vulnerabilities and Exposures

CVE: CVE-2023-26941

Weak encryption on the MIFARE Classic 1K chipset used in the Yale Smart Life RFID keycards, allows

malicious actors to create a cloned tag via physical proximity to the original (CVE, 2024).
Yale are aware of this vulnerability and have published a “Product Security Advisory – MIFARE Classic” in 2023 advising customers of this.

4.4.1.2 Description

Using the Proxmark3 and associated terminal, the tester was able to identify the UID of the authorised Yale Smart Life Keycard and was able break the weak encryption deployed on the MIFARE 1K Classic, revealing all blocks and sectors for key A and key B used to authenticate the lock. The tester was able to upload the decrypted keys and UID onto a blank Magic MIFARE 1K Classic card, which was then able to authenticate when presented to the Yale Conexis L1.

Whilst the manufacturer has endeavoured to mitigate this type of attack by means of the lock writing to a pre-determined sector of the keycard once it has been used to authenticate so that any cloned copies of the keycard would no longer present correct data to the reader, if the cloned magic card is read and authenticated earlier than the Yale Smart Life keycard, the cloned card will be accepted, and the Yale Smart Life keycard will no longer be able to authenticate the lock.

4.4.1.3 Impact and Likelihood

The potential impact of this attack could allow a malicious actor to authenticate the lock, with a replay attack if they had access to an authorised keycard and were able to break the encryption of it.

Unless the malicious actor was an insider threat, it is not very likely that a malicious actor would have access to a keycard, unless it had been stolen or lost. However, this attack is very simple to execute using tools such as the Proxmark3 or Flipper Zero and can be performed by malicious actors who have low level RFID hacking skills.

As per *Appendix 1 Risk Severity Ratings,* this finding has been rated as follows:
Impact: High
Likelihood: High
Overall Risk Severity: Critical.

4.4.1.4 Remediation & Mitigation Techniques

According to Yale’s Product Security Advisory – MIFARE Classic (2023), mitigation techniques include:

- Switching to an alternative form of authentication provided by the lock, which are unaffected by this vulnerability (For example, BLE).
- Always keep your card out of reach of people you don’t know and trust, keep your card safe and secure.

Whilst these are both appropriate mitigation techniques provided by Yale, further mitigations that could be implemented by the manufacturer include:

- Implementation of an alternative RFID chipset that uses strengthened encryption methods, such as AES-128, used by MIFARE DESFire cards that currently do not have any known vulnerabilities and cannot be cloned.
- Implementation of detection methods in the reader to identify Magic cards, to ensure that cloned cards are not able to authenticate the lock.

4.4.2 2. BLE Authentication Vulnerability

4.4.2.1 Common Vulnerabilities and Exposures

Without the requirement to authenticate before a connection, BLE often allows a peripheral (such as a Smart lock) to be connected to a client and will display its characteristics.

4.4.2.2 Description

The tester was able to connect to the Yale Conexis L1 lock using the nRF52480 and the nRF Connect application, this connection did not require authentication, and the tester was able to enumerate the characteristics of the Yale Conexis L1, such as the services the lock can perform and the name, manufacturer and the Bluetooth device address.

In this test the tester was not able to actuate the lock through sending commands (actioning services), however, the details provided by the enumeration of the Yale Conexis L1, provided plenty of detail that a malicious actor could utilise as reconnaissance to build a more advanced attack.

4.4.2.3 Impact and Likelihood

The impact of this attack is relatively low, all that a malicious actor would gain from this attack is reconnaissance, however, it must be noted that the reconnaissance provided may lead to further attacks.

The likelihood of this attack is fairly high, this attack is easily performed using both specialist equipment, and also on free applications available on smartphones.

As per *Appendix 1 Risk Severity Rating*, this finding has been rated as follows:
Impact: Low
Likelihood: High
Overall risk: Medium.

4.4.2.4 Remediation & Mitigation Techniques

- Where possible, BLE advertising channels should display a minimum amount of information regarding the device, and its services, to limit enumeration techniques from a malicious actor.

- The manufacturer should implement a physical button on the device to turn BLE communications on when required, and this should be set to be off when not required.

4.4.3 3. BLE Encryption Vulnerability

4.4.3.1 Common Vulnerabilities and Exposures

CVE: CVE-2019-17627

The Yale Bluetooth Key application for mobile devices allows unauthorised unlock actions by sniffing BLE traffic during one authorised unlock action (CVE, 2019).

4.4.3.2 Description

Through sniffing using the Wireshark, the tester was able to find unencrypted packets being broadcast from and to the Yale Conexis L1. This unencrypted data contains details such as UUIDS (Universal Unique Identifiers), Scan Response Data, and advertising addresses, which could be used by a malicious actor to develop further attacks to calculate authentication keys, which in turn could be used in a replay attack.

4.4.3.3 Likelihood and Impact

The impact of this attack could allow for a malicious actor to capture unencrypted BLE packets and use them to craft a replay attack to authenticate the lock remotely at any point in time.

Given that the packets are communicated over a BLE channel that is unencrypted, this attack could be performed by anyone covertly within the range of the BLE broadcast signal. This makes the attack easy to perform by a malicious actor, with little risk associated when compared to RFID attacks where the malicious actor must be in a close physical proximity to the device.

As per *Appendix 1 Risk Severity Rating*, this finding has been rated as follows:

Impact: High

Likelihood: High

Overall risk: Critical.

4.4.3.4 Remediation & Mitigation Techniques

As per Finding 2. BLE Authentication Vulnerability.

- The manufacturer should implement a physical button on the device to turn BLE communications on when required, and this should be set to be off when not required.

The manufacturer should also ensure that sensitive data, such as Scan Response Data that can contain cryptographic keys should be encrypted whilst in transit via BLE.

4.5 Detailed Walkthrough

4.5.1 RFID Attacks on Yale Smart Living Keycard

4.5.1.1 Proxmark3 Keycard Cloning Attack

1. Using the Proxmark3 tooling and associated terminal, the tester was able to use the **hf search** command to obtain the keycards UID (Unique Identifier), **DB 29 FF C3**, and identified the chipset type as MIFARE Classic 1K.

Figure 4.4 Proxmark3 "hf search" Command Performed on the Yale Smart Living Keycard

2. The tester then was able to use the **hf search** command to obtain the UID (Unique Identifier) of a second keycard, one that is not authorised to authenticate the Yale Conexis L1 lock, however, is of the same type (MIFARE Classic 1K), this keycard is known as a "Magic" MIFARE Classic 1K RFID card (henceforth, this will be referred to as the *Magic card*), and has the ability to alter its associated UID

(See Appendix 4). The UID of this Magic keycard was set to **CA DD 7A 26**.

```
[usb] pm3 --> hf search
[/] Searching for ISO14443-A tag...
[+]  UID: CA DD 7A 26
[+] ATQA: 00 04
[+]  SAK: 08 [2]
[+] Possible types:
[+]    MIFARE Classic 1K
[=] proprietary non iso14443-4 card found, RATS not supported
[+] Prng detection: weak
[#] Auth error
[?] Hint: try `hf mf` commands


[+] Valid ISO14443-A tag found

[usb] pm3 -->
```

Figure 4.5 Proxmark 3 "hf search" Command Performed on the Magic Card

Figure 4.6 Magic MIFARE Classic 1K Keycard.

3. Using the **hf mf auto** command on the Yale Smart Living Keycard automatically performed attacks on all of the encrypted sectors of both keys stored on the MIFARE Classic 1K chipset, this attack was successful, providing the tester with the decrypted keys.

