Degree Project

Illuminating threats:

Exploring cybersecurity threats in smart bulbs and illuminating a path to enhanced protection

Master Degree Project in Informatics with a specialization in Privacy, Information and Cyber Security

Second Cycle 30 credits

Spring term 2024

Student: Francisco Formosinho

Supervisor: Sten F Andler

Industrial Supervisor: Yousef Abdelkhalek, Knightec AB

Examiner: Ali Padyab

Abstract

There are serious security risks with the growing use of IoT devices. Historically, manufacturers prioritized profit over security due to high demand, a perspective that has evolved but remains a challenge. With this, the security of IoT devices has been overlooked, especially regarding smart bulbs, as they tend to be bundled with other IoT devices by the research community, and consequently not receive the attention they require.

This thesis aims to identify and analyze potential threats regarding smart bulbs, and it does so by exploring proactive strategies in order to mitigate vulnerabilities. To understand the challenges smart bulbs face, some of the current applicable legislation, cyber attacks, defense mechanisms, and vulnerabilities were analyzed. Then, a network topology and a data flow diagram of a home network with smart bulbs was developed. Consequently, layers were assigned to the smart bulb, and threat modeling was performed on a each layer using STRIDE. This procedure was then formalized with a framework that encapsulates the stages of analysing the smart bulb's landscape through threat modeling.

This work contributes to the research community's body of knowledge by providing valuable insights detailing the smart bulb's landscape, not only through the framework but also through the conducted threat modeling, the data flow diagrams, and the information gathered regarding the threats to smart bulb security.

Keywords: Smart bulb security, Internet of Things, Threat modeling, Framework, Design Science Research

Contents

List of Figures

List of Tables

1. Introduction

With the increasing integration of products into the Internet in today's digital era, ensuring their safety and security has made product cybersecurity essential. Cybersecurity incidents may result in serious consequences for manufacturers and consumers alike, such as financial losses or reputational damage. In product cybersecurity, the entire lifecycle of the product is carefully considered, from design and development to deployment. This involves implementing features and protocols to prevent vulnerabilities, unauthorized access, data breaches, amongst other cyber threats, while also covering domains such as secure coding practices, robust encryption methods, strict access controls, and timely software update procedures. Proactive identification and mitigation of potential risks is a key component of product cybersecurity, as it ensures that products not only meet functional requirements but also adhere to high standards of resilience and protection against evolving cybersecurity challenges.

The Internet of Things (IoT) has made the Internet more immersive and more prevalent by connecting everyday devices to it. These devices are usually equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks. Due to the heterogeneous application of IoT devices and their rapid adoption rate, there are no strict standards that every IoT device follows. There are simply too many protocols, standards, and a lack of agreement on which works best for individual layers of the IoT (Al-Qaseemi et al. 2016). Despite the initial inclination to develop a unified system to manage this diversity, the reality is that existing IoT infrastructure and deployed devices cannot be easily redesigned. This poses a challenge in simplifying the management, operation, and security of IoT devices. Due to not being able to redesign the devices that have been deployed, efforts are made to fortify them instead.

The increasing adoption of IoT devices raises significant security concerns. Historically, manufacturers prioritized profit over security due to high demand, a perspective that has evolved but remains a challenge. Generally, it is never a good idea to postpone the security of a system, but it is especially not a good idea when the system faces the challenges IoT devices face. These inherent challenges arise from factors such as limited processing power, memory constraints, and difficulty accessing devices. Consequently, the security of these devices has often been compromised. Despite these challenges, the growth of adoption shows no signs of slowing down. As of the current writing in 2024, there are more than 15 billion devices connected to the IoT globally, and projections suggest that this number will nearly double by 2030 (Statista 2023).

Smart bulbs represent a frequently overlooked category of IoT devices due to their apparent limited impact if compromised, but the unsuspecting user may not realize to what extent data, such as usage patterns or even network credentials, can be gathered from these seemingly simple devices. Smart bulbs were designed for convenient lighting control and are embedded with communication capabilities which are often connected to the Internet. As a result, if these devices are compromised, they might unintentionally start acting as channels for private information. Security concerns with smart bulbs usually originate from their connectivity features which, if compromised, can lead

to unauthorized access and data exposure. Due to the widespread consumer adoption in recent years, smart bulbs have become a prevalent component of smart home ecosystems and their popularity ensures that research findings can impact a large and diverse user base.

An example of extending the functionality of a smart bulb, beyond what a regular user might suspect is feasible, was demonstrated when a smart bulb was used to create a covert channel to exfiltrate data (Ronen and Shamir 2016). This channel was resistant to interference, easily detectable from a long distance, and not perceivable to the human eye. In the end, the authors claim their channel could be used to leak more than 10KB per day, which is enough bandwidth to leak private encryption keys and passwords from a highly secure, or even fully air-gapped office building (i.e., physically isolated from external networks and internet connections).

Another example was demonstrated when a new type of threat was described in which adjacent IoT devices would infect each other, given that the density of the devices (i.e., the number of devices randomly spread over a certain area) was greater than a certain critical mass. Essentially, this describes an IoT worm, and it could target smart bulbs and spread by infecting its neighbors, using only their built-in Zigbee wireless connectivity (more on Zigbee in Section 2.1.4) and their physical proximity (Ronen, Shamir, et al. 2017). In essence, the authors showed that, by plugging in a single infected bulb, it was possible for an attacker to infect an entire city. Although specific numbers describing the deployment of smart bulbs were not found, the authors claim that the critical mass for the city of Paris, whose area is about 105 km^2, is 15.000 smart bulbs. This means that the chain reaction would fizzle if there were fewer than 15.000 smart bulbs in Paris and spread otherwise. The authors also claim that this number has almost certainly been passed already, which indirectly shows the proliferation of smart bulbs.

Furthermore, due to their low cost and easy deployment, IoT devices may be installed in a variety of critical sectors such as healthcare, supply chain, energy production and distribution, water supply, and transportation (Stellios, Mokos, and Kotzanikolaou 2021). Naturally, in the context of critical infrastructure, the impact of an incident can be catastrophic as the provision of basic needs may be halted. For example, if lighting systems from an hospital's surgery room are compromised, surgeries can be interrupted. Additionally, it is feasible to cause epileptic seizures with flickering lights (Morgner, Mattejat, and Benenson 2016).

As the proliferation of IoT continues, understanding the latent privacy and security implications associated with seemingly benign devices like smart bulbs becomes imperative. Users should not only be aware that privacy and personal information may be jeopardized by security flaws, but also actively protect themselves. Choosing robust encryption algorithms, strong authentication procedures or updating their firmware frequently, are just a few examples of the security measures that can be put in place to mitigate potential risks associated with these interconnected IoT devices.

This thesis aims to contribute to the research community's body of knowledge by providing valuable insights into detailing the smart bulb's landscape, which is achieved by providing a framework that performs threat modeling on each layer that composes a smart bulb, along with countermeasures to each identified threat.

1.1. Research problem

While awareness of IoT security risks has increased over the years, it is important to note that the security landscape is constantly evolving and new vulnerabilities consistently emerge. Smart bulbs have reimagined lighting, granting users control over brightness, color, and schedules through apps or voice commands. However, this convenience comes with cybersecurity concerns. Striking a harmony between innovation and cybersecurity ensures that our illuminated homes remain both connected and protected.

Although there are several standards and frameworks regarding IoT security, they typically adopt a holistic approach, addressing the overall security of IoT devices. This is because regulations, frameworks, and standards are intentionally broad in order to encompass different scenarios. Consequently, despite the objectives being clear, how to achieve them is often not. An example of this can be found in a study where the authors examined the overwhelming number of standards that apply to IoT-based smart environments, such as smart homes and smart cities (Karie et al. 2021). The authors concluded that most of the conventional security standards and assessment frameworks did not directly address the security needs of IoT-based smart environments, since they focused on specific areas (e.g., smart home, cloud, health) but had the potential to be adapted into other IoT-based smart environments. To make such claims, the authors analyzed 80 ISO/IEC security standards, 32 ETSI standards, and 37 different conventional security assessment frameworks, which included 7 NIST special publications on security techniques. Naturally, given that smart bulbs are usually found in IoT-based smart environments, they are included in this study's scope. Ultimately, this study highlights the complexity of securing these devices given the numerous standards and frameworks applicable to the broader IoT ecosystem.

The research problem lies in the absence of a tailored security framework, a gap this thesis aims to close when considering smart bulbs.