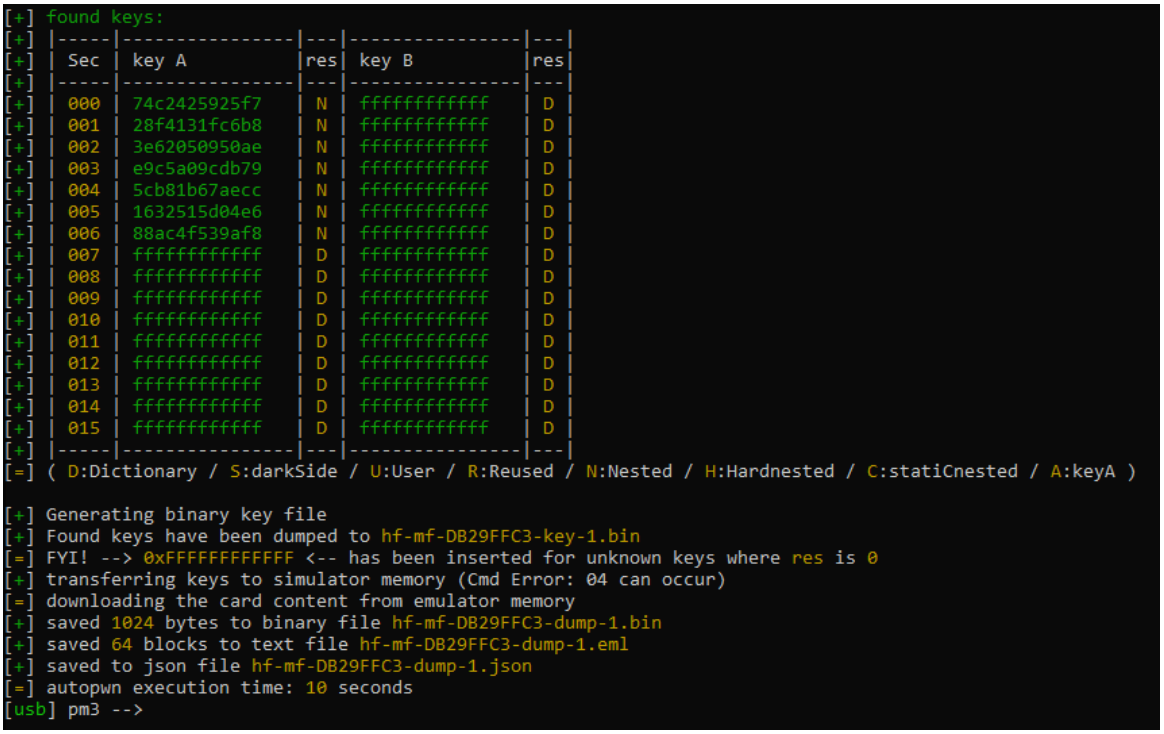


Figure 4.7 Proxmark 3 "hf mf auto" command on the Yale Smart Living Keycard

4. The tester then set the UID of the Magic card to match the UID of the Yale Smart Living Keycard using the **hf mf csetuid** command.

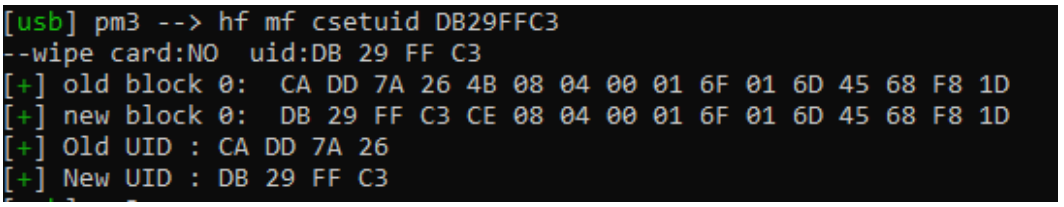


Figure 4.8 Proxmark3 "hf mf csetuid" Command.

5. Then the tester added the decrypted keys onto the Magic card using the Proxmark3 command **hf mf restore** to finish cloning the Yale Smart Living Keycard.

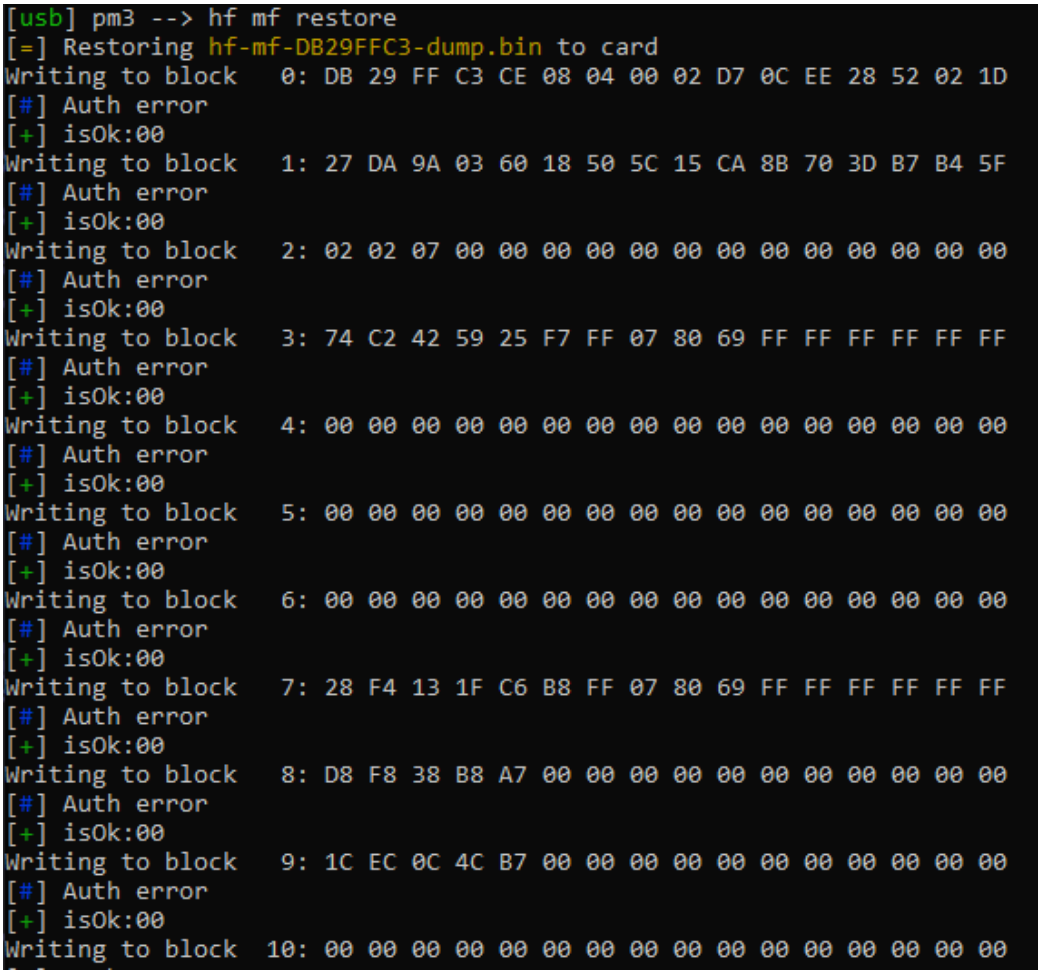


Figure 4.9 Proxmark3 "hf mf restore" Command.

6. With the Yale Smart Living Keycard's UID and keys now cloned to the Magic card, the tester was able to authenticate the Yale Conexis L1 using the Magic card, meaning that the clone had been successful. However, when the tester tried to use the Yale Smart Living Keycard to authenticate the lock, the authentication failed. The tester then ran the **hf mf auto** command on both keycards to identify what had changed to cause the Yale Smart Keycard to no longer authenticate, and when comparing the dumped blocks from the Proxmark3 for both cards, it was identified that Block 8 on the Magic card had been altered as the Yale Conexis L1 Lock had written to the card, this is assumed to be a security feature implanted by the manufacturer to mitigate this type of attack.

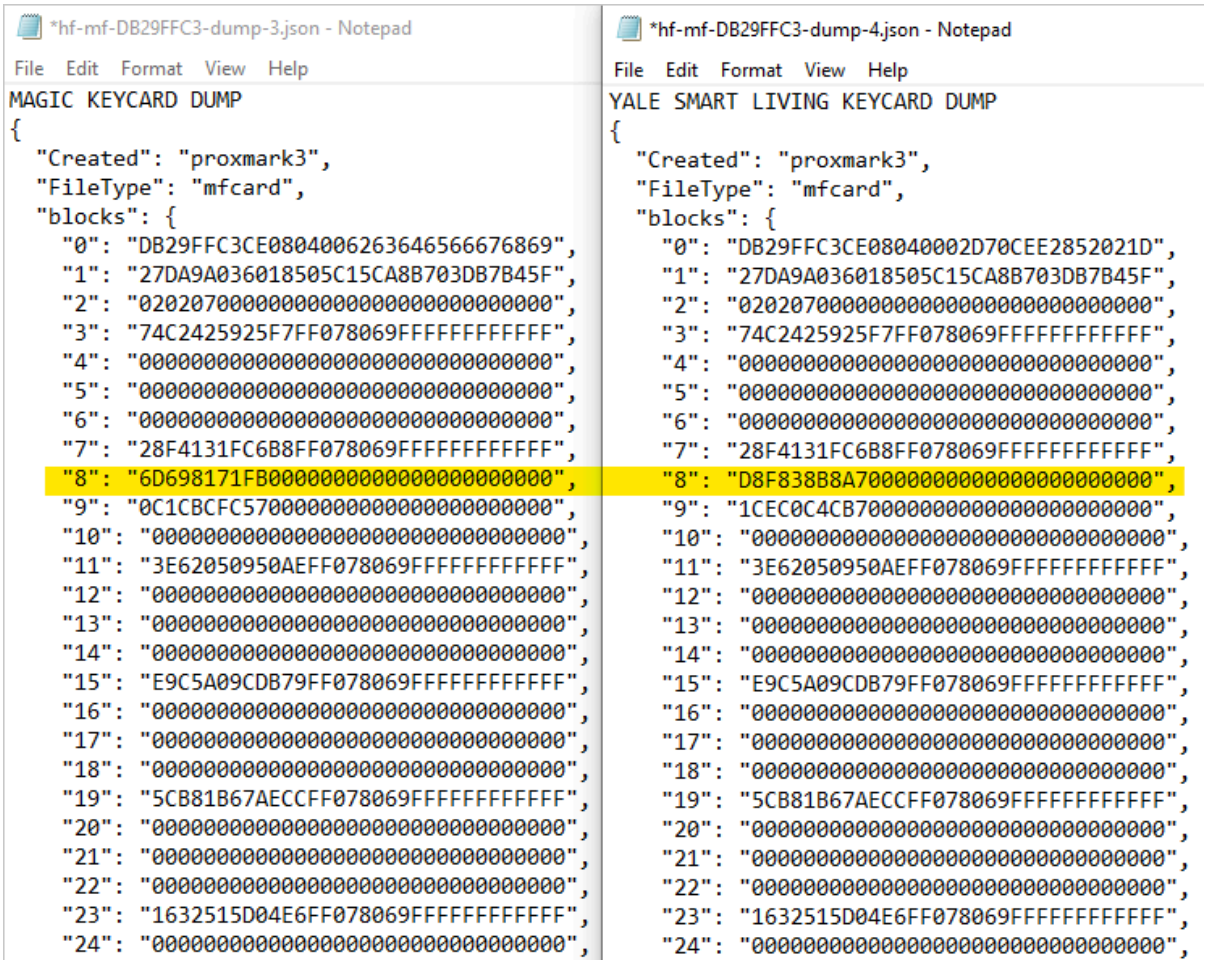


Figure 4.10 Block Dumps from the Magic Card and Yale Smart Living Keycard, Block 8 (Highlighted) shows a different block on each card.

4.5.2 RFID Attacks on Yale Conexis L1 Lock

4.5.2.1 Flipper Zero Brute-Force Attack

1. Using the Flipper Zero, the tester attempted to launch a brute-force attack using the fuzzer tool on the RFID reader in the lock, this test proved to be unsuccessful, the lock did not provide any feedback (the lock has an LED and audio indicator to show both successful and unsuccessful authorisation attempts). This would suggest that the lock was not reading the Flipper Zero.
2. Checking the debugging logs provided by the Flipper Zero, the tester identified that during the brute-force attack, the logs showed the command “R: 60 01” displayed at each pass of the attack, which suggests that the lock did read the flipper.

   This command suggests that the reader is communicating with the flipper, attempting to authenticate with the first sector, however it is failing to authenticate, suggesting that the firmware installed on the Yale Conexis L1 lock has some mitigation techniques to combat communicating with keycards that have not previously been authenticated to the lock.

4.5.3 BLE Attacks on Yale Conexis L1 Lock

4.5.3.1 nRF52480 Authentication Bypass Attack

1. Using the nRF52840, and the nRF Connect for desktop application, the tester attempted to scan and interact with the Yale Conexis L1 Lock to interact with the lock through its BLE communications protocol, without being authenticated through the Yale Home smartphone application. The tester was able to identify the device which had the name broadcast over BLE as “M402QP” and the device’s address as “98:1B:B5:03:FA:A3” and was able to connect to the device without authentication successfully.

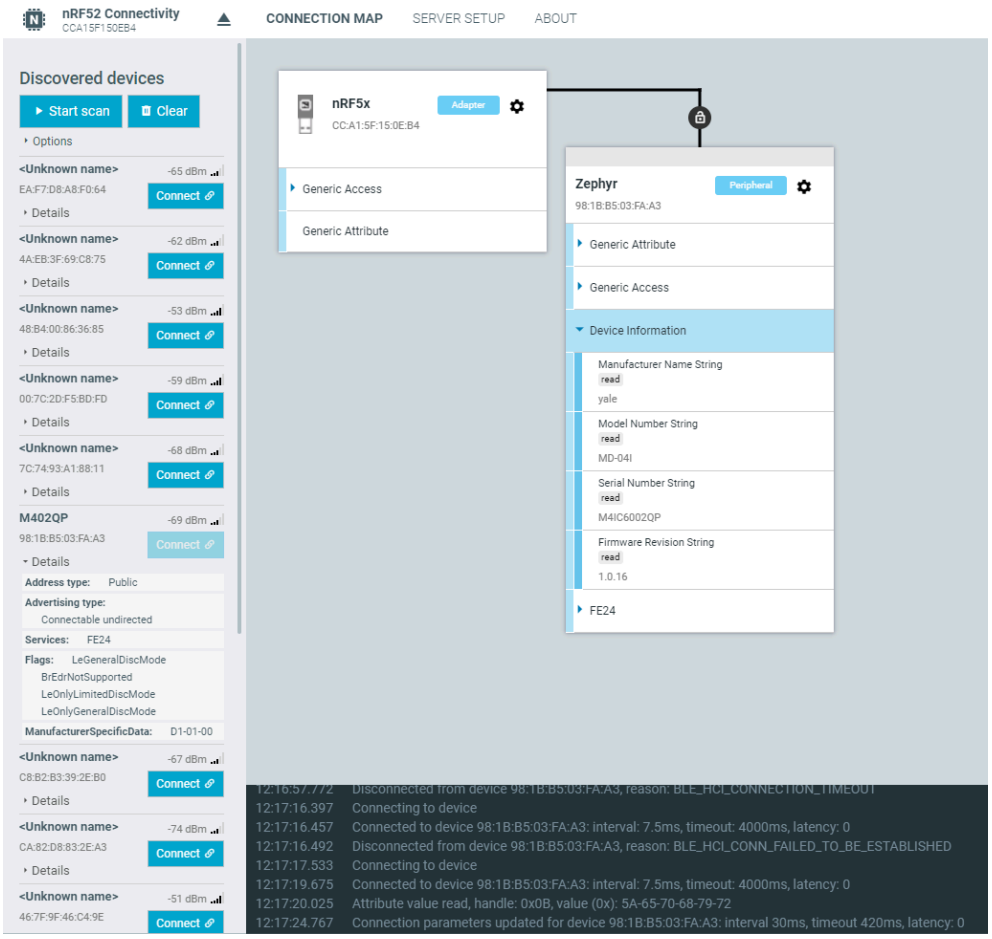


Figure 4.11 Successful BLE Connection from the nRF52840 to the Yale Conexis L1 Lock

2. After 30 seconds of being connected, the lock disconnected from the device, likely a security measure implemented by the manufacturer into the device’s firmware.

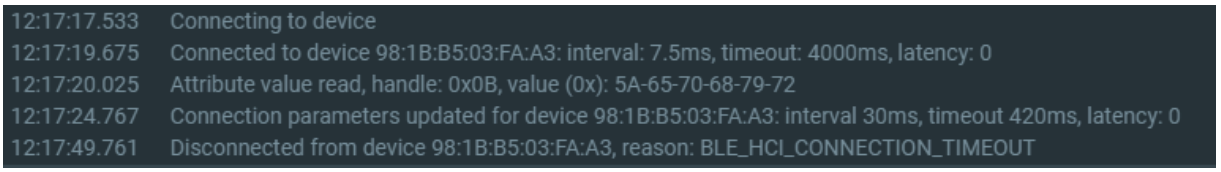


Figure 4.12 nRF Connect Application Logs

3. The tester was able to identify specific attributes broadcast by the lock such as the manufacturer name, model number, firmware installed and the database hash, which could assist for a malicious actor in the reconnaissance stage of the cyber-attack life cycle, providing details for them to launch a more specific attack on the device.

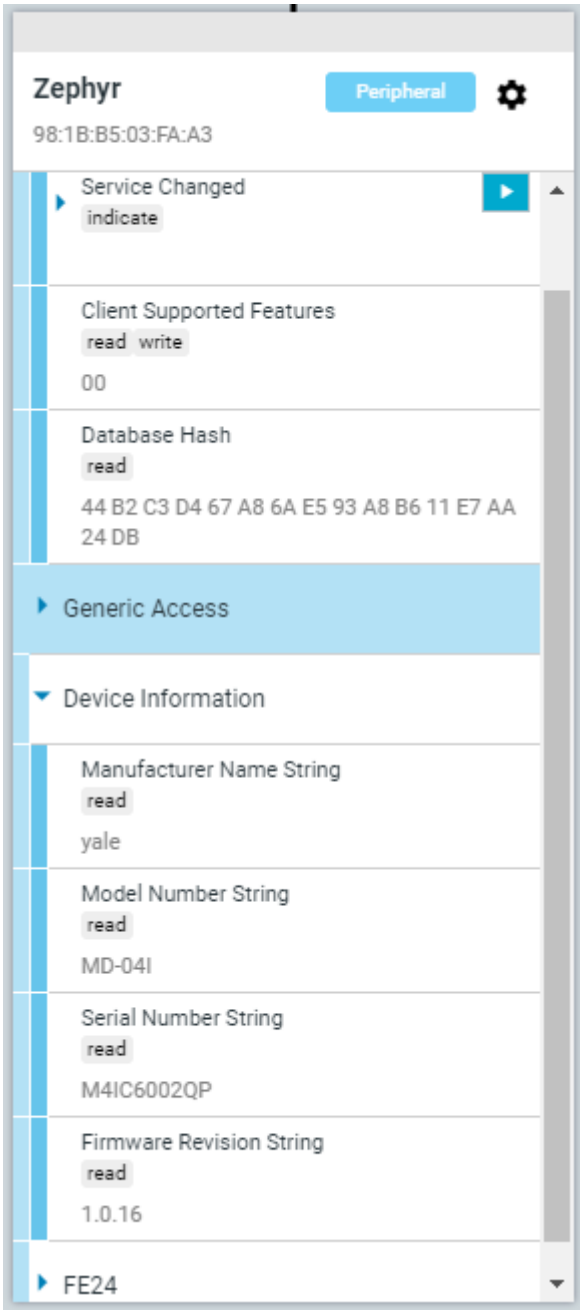


Figure 4.13 Device information Broadcast via BLE from the Yale Conexis L1 Lock

4. The tester attempted to send commands to the Yale Conexis L1 to cause the locking mechanism to actuate, these commands were successfully sent to the lock as per the logs, however the lock did not respond in any way to these, suggesting that the lock has a challenge-response scheme at the

application layer for the authentication of commands being sent to the lock which would be done on the smartphone application.