1.2. Research question

By meticulously examining the vulnerabilities inherent in smart bulb technology, this research aims to identify and analyze potential threats. Additionally, this study explores proactive strategies to mitigate these vulnerabilities. To do so, it conducts an in-depth analysis of the security features and potential vulnerabilities of smart bulbs in order to assess a smart bulb's security posture comprehensively and develop countermeasures in order to enhance its resilience against cyber threats.

The ultimate goal is to develop a tailored framework towards smart bulbs with a threat model at its core that contributes with valuable insights to the ongoing discourse on enhancing the security of smart bulbs. The target audience of this work is the research community and its novelty lies in the in-depth analysis focused on the security of the smart bulb. As a result, the research question is posed as:

What are the security threats and vulnerabilities of smart bulbs in home IoT environments, and how can a tailored framework guide the development of countermeasures

to safeguard these devices?

1.3. Delimitations

This thesis focuses on evaluating the overall security of smart bulbs and their components, excluding expansive topics such as privacy, artificial intelligence, and blockchain from its scope. Another notable delimitation is the fact that this research focuses on smart bulbs rather than the general IoT.

Lastly, due to the heterogeneity of smart bulb controllers (e.g., mobile applications, radio frequency or infrared remotes, voice assistant), only the most common controller was analyzed, namely the mobile application.

1.4. Thesis structure

The outline of this thesis is structured as follows:

- Chapter 1 - Introduction: provides the introduction to the topic, its relevance, and the thesis' aim and objectives. Additionally, it exposes the research problem, highlights the research question, and presents the delimitations of this work;
- Chapter 2 - Background: provides the necessary knowledge needed in order to grasp the rest of the work by giving definitions and brief introductions to essential concepts (Section 2.1), highlights the tripartite amongst legislators, manufacturers and threat actors (Section 2.2), what countermeasures are taken in order to prevent cyber attacks, namely through penetration testing and threat modeling (Section 2.3), and summarizes the relevant state of the art (Section 2.4);
- Chapter 3 - Methodology: introduces design science research, along with the process of data collection, analysis, and the chosen approach to threat modeling;
- Chapter 4 - Threat modeling: presents and describes the proposed threat model, resorting to tools such as data flow diagrams and STRIDE (Microsoft 2022). This chapter is then split into subchapters, each concerned with a layer of the smart bulb;
- Chapter 5 - Framework: presents and describes each stage of the framework;
- Chapter 6 - Implementation & Results: describes how design science research was applied in order to validate the research;
- Chapter 7 - Discussion: contextualises the results of the framework and discusses its impact, its ethical and societal aspects, and its limitations;
- Chapter 8 - Conclusion: summarizes and concludes the thesis, with future work being suggested.

2. Background

This chapter serves as the backbone of the conducted research and it is organized into four subchapters: "Preliminaries" (Section 2.1), which covers the essentials of what is required to know in order to understand this research, "Legislation & Cyber Attacks" (Section 2.2), which highlights the tripartite amongst legislators, manufacturers and threat actors, "Defense Mechanisms" (Section 2.3), which presents countermeasures that are taken to prevent crime, namely penetration testing and threat modeling, and "Research background" (Section 2.4), that summarizes the relevant state of the art.

2.1. Preliminaries

This subchapter contains the definitions and brief introductions of what is required to know in order to understand the conducted research.

2.1.1 What is a smart bulb?

A "smart bulb" (also referred to as "smart light" or "smart lamp") is a bulb with connectivity capabilities. The key components that every smart bulb has are LEDs, or other forms of light emitters, a connectivity module (e.g., Wi-Fi, Bluetooth, Zigbee), a power supply module, integrated circuits, and a heatsink. The LEDs provide the visible output with components such as brightness, hue, and colour. The connectivity module acts as a bridge between the bulb and the user, by enabling remote control and providing feedback in return. The power supply module provides power to the whole system. The integrated circuits include a microcontroller that has been programmed with firmware that operates the logic controlling the bulb. Lastly, smart bulbs contain a material with high thermal conductivity (e.g., aluminum) that provides a large surface area for heat to transfer into the surrounding air, thereby dissipating heat and acting as a heatsink.