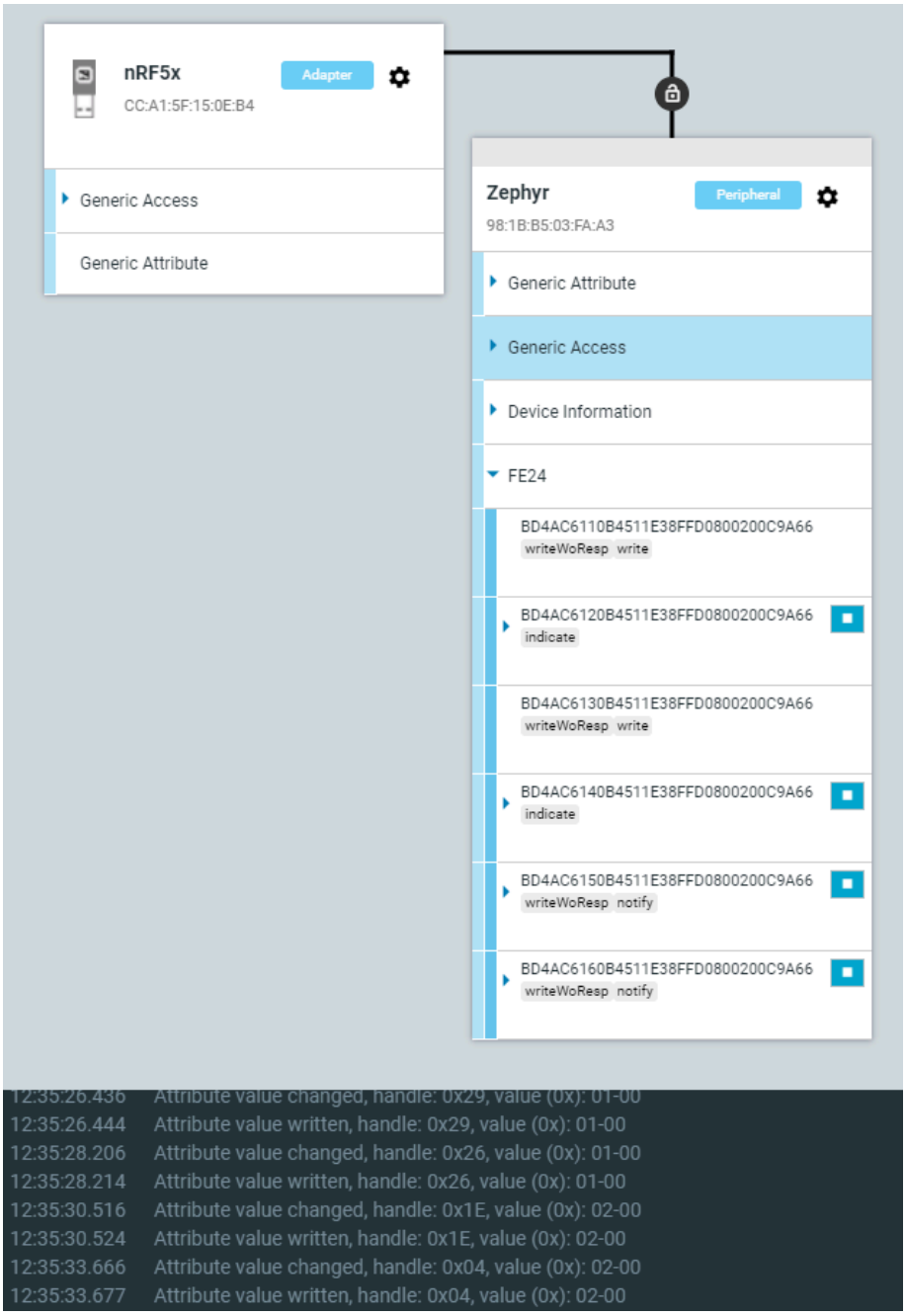


Figure 4.14 Commands Written Successfully to the Yale Conexis L1 via the nRF Connect Application

4.5.3.2 Wireshark Sniffing for Unencrypted BLE Data

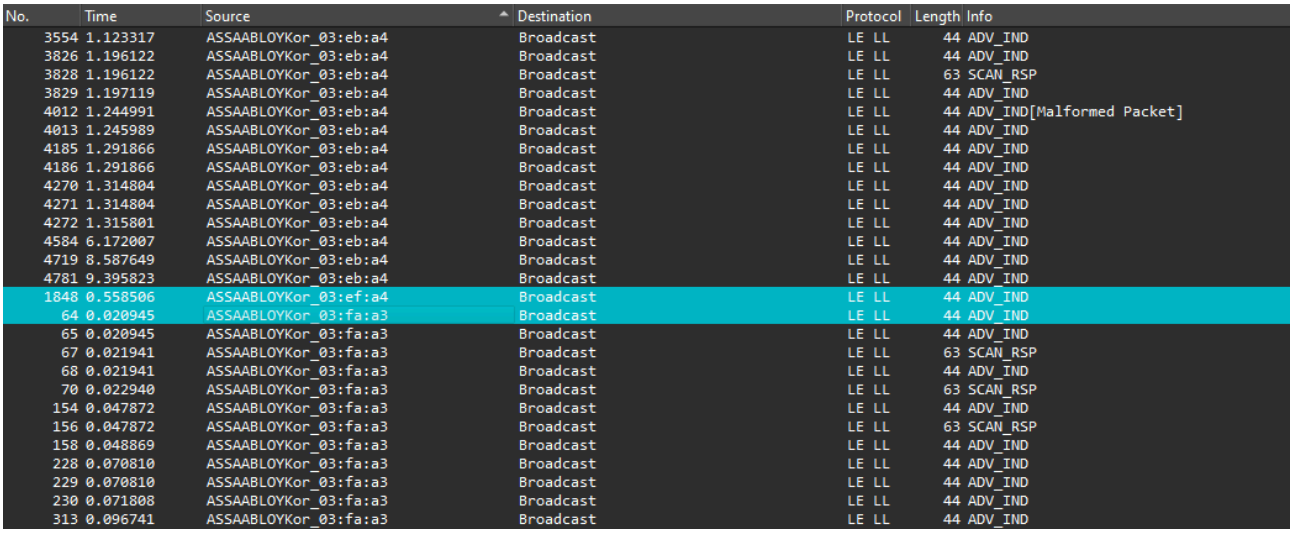
4. Using Wireshark and the nRF52840, the tester was able to sniff Broadcast packets from the Yale Conexis L1 lock, coming from two separate advertising channels;

- ASSAABLOYKor_03:be:a3 (98:1b:b5:03:be:a4) – As previously discovered in test 4.5.3.1.
- ASSAABLOYKor_03:fa:a3 (98:1b:b5:03:fa:a3)

These broadcasts from the Yale Conexis L1 show two packet types;

- **ADV_IND** which is “Advertising Indication”, advertising itself with basic information about the device, such as its address.

- **SCAN_RSP** which is “Scan Response”, an answer to a “Scan Request” (or **SCAN_REQ)** packet, which can contain additional device information, such as local names and service UUIDs (Universally Unique Identifiers).