Generally, smart bulbs allow users to remotely control them by adjusting their status (on/off), colour, brightness and hue. Additionally, smart bulbs can contain features such as voice recognition, voice assistant integration, motion sensors, energy monitoring, music syncing, and many more. Moreover, smart bulbs can have schedules (e.g., dim lights for x minutes before bedtime) or even integrate a more complex environment where their activity is orchestrated by an external device (e.g., turn the light red and blink when a device connected to the network is being attacked).

2.1.2 What is an IoT Gateway?

An "IoT gateway" (also referred to as "gateway" or "hub" (Morgner, Mattejat, and Benenson 2016)) is a device that acts as a bridge connecting IoT devices and the wider network or cloud infrastructure. These devices provide several functionalities including serving as a central communication hub linking diverse IoT devices within

a home network. They also play a crucial role in protocol translation, addressing the heterogeneity of protocols used amongst IoT devices. As such, they facilitate internet connectivity, ensuring seamless communication between devices and external services. Moreover, they contribute to security measures, offering capabilities such as encryption and authentication to safeguard communication.

If an attacker compromises a gateway, every device connected to it can be targeted. Therefore, gateways are considered high-value assets. Despite playing a crucial role, Lins and Vieira (2021) claim IoT gateways have not received the necessary attention by the community, as most standards focus on the security of the individual things, or smart bulbs, while disregarding the properties of the gateway itself.

2.1.3 What are IoT layers?

An "analysis" is the process of examining, breaking down, and studying something in detail to understand its components, structure, and functionality. If this process is applied to an IoT device, then a layer refers to each component, structure, or functionality that composes the device being analyzed. Despite the number of layers not being fixed due to its dependency on the analyzed device and its context, it usually ranges from 3 to 7 layers. For example, a 3-layer architecture would have "perception, network and application" layers while a 5-layer architecture would have "perception, network, processing, application and business". Due to its popularity and simplicity, this work expands on the 3-layer architecture, which consists of:

- **Perception:** consists of the light bulb itself, equipped with sensors, actuators, and connectivity features to collect data on its environment (e.g., ambient light levels, motion detection). This layer acts as a medium between the digital and the real world;
- **Network:** responsible for bridging the perception and the application layer (e.g., IoT gateway, router);
- **Application:** where the data is analyzed and utilized to make decisions or trigger actions (e.g., smartphone app).

This 3-layer architecture is expanded and contextualised to a smart bulb's environment in Chapter 4.

2.1.4 What is Zigbee?

Zigbee is a wireless network communication protocol designed for low-power, low-data-rate, and close proximity devices. This protocol has become one of the most popular in order to connect smart home devices and appliances. In a Zigbee network, there are three types of devices, each playing a specific role in the network (Fan et al. 2017):

- **Zigbee Coordinator (ZC):** is the most critical device in the network, and there can only be one ZC. It is responsible for initiating, forming, and maintaining the Zigbee network. The ZC cannot sleep, and continuously manages the network.
- **Zigbee Router (ZR):** acts as intermediate nodes between the ZC and ZEDs, facilitating the routing of traffic. ZRs extend the network's range by relaying

messages between devices and can also allow other ZRs and ZEDs to join the network. ZRs cannot sleep, ensuring they are available for routing and network maintenance.

- **Zigbee End Device (ZED):** are the simplest devices in the network, often designed for low power consumption. They do not participate in routing traffic or network management, making them straightforward devices. ZEDs can enter sleep mode to conserve power when not actively communicating.

When dealing with smart bulbs, if the smart bulb is equipped with Zigbee functionality, it requires a smart hub. In this scenario, the smart bulb operates as the ZED, while the smart hub serves as the ZC.

2.1.5 What is a cyber attack?

The National Institute of Standards and Technology (NIST) defines a cyber attack as "any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself" (NIST 2024a). It is also common to refer to the compromise of one of the CIA triad components when defining a cyber attack. The CIA triad is the basis of information security and it stands for "confidentiality, integrity and availability", where each component is compromised when data is accessed, modified, or made inaccessible, by non-authorized entities, respectively.

2.1.6 What is threat modeling?

One of the many definitions of "threat" is "any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service" (ENISA 2023). With this broad definition, a threat can assume many shapes and forms.

Threat modeling is an essential component regarding the analysis of the security of an asset. First, one must understand the system in order to truly understand what threats are most applicable to it. Thus, threat modeling serves as a foundational pillar for subsequent activities, such as informing risk management, and therefore preceding it. The ultimate goal of threat modeling is to enhance decision-making about an asset's security risks, by identifying relevant threats and then suggesting appropriate countermeasures to mitigate, or even prevent, possible threats. Naturally, this analysis is the first step when improving the overall security posture of the target asset, since it consequently sheds light on where resources should be applied in order to effectively tackle security concerns.

2.2. Legislation & Cyber Attacks

This section attempts to portray the surface of the landscape that represents the tripartite amongst legislators, manufacturers and threat actors. In short, the manufacturers have historically responded to meet the consumers' demand for IoT devices, while concurrently threat actors have exploited the security vulnerabilities associated with

these devices. To address this issue, new legislation has been developed in an attempt to improve the vendor's security posture, and while stringent laws may improve the manufacturer's security and deter threat actors, they may also come at the expense of hindering manufacturers' production. In essence, there has been an effort for legislators to develop legislation that attempts to reduce the criminality while not posing as an obstacle for manufacturers.

This section briefly covers three topics, namely: the Cyber Resilience Act (CRA) (European Commission and Directorate-General for Communications Networks, Content and Technology 2022) in Section 2.2.1, which is a legislation directed towards manufacturers and lays out the requirements in order to strengthen their security; the IoT Security Assurance Framework (Section 2.2.2), which is a framework that provides a comprehensive set of guidelines and best practices for securing IoT devices; and cyber attacks in IoT (Section 2.2.3), which examines the common criminal aspects of IoT devices.

2.2.1 Cyber Resilience Act

According to the European Commission (EC), successful cyber attacks had an estimated global annual cost of EUR 5.5 trillion by 2021. In order to mitigate this, the EC considered it was necessary to lay down a uniform legal framework for essential cybersecurity requirements since the targeted products showed a low level of cybersecurity and lacked the availability of information regarding its cybersecurity properties. Consequently, this prevented users from choosing products that have a better security posture or from using products in a more secure manner. In order to improve this scenario, this regulation lays down requirements for ensuring the cybersecurity of digital products such as in the stages of design, development and production and vulnerability handling, with the ultimate goal of exercising due diligence, enhancing transparency to customers, ensuring security support via updates in a proportionate way, and overall improving the security of a product throughout its lifecycle. With this regulation, the number of cyber incidents, incident handling costs and reputational damage would be reduced. For the whole EU, it is estimated that it could reduce the costs of incidents affecting companies by roughly EUR 180 to 290 billion annually.

Expanding on the vulnerability handling, manufacturers are expected to put in place vulnerability disclosure policies that incentivize reporting vulnerabilities by ensuring that individuals or entities receive recognition and a compensation for their efforts. Additionally, manufacturers should also report to the European Union Agency for Cybersecurity (ENISA) any incident having an impact on the security of their product. In order to help the customer identifying products that are in conformity with this regulation, a visible CE marking will be displayed on them.

2.2.2 IoT Security Assurance Framework

The IoT Security Foundation (IoTSF) was established to address the challenges of IoT security in an increasingly connected world. Their mission is to "Build Secure, Buy Secure, Be Secure" and to do so, they have developed the IoT Security Assurance Framework. This framework provides a comprehensive set of guidelines and best prac-

tices for securing IoT devices and highlights key requirements and the respective actions that are required to achieve such goals (e.g., management governance, engineered for security, fit for purpose cryptography, secure network framework and applications).

This framework is intended for managers, who will gain a thorough overview of the management process required to adopt best practices; developers, engineers, logistics, and manufacturing staff, who will find it useful in project reviews and daily work; and supply chain managers, who will benefit from a framework that can be used to guide the auditing of security practices.

Additionally, this framework produces an assurance questionnaire that may be used at various stages in the product lifecycle. First, by identifying the necessity for security at the concept stage; next, by enumerating the evidence that has been acquired; and last, by approving the security requirements for production release. For example, it provides a table with the requirements, and the respective required assessment method, evidence type, evidence and who is responsible.