No.	Time	Source	Destination	Protocol	Length	Info
3554	1.123317	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
3826	1.196122	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
3828	1.196122	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	63	SCAN_RSP
3829	1.197119	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
4012	1.244991	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND[Malformed Packet]
4013	1.245989	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
4185	1.291866	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
4186	1.291866	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
4270	1.314804	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
4271	1.314804	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
4272	1.315801	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
4584	6.172007	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
4719	8.587649	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
4781	9.395823	ASSAABLOYKor_03:eb:a4	Broadcast	LE LL	44	ADV_IND
1848	0.558506	ASSAABLOYKor_03:ef:a4	Broadcast	LE LL	44	ADV_IND
64	0.020945	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	44	ADV_IND
65	0.020945	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	44	ADV_IND
67	0.021941	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	63	SCAN_RSP
68	0.021941	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	44	ADV_IND
70	0.022940	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	63	SCAN_RSP
154	0.047872	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	44	ADV_IND
156	0.047872	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	63	SCAN_RSP
158	0.048869	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	44	ADV_IND
228	0.070810	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	44	ADV_IND
229	0.070810	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	44	ADV_IND
230	0.071808	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	44	ADV_IND
313	0.096741	ASSAABLOYKor_03:fa:a3	Broadcast	LE LL	44	ADV_IND

Figure 4.15 Identified Broadcasts from the Yale Conexis L1

5. Inspecting a **SCAN_RSP** frame broadcast from ASSAABLOYKor_03:be:a4 reveals the packet containing data broadcast from the Yale Conexis L1 Lock, including the UUID (Company ID) as August Home, Inc (0x01d1), and the Scan Response Data.

   A malicious actor could sniff this packet, and use it to craft a replay attack, in which they could replay the handshake of these packets, to bypass authentication and actuate the lock.

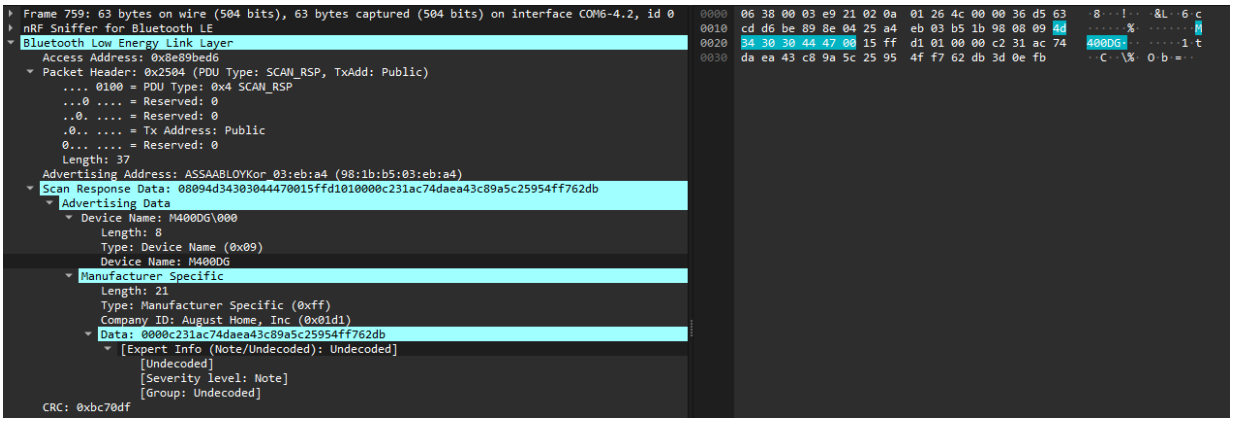


Figure 4.16 Inspection of a SCAN_RSP Broadcast packet sent by the Yale Conexis L1

Chapter 5 eLinkSmart Padlock P5BF Penetration Test

5.1 Engagement Contacts

Contact Name	Title	Contact Email
Callum Giblin	Primary Tester	cllmgbln@gmail.com

Table 5.1 Engagement Contacts for the eLinkSmart Padlock P5BF Penetration Test

5.2 Purpose & Scope

The purpose of this penetration test is to evaluate the security of the Yale Conexis L1 smart lock, with a specific focus on its BLE (Bluetooth Low Energy) technology, which serves as the smart component of this device. This assessment aims to identify potential known vulnerabilities within the lock, which could be exploited by malicious actors to gain unauthorised access.

This test will examine the BLE communication protocols, and the data encryption used by the device, documenting attack methods used and providing scoring and recommendations for any vulnerabilities found.

The scope of the testing is limited to the BLE functionality of the device, the in-scope assets can be found in Table 5.2 In-Scope Assets, below.

Asset (Device/Module/Unit)	Description
eLinkSmart Padlock P5BF	Physical lock device, a metal black circular padlock featuring a fingerprint biometric reader, with a metal shackle.

Table 5.2 In-Scope Assets.

Figures 5.1 show the assets outlined in Table 5.2 In-Scope Assets.

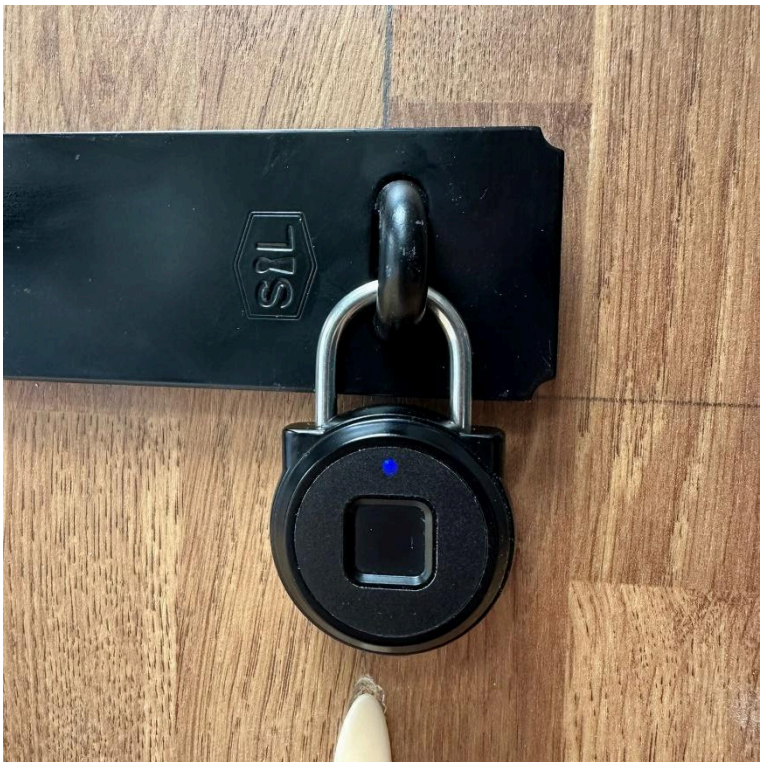


Figure 5.1 eLinkSmart Padlock P5BF

5.3 Summary of Findings

During the penetration test of the eLinkSmart Padlock P5BF, the tester found a total of 1 finding that highlight potential risks associated with this smart lock. Table 5.3 below, details the finding count and severity measurements.

Findings & Severity					
Critical	**High**	**Medium**	**Low**	**Informational**	**TOTAL**
1	0	0	0	0	1

Table 5.3 eLinkSmart Padlock P5BF Finding Severity Summary

Table 5.4 shows a high-level overview of the findings discovered during the testing process. The details of these findings are further examined in section 5.4 Detailed Findings.

Finding	Severity Level	Title	Description
1	Critical	BLE Authentication Vulnerability	No requirement to authenticate a BLE connection to connect to the device and gather details regarding the lock and send hexadecimal codes through the BLE services.

Table 5.4 eLinkSmart Padlock P5BF Findings Summary

5.4 Detailed Findings

5.4.1 1. BLE Authentication Vulnerability

5.4.1.1 Common Vulnerabilities and Exposures

Without the requirement to authenticate before a connection, BLE often allows a peripheral (such as a Smart lock) to be connected to a client and will display its characteristics.

5.4.1.2 Description

The tester was able to connect to the eLinkSmart Padlock P5BF and the nRF Connect application, this connection did not require authentication, and the tester was able to enumerate the characteristics of the eLinkSmart Padlock P5BF, such as the services the lock can perform and the name, manufacturer and the Bluetooth device address.

The tester was then able to actuate the lock through sending 4-bit hexadecimal code through the 2ADF service, this suggests a large security vulnerability, in which data sent via this BLE service, is not only unencrypted, but will accept any input to actuate the lock to unlock.

5.4.1.3 Impact and Likelihood

The impact of this attack would cause a malicious actor to be able to unlock the lock via BLE signals using simple equipment such as an nRF52840 and the nRF Connect for Desktop application, or the nRF Connect smartphone application, which would allow a malicious actor to be covert in the attack.

The likelihood for this attack is quite high, if this vulnerability was known by the malicious actor to be present within the estate.

As per *Appendix 1 Risk Severity Rating*, this finding has been rated as follows:
Impact: High
Likelihood: High
Overall risk: Critical.

5.4.1.4 Remediation & Mitigation Techniques

- The manufacturer should update the lock's firmware to enforce authentication checks before processing any input commands and should only accept authenticated and valid inputs to be able to actuate the lock.
- The manufacturer should implement secure communication channels when sending critical data over BLE and ensure that data is encrypted whilst in transit.
- The manufacturer should implement authentication for BLE communication, such as a challenge and response mechanism to verify the client (device) attempting to unlock the host (lock).