2.2.3 Cyber Attacks in IoT

The challenges faced by IoT devices naturally become opportunities for threat actors, as balancing resource constraints and security proves to be a difficult task. One such challenge is the extraction of data from IoT environments in order to produce evidence admissible in a court of law. The challenge arises from the need to collect and manage substantial amounts of empirical data, sourced from a multitude of IoT devices. Not only do these devices often produce data in vendor-specific formats, but they also have constrained computing resources, combined with their cloud-based infrastructure (i.e., cloud forensics poses significant challenges to digital forensics due to lack of international collaboration, combined with the legal and jurisdictional issues), further complicates the storage of data on these devices for forensic purposes (Reedy 2023).

In the past decade, the emergence of IoT botnets exemplified the consequences of this delicate balance. During this period, botnets comprised of IoT devices were responsible for some of the largest distributed denial of service (DDoS) attacks ever witnessed. To execute a denial of service (DoS) attack, one must overwhelm the target with information, and while traditionally this has been performed by having a more powerful machine, IoTs have their strength in numbers. Although these devices possess less computational power, their lack of security allowed for the infection of millions of devices, leading to an exceptionally rapid increase in the volume of requests during a DoS attack.

Mirai, one of the most widely known IoT malwares, was initially discovered in August 2016 and primarily exploited known weak telnet credentials, as strengthening credentials could have easily prevented infection (Affinito et al. 2023). This malware did not establish persistence, making a simple reboot effective in removing it. Mirai was a self-propagating worm that infected and consequently handed the control of the infected IoT device to a command and control (C&C or C2) server. Because its source code was made public, many of the botnets that followed were variants of Mirai, such as Okiru, Satori, Masuta, PureMasuta, and many more (Victor et al. 2023). Unlike Mirai, and instead of exploiting weak credentials, IoTReaper/IoTroop targeted devices vulnerable

to disclosed vulnerabilities. BrickerBot followed a distinctive approach which instead of focusing on infecting and controlling targets, it sought a permanent denial of service (PDoS). Essentially, its goal was to irreversibly disable ("brick") insecure IoT devices.

2.3. Defensive Mechanisms

This chapter presents a couple of countermeasures to prevent cyber attacks, namely "Penetration Testing" (Section 2.3.1) and "Threat Modeling" (Section 2.3.2). Both are proactive approaches that attempt to prevent crime: the former by finding the vulnerabilities before malicious actors take action, and the latter by identifying and analysing threats to an asset, therefore contributing to its risk management.

2.3.1 Penetration Testing

Over the past decade, organizations have come to the realization that becoming compromised is not a matter of *if* but rather *when*. With this, many organizations have embraced a more proactive approach to enhance their security posture, and this shift is evident in the adoption of practices such as security audits, vulnerability assessments, penetration tests, and bug bounty programs. With these initiatives, the perception of finding a vulnerability in a product has gradually evolved from "the organization neglected security" to "the organization is actively working to enhance its security". This change reflects the acknowledgment that cybersecurity measures are essential and hard to implement. Furthermore, it acknowledges that organizations are not merely passive victims but are actively engaging in security measures. The transition from a blame-oriented mindset to a collaborative one has surely played a role in the overcoming of the "security by obscurity" ideology that organizations may be tempted to employ.

The key difference between a penetration tester and a cyber criminal lies in the legality of actions. Although there are many other actions that penetration testers would never be asked to conduct (e.g., performing ransomware attacks, extortion), or that would rarely be asked to conduct (e.g., data exfiltration in order to test a data loss prevention system, phishing and social engineering in order to test the employees' awareness and susceptibility to such attacks), there are many similar steps that cyber criminals and penetration testers alike must follow in order to compromise a target. One of the most popular frameworks used to identify the necessary steps for adversaries to achieve their objective is the Cyber Kill Chain (CKC), developed by Lockheed Martin (Lockheed Martin 2024). By identifying these steps, the CKC can pinpoint the current stage of a threat actor and determine the next stage. In other words, through the use of the CKC, it becomes feasible to predict the next stage of the attack and attempt to thwart it preemptively. The CKC comprises of seven steps, namely:

1. **Reconnaissance:** information about the target is gathered;
2. **Weaponization:** an vulnerability is discovered and the corresponding exploit is developed;
3. **Delivery:** the weaponized bundle is delivered to the target;

4. **Exploitation:** the target's vulnerability is exploited and the payload executes;
5. **Installation:** the payload installs malware in order to establish additional capabilities (e.g., persistence);
6. **Command & Control (C2):** the malware creates a channel that enable remote control of the target;
7. **Actions on Objectives:** the threat actors accomplish their initial goals.

Although CKC was developed to identify Advanced Persistent Threats (APTs), it can be contextualized to smart bulbs and to penetration testing, as it details similar steps describing a threat actor that aims to control smart bulbs. Every attack starts with reconnaissance, where information about the target is gathered by collecting different types of relevant information (e.g., historical data, encryption, protocols and specific hardware used). Naturally, purchasing and testing the target device eases this step. Then, a vulnerability would be discovered and an exploit tailored to that vulnerability would be crafted. Vulnerabilities come in many forms (e.g., exposure of sensitive information, remote code execution) and therefore how the attack is perpetrated onwards varies widely depending on the vulnerability that was found. Assuming the worst (i.e., remote code execution), the victim would receive the weaponized bundle and execute the payload in it. Unlike cyber criminals and their use of botnets, it is uncommon for a penetration tester to establish a C2 system that intends to infect more targets. Usually, during a penetration test for a particular system, the penetration testers halt their operations when they exploit a specific vulnerability. They document their findings, try to chain with other vulnerabilities or continue to search for different ones, unless they were instructed otherwise in their penetration test agreement.

While this framework details the steps taken by an adversary, it is also useful to expand on the second step, weaponization, in order to understand what is usually targeted and fortify the respective defence mechanisms. Although it is not its initial intent, the Open Worldwide Application Security Project (OWASP) created a "Top 10" related to the things to avoid when building, deploying, or managing IoT systems (OWASP 2018), which can complement the aforementioned. The first version was released in 2014 and the latest version in 2018 , which includes: "Weak, Guessable, or Hardcoded Passwords", "Insecure Network Services", "Insecure Ecosystem Interfaces", "Lack of Secure Update Mechanism", "Use of Insecure or Outdated Components", "Insufficient Privacy Protection", "Insecure Data Transfer and Storage", "Lack of Device Management", "Insecure Default Settings" and "Lack of Physical Hardening". This list aims to help manufacturers and consumers alike to better understand the security issues associated with IoT. Unfortunately, preventing these issues is more complicated than it may initially appear, as they may be hidden in the complexity of the IoT environments.

Another perspective to evaluate the security of smart bulbs is to take a historical approach and analyze the respective CVEs and scores. CVE stands for "Common Vulnerabilities and Exposures" and it is a system that catalogs known vulnerabilities. For each vulnerability, an identifier (ID), a score, and description are assigned. The score ranges from 0 to 10 (lowest to highest) depending on the severity of the vulnerability, which is calculated using the Common Vulnerability Scoring System (CVSS). In order

to assess the severity accurately, several base metrics are taken into consideration such as, for example, the "Attack Vector" (AV) that is determined based on the type of access the attacker needs ("Network", "Adjacent", "Local" or "Physical"). By querying two popular CVE databases, namely MITRE (MITRE 2024) and NVD (NIST 2024b), with the search terms of "smart bulb", "smart light" and "smart lamp" the Table 1 was constructed.

The following CVEs were removed from this table due to not fitting the context:

- CVE-2012-5878 and CVE-2012-5693∼97: related to Bulb Security Smartphone Pentest Framework (SPF). It was a match due to the name of the organization that developed the SPF (Bulb Security);
- CVE-2016-0863∼66: related to Tollgrade SmartGrid LightHouse Sensor Management System. This system is part of smart grid infrastructure and it may indirectly impact devices such as smart bulbs that rely on the underlying smart grid technology, but it does not impact smart bulbs directly.

The CVE IDs have the following format: CVE-YEAR-ID. The CVE IDs in Table 1 were ordered based on their year, and then on their ID, on a descending order. It is important to highlight that a higher ID does not necessarily imply the vulnerability being more recent, since assigning an ID to a CVE has many factors, such as when it was discovered, reported, and officially assigned a CVE ID. There are a total of 10 CVEs and the average CVSS score is 7,06. Although this score is considered "high", it is very close to the threshold between "medium" and "high". It is also important to highlight that despite different CVE IDs being assigned, some vulnerabilities are related, such as CVE-2023-38906∼38909. Lastly, it is also crucial to understand that Table 1 does not contain every vulnerability that targets smart bulbs, as some vulnerabilities may lack the search terms that were queried in their details. For example, a vulnerability that primarily targets Zigbee may also be used to target any other device that uses that specific communication protocol. In these cases, it is simply not feasible to explicitly state every device that is affected.

CVE-ID	CVSS	Description	Affected Device(s)
CVE-2023-42189	7,5	Insecure permissions allow a remote attacker to cause DoS via crafted script to KeySetRemove function.	Matter SDK, Nanoleaf Light strip v.3.5.10, Govee LED Strip v.3.00.42, switchBot Hub2 v.1.0-0.8, Phillips hue hub v.1.59.1959097030, Yeelight smart lamp v.1.12.69.
CVE-2023-38909	6,5	Exploit retrieves sensitive information via AES128-CBC IV component.	TPLink Smart bulb Tapo series L530 v.1.0.0, Tapo Application v.2.8.14.
CVE-2023-38908	6,5	Exploit retrieves sensitive information via TSKEP authentication.	TPLink Smart bulb Tapo series L530 v.1.0.0, Tapo Application v.2.8.14.
CVE-2023-38907	7,5	Exploit retrieves sensitive information via session key in message function.	TPLink Smart bulb Tapo series L530 v.1.0.0, Tapo Application v.2.8.14.
CVE-2023-38906	6,5	Exploit acquires sensitive data through UDP message authentication code.	TPLink Smart bulb Tapo series L530 v.1.0.0, Tapo Application v.2.8.14.
CVE-2022-47100	7,5	Arbitrary factory reset via crafted IEEE 802.15.4 frame.	Sengled Smart Bulb 0x0000024.
CVE-2022-39065	6,5	Malformed Zigbee frame disrupts TRÅDFRI gateway, affecting IKEA Home Smart app and TRÅDFRI remote control.	TRÅDFRI Gateway, Connected Lighting.
CVE-2022-39064	8,1	Triggers factory reset on TRÅDFRI bulb via malformed Zigbee frame, causing loss of configuration.	IKEA TRÅDFRI.
CVE-2019-18980	7,5	Unprotected API allows remote control without authentication. Attacker can manipulate bulb settings.	Philips Taolight Smart Wi-Fi Wiz Connected LED Bulb 9290022656.
CVE-2017-18642	6,5	RGB parameters transmitted over clear-text BLE, exposing vulnerabilities to sniffing and attacks.	Syska Smart Bulb.

Table 1: CVEs regarding smart bulbs

2.3.2 Threat Modeling

Threat modeling is an iterative process that should be performed early in the product's lifecycle. Ideally, threat modeling should not integrate into the system's lifecycle as an add-on, but as a regular process instead. Additionally, similarly to a system, a threat model should also be maintained, updated, and refined (OWASP 2024).

While a data flow diagram (DFD) models a system and its interactions with data or other entities (e.g., the control commands flow from the user interface to the smart bulb, instructing it to turn on/off, adjust brightness, color), STRIDE aims to identify and analyze threats in a system (Microsoft 2022). STRIDE is a framework developed by Microsoft and its name is derived from a mnemonic of each of its threat categories, namely:

- **Spoofing:** consists of illegally accessing and then using another user's authentication information (e.g., username and password), breaching authenticity;
- **Tampering:** entails the malicious modification of data (e.g., unauthorized changes made to persistent data, and the alteration of data as it flows between two computers over an open network), undermining integrity;
- **Repudiation:** is associated with users being able to deny performing an action without other parties having any way to prove otherwise (e.g., the system lacks the ability to trace operations back to the entity that has performed them), violating non-repudiation;
- **Information disclosure:** encompasses the exposure of information to entities that are not supposed to have access to it (e.g., the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers), infringing confidentiality;
- **Denial of service:** is associated with attacks that deny service to valid users (e.g., making a Web server temporarily unavailable or unusable), compromising availability;
- **Elevation of privilege:** occurs when an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system, contravening authorization.

2.4. Research background

When using the academic literature to review the penetration testing of smart bulbs, some of the aforementioned issues resurface in different vulnerabilities, with one such example being Zigbee Light Link (ZLL). ZLL is a network standard used by lighting systems which uses two methods to add a device to the network: regular commissioning or touchlink commissioning. When using touchlink commissioning, a ZLL master key is used to encrypt the network key that is sent to the joining device (Morgner, Mattejat, and