5.5 Detailed Walkthrough

5.5.1 BLE Attacks on eLinkSmart Padlock P5BF

5.5.1.1 nRF52480 Authentication Bypass Attack

1. Using the nRF52840, and the nRF Connect for desktop application, the tester attempted to scan and interact with the eLinkSmart Padlock P5BF, in order to execute services over BLE and attempt to get the lock to actuate, without being authenticated through the eSmartLock smartphone application. The tester was able to identify the device which had the name “P5BF-PG” broadcast over BLE, and the associated Bluetooth device address “A4:C1:38:2A:B1:EA”, and the tester was able to initiate a connection to the device without authentication successfully.

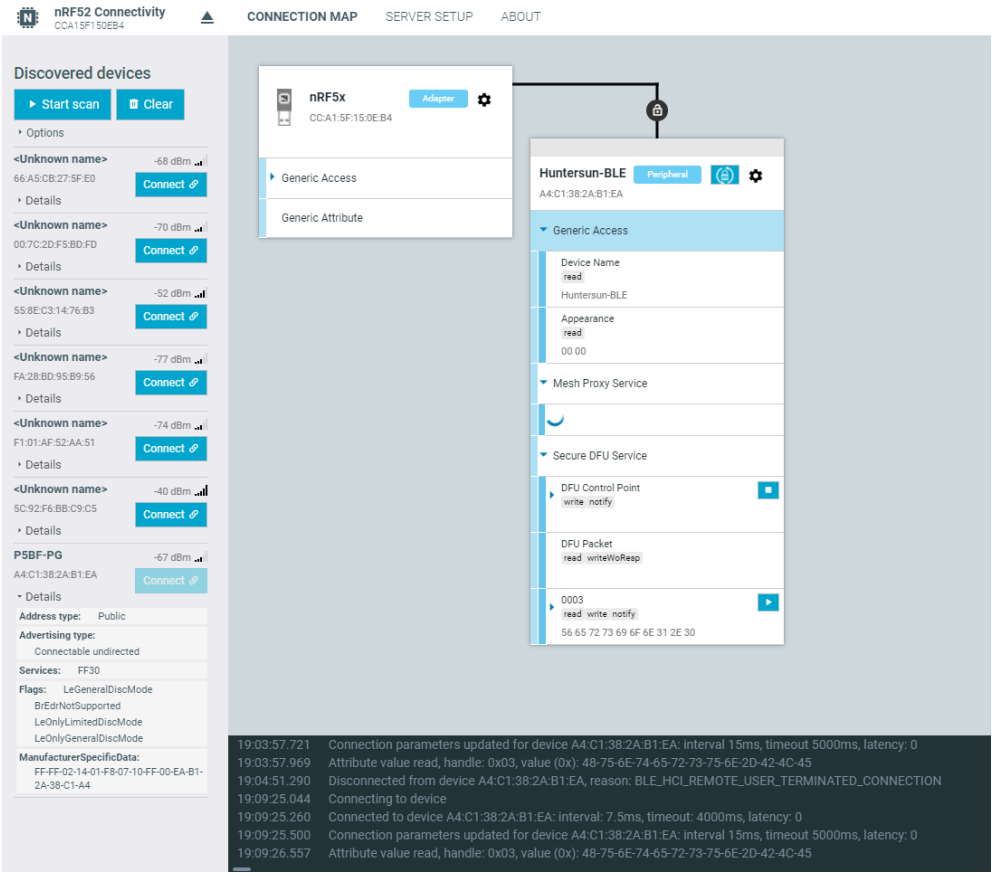


Figure 5.2 Successful BLE Connection from the nRF52840 to the eLinkSmart Padlock P5BF

2. After 1 minute of being connected, the lock disconnected from the nRF52840, likely a security measure implemented by the manufacturer into the device's firmware.

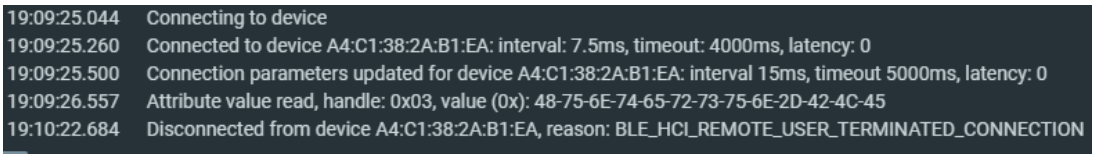


Figure 5.3 nRF Connect Logs Showing the Connection and Subsequent Disconnection to the eLinkSmart Padlock P5BF

3. The tester proceeded to attempt to cause the lock to actuate by sending commands through the services available through the nRFConnect application, the tester attempted sending multiple hexadecimal codes through the service named "2ADF", this actuated the lock. The tester tried sending multiple different hexadecimal codes through the service, all of which actuated the lock to unlock.

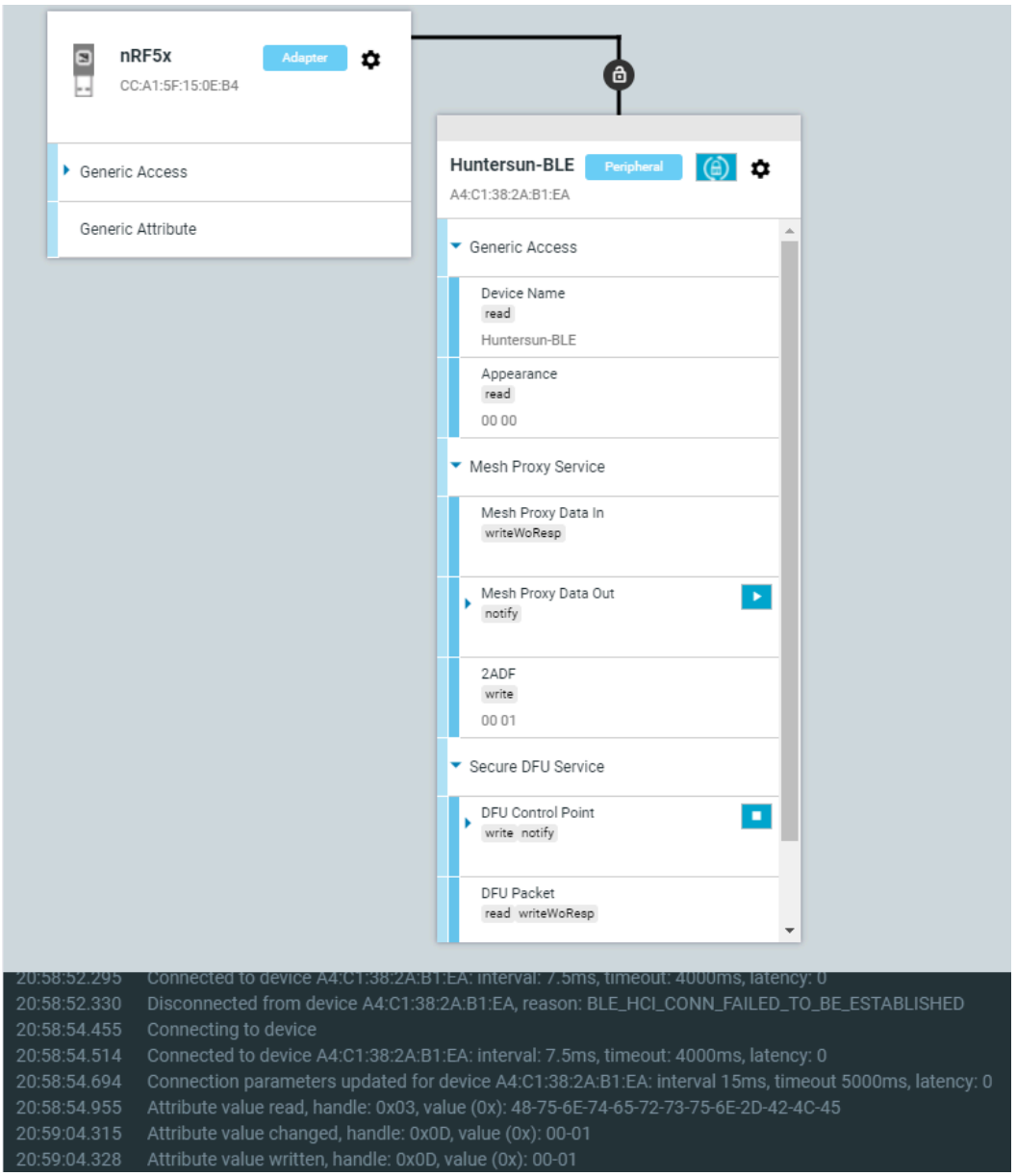


Figure 5.4 nRFConnect Sending Hexadecimal Codes via the 2ADF Service.

Chapter 6 Conclusion

6.1 Theme of Findings

Through the penetration testing process, there was a clear theme of vulnerabilities and weaknesses across the range of Smart IoT Locks discovered, highlighting a potential issue with the current smart locks available, that requires to be addressed before deployment of this technology to avoid creating additional vulnerabilities for DNO and CNI organisations.

Most of these findings are vulnerabilities introduced by the manufacturer not implementing strong authentication and encryption methods, therefore it is the manufacturer's responsibility to remediate these vulnerabilities, for example by distributing new firmware patches. The findings of this project have been sent to the manufacturers, detailing the vulnerabilities and weaknesses discovered in their products, as is required through the ethical standards of being a responsible cyber security professional performing penetration testing.

Three themes in the findings from this project highlight critical gaps in the locks security architecture that could be exploited are:

- Weak RFID Encryption: All the smart locks that had RFID functionality contained known vulnerabilities with insufficient encryption on RFID communications, making the lock vulnerable to cloning and interception attacks, allowing for unauthorised access with minimal effort using commercially available tooling and smartphone applications.
- Lack of BLE Encryption: The absence of encryption in the BLE communications, across the smart locks that used BLE as a communications protocol, exposed information that was broadcast between the host and the client. This allows for eavesdropping and Man-in-the-middle (MITM) attacks.
- Lack of authentication: Multiple locks tested lacked authentication protocols, not verifying authentication methods such as the validity of an RFID key card presented or the validity of a device sending the lock commands via BLE.

6.2 Recommendations from Findings

The recommendations from the findings outputted from the penetration tests carried out in this project include:

- Implementation of strong RFID encryption: Manufacturers should not rely on RFID technology that contains known vulnerabilities such as weak encryption, such as those found in the MIFARE Classic 1K RFID chipset. A better alternative would be using the MIFARE DESFire EV1 chipset, which

employs an AES hardware cryptographic engine for enciphering transmission data (NXP Semiconductors, 2015).

- Implementation of BLE encryption: Manufacturers should apply strong encryption standards to their BLE communications, and the data being transmitted over the protocol, for example using AES-128, which is currently not considered vulnerable to attacks with existing computational capabilities.
- Using an alternative communications protocol: There are alternative communications protocols to BLE that operate on the same frequency band (2.4 GHz), such as Zigbee, which natively supports AES-128, they may still be "sniffed" in an eavesdropping attack, however only the PAN ID and MAC-Layer addresses are non-encrypted, the payload (data being transmitted over the Zigbee protocol), is encrypted. (Digi, 2024).
- Internal testing before product deployment: The manufacturers should implement security testing as part of their product life cycle, following a DevSecOps lifecycle whilst developing their smart locks would allow specialist professionals to test and highlight commonly known vulnerabilities and weaknesses before the product is available to consumers containing security flaws.

6.3 Future Work

For the continuous research and development of this project, research of emerging threats for new IoT vectors could help identify potentially unknown vulnerabilities to smart locks. Performing threat-hunting activities such as vulnerability research focusing on the hardware of the smart lock. Such hardware attacks like fault injection attacks and side channel power analysis will give the tester details on the relationship of the hardware and how it interacts with associated firmware, it may also be possible to extract cryptographic keys from the integrated circuits in the lock.

Furthermore, to identify emerging threats, the development of a threat intelligence feed that can utilise existing intelligence platforms, and security advisories, would assist in keeping informed on any developing attack methods, vulnerabilities and weaknesses that could impact smart IoT locks.

If permission was granted by manufacturers, it may be useful during the penetration testing process to reverse engineer the associated smartphone applications, as this may provide encryption keys, authentication mechanisms and credentials that could be used by a malicious actor to launch further attacks on a smart lock, such as bypassing authentication.

Chapter 7 Critical Evaluation

7.1 Strengths and Achievements

Within this project, I was able to successfully develop my penetration testing skillset to be tailored to a specific niche of penetration testing IoT devices, I employed techniques that I had learned through a combination of reading technical sheets, training materials and through trial and error of various testing methods. I leveraged a range of hardware and software tools, which I am now proficient in using, such as Proxmark3, Wireshark and nRFConnect for Desktop and the associated hardware and setup to allow the hardware to communicate successfully with the software, something that I did not document within this project. The successful identification of vulnerabilities within the IoT smart locks selected for this project is evidence of the knowledge and skills I have gathered in my training.

The testing methodologies I utilised within this project, whilst limited in scope, proved to correctly identify key vulnerabilities and flaws within the products tested, and the findings have been responsibly disclosed to the manufacturers involved, to ensure that they can develop patches and other mitigation measures where appropriate.

Upon completion of this project, I have contributed to the wider industry knowledge, by sharing this knowledge with manufacturers, CNI and DNO organisations, offering actionable security recommendations to enhance future IoT smart lock security models, their associated firmware, and an awareness of common vulnerabilities that can impact the security of this type of device so organisations can make further informed decisions about what technology they choose to deploy.

7.2 Project Limitations

The project did have some limitations, for example, the limited testing scope focusing on BLE and RFID security, I chose products that had these two technologies as their main form of being “smart”, whilst it should be noted that there are other smart lock products available that have other communication protocols, such as Wi-Fi or Zigbee, and have other technologies such as biometrics and encrypted infrared (IR) signals. However, the technology required for the penetration test of these technologies is often costly and requires a high level of skill to understand and I didn’t provision time for this type of testing.

There was also a limitation in the BLE penetration of the smart locks, whilst often in the findings I referred to the malicious actor being able to enumerate the unencrypted data, the attacks that could be crafted with this data were not demonstrated within the testing, this is largely due to the complex nature of crafting specific attacks that can inject and manipulate BLE packets. Given more time and resources I would like to have been able to perform this type of testing, however, I was confident in reporting the unencrypted data

that was available and highlighting that subsequent attacks could be mitigated by having this data encrypted.

Some limitations in the project came from my own understanding of specific technology, as I was developing my skills and knowledge in RFID, I was not aware of the width and breadth of available RFID chipsets, and how each chipset from each manufacturer was able to perform different functions and how different the structure of data is stored across different chipset types, I was able to consult specialists via public RFID forums on specific queries I had which proved to be useful when I needed guidance, however, the technical data sheets provided by manufacturers, for example NXP Semiconductors also provided low-level technical details.

Reference list / Bibliography

Caballero-Gil, C. et al. (2023). Research on smart-locks cybersecurity and vulnerabilities. Available at: https://link.springer.com/article/10.1007/s11276-023-03376-8 (Accessed: 01 May 2024).

Computer Misuse Act 1990, s 3. Available at: https://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences (Accessed: 01 August 2024).

CVE (2019) *CVE-2019-17627*. Available at: https://www.cve.org/CVERecord?id=CVE-2019-17627 (Accessed 15 August 2024).

CVE (2024) *CVE-2023-26941*. Available at: https://www.cve.org/CVERecord?id=CVE-2023-26941 (Accessed: 15 August 2024).

Digi (2024) *ZigBee Encryption*. Available at: https://www.digi.com/support/knowledge-base/zigbee-encryption (Accessed: 17 August 2024).

Elison, J. (2024) *New legislation will help counter the cyber threat to our essential services*. Available at: https://www.ncsc.gov.uk/blog-post/legislation-help-counter-cyber-threat-cni (Accessed: 30 July 2024).

Fitzsimmons, F. (2016) *Crooks putting lives at risk by targeting electricity substations to steal metal*. Available at: https://www.liverpoolecho.co.uk/news/liverpool-news/crooks-putting-lives-risk-targeting-11948366 (Accessed: 01 May 2024).

Giblin, C. (2024a) Photograph of a *Danger of Death Signage on an Electrical Substation*. Liverpool, England.

HackerOne (no date) *Why You Need Responsible Disclosure and How to Get Started*. Available at: https://www.hackerone.com/knowledge-center/why-you-need-responsible-disclosure-and-how-get-started (Accessed 01 August 2024).

ISEO (no date) *How the administrators of Enedis assign temporary access permissions to sensitive sites also to external consultants and track their use with LSA software*. Available at: https://iseo.com/en/SuccessStories/EnedisElectricityCompany?_gl=1*1rz12ut*_up*MQ..*_ga*MjExMDI2NjMyMS4xNzE1NzE4NDcy*_ga_WMP0WZ2FVG*MTcxNTcxODQ3Mi4xLjEuMTcxNTcxODUzNi4wLjAuMA (Accessed: 01 May 2024).

LAB401 (no date) *Ultimate Magic Card (Gen4)*. Available at: https://lab401.com/products/ultimate-magic-card-gen4?srsltid=AfmBOoqkDbSt7fOFn950xgUZrEbhL6r4pO5o6wWtp8MWfXV9CAt_Bihf (Accessed: 17 August 2024).

Marcel, J. (2022) *New Wireless Trends and Forecasts for the Next 5 Years*. Available at: https://www.bluetooth.com/blog/new-trends-and-forecasts-for-the-next-5-years/ (Accessed: 20 August 2024).

MITRE (2022) *CWE-1394: Use of Default Cryptographic Key*. Available at: https://cwe.mitre.org/data/definitions/1394.html (Accessed: 20 August 2024).

NCSC (2024) *Cyber Assessment Framework*. Available at: https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-b/principle-b2-identity-and-access-control (Accessed: 01 May 2024).

NXP Semiconductors (2015) *MIFARE DESFire EV1 contactless multi-application IC*. Available at: https://www.nxp.com/docs/en/data-sheet/MF3ICDX21_41_81_SDS.pdf (Accessed: 17 August).

OFGEM (2024) *Network price controls 2021-2028 (RIIO-2)*. Available at: https://www.ofgem.gov.uk/energy-policy-and-regulation/policy-and-regulatory-programmes/network-price-controls-2021-2028-riio-2/network-price-controls-2021-2028-riio-2-electricity-distribution-price-control-2023-2028-riio-ed2 (Accessed: 30 July 2024).

Okin, S. (2020) *RIIO-2 Cyber Resilience Guidelines.* Available at: https://www.ofgem.gov.uk/sites/default/files/docs/2020/04/riio2_cyber_resilience_guidelines.pdf (Accessed: 30 July 2024).

OWASP (2023) *OWASP Risk Rating Methodology*. Available at: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (Accessed: 01 May 2024).

Trading Economics (2024) *Copper*. Available at: https://tradingeconomics.com/commodity/copper (Accessed: 16 August 2024).

U.S Department of Homeland Security (2024) *Radio Frequency Identification (RFID): What is it?* Available at: https://www.dhs.gov/archive/radio-frequency-identification-rfid-what-it (Accessed: 19 August 2024).

Yale (2023) *Product Security Advisory – MIFARE Classic*. Available at: https://www.yalehome.com/global/legal-and-privacy/product-advisory/Yale-PA-2023-01.pdf (Accessed: 15 August 2024).

Appendix 1 Risk Severity Ratings

To calculate the potential risks caused by the vulnerabilities found in the penetration tests, tables 7.1 and 7.2 below has been developed, loosely based on the OWASP Risk Rating Methodology.

Table 7.1 details the rating scales for the levels of likelihood and impact. The likelihood is scored on the probability that the identified vulnerability could be exploited, considering the ease of attack and exposure. The Impact is scored on the potential damage or harm that could result from the exploitation of the vulnerability.

Likelihood and Impact Levels	
Score	**Rating**
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Table 7.1 Likelihood and Impact Levels Matrix

Combining the scores from the likelihood and impact levels will give an overall risk severity rating, as detailed in Table 7.2.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Negligible	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Table 7.2 Overall Risk Severity

(OWASP, 2023)

Appendix 2 RFID Technology

Radio Frequency Identification RFID is a wireless communications technology that consists of two devices, one is the “reader”, which reads information contained in the wireless RFID tag (also referred to as a card, key card or key fob).

According to the U.S. Department of Homeland Security, RFID technology has been commercially available in one form or another since the 1970s, and it has multiple use cases, such as car keys, employee identification, medical history/billing, highway toll tags, and security access cards (2024).

Most RFID tags do not contain any power source, instead receiving power from electromagnetic fields output by the reader, this kind of tag is known as a passive tag. On the other hand, active tags contain an internal power source, such as battery, giving the tag a longer range and the ability to continuously broadcast data.

RFID can be put into three different categories, depending on what part of the spectrum it operates in;

- Low Frequency (LF) – operating between 30-300 kHz. For example, the T577 125kHz RFID chip.
- High Frequency (HF) – operating at 13.65 MHz. For example, the MIFARE Classic 1K RFID chip.
- Ultra-High Frequency (UHF) – operating at 300 MHz-3 GHz. For example, the Impinj Monza R6 series RFID chips.

Each category of RFID chip offers different tangible benefits, depending on the use case scenario, such as the physical range the chip can be wireless communicated with, and each chip type within these categories can also offer its own tangible benefits, such as integration to specific technologies.

Some RFID chips can contain data that can be communicated to a reader, and be written, and re-written to as desired, the data held on the chip depends on the chip type, but can include data such as:

- Cryptographic keys
- UIDs that act as a key
- Inventory details
- Metadata
- User data

Modern-day applications for RFID technology include making contactless payments, either through a physical credit/debit card or through emulation from a smartphone or other smart device such as a smartwatch.

Whilst some applications of RFID use require high levels of security, such as making wireless payments, other applications do not require such strict security considerations. For example, the LF chips that are used as “microchips” in pets such as dogs and cats, are unlikely targets for a malicious actor, therefore the risks associated with using an RFID chip that has known vulnerabilities are much lower than other use cases.

In this project, the terms *chipset, tags, cards, keycards,* and *key fobs* are used interchangeably depending on the specific use case.

Appendix 3 BLE Technology

Released in 2010 as part of the Bluetooth 4.0 Specification, Bluetooth Low Energy (BLE) is a wireless communications protocol technology, designed for low-power, short-range connectivity. The protocol has many use cases, such as smartphones, smartwatches, wireless headphones and smart locks to name a few examples.

The use of BLE is forecast to increase, and Bluetooth Classic is expected to decrease, following its trend over the past 7 years, as the proprietary form of Bluetooth communication in Bluetooth Enabled Devices in the coming years, with 95% of all Bluetooth devices to include BLE by 2026 (Marcel, 2022).

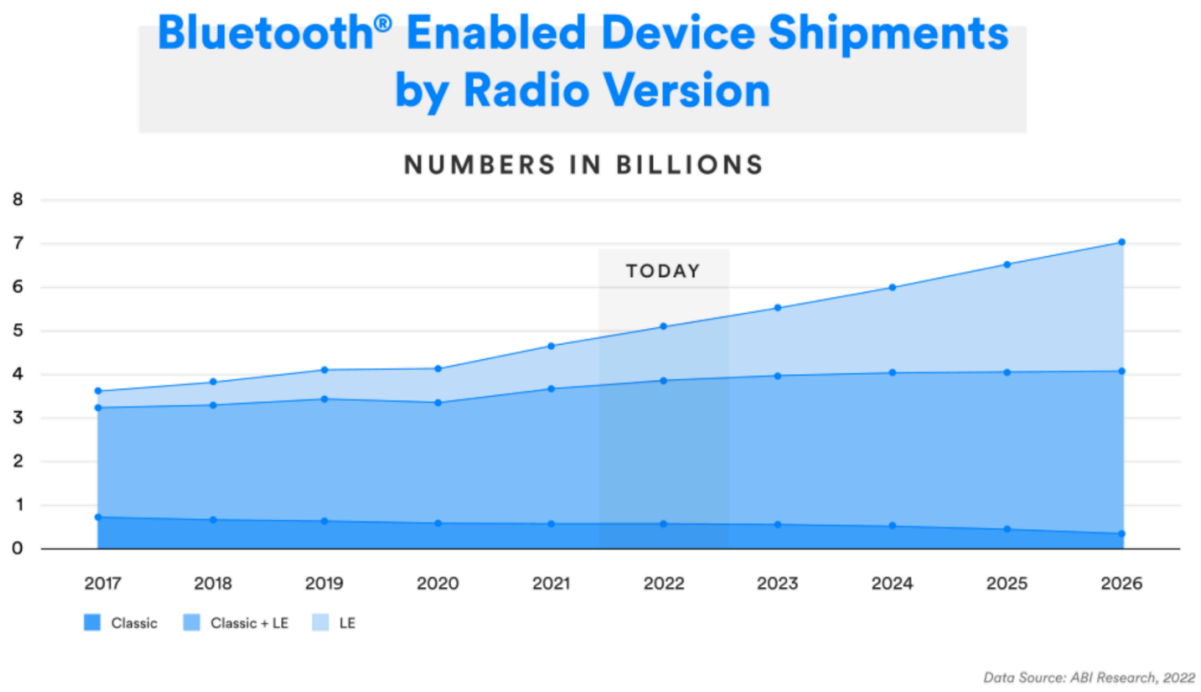


Figure 7.1 Bluetooth Enabled Device Shipments by Radio Version

BLE operates on the 2.4 GHz band, similar to Wi-Fi and Bluetooth Classic, but uses different protocols. BLE communications can be sent between a client and a host, connection between these devices works through advertising packets, scan response packets and connection request packets, working together in a 3-way handshake between the devices.

Appendix 4 Magic Cards

Magic cards are specific types of RFID cards that are designed to allow users to bypass restrictions that are usually in place on RFID tags, for example, MIFARE Classic cards do not have UIDS that can be altered, however, their Magic counterparts do have the ability to change this data, enabling them to be used as cloned versions of MIFARE Classic cards.

Magic cards are a tool often used by penetration testers and security researchers to identify weaknesses in RFID security systems.

According to LAB401 (no date), a company that sells cyber security tools and produces informational articles aimed at cyber security professionals, Magic cards have the following configurable parameters:

- Preset Card Type
- UID
- UID Length (4-byte / 7-byte / 10-byte)
- SAK (1 byte)
- ATQA (2 byte)
- ATS (Custom length / disable)

Appendix 5 LEPSI Form

REDACTED

Name: Callum Marc Giblin

Date: 13/09/2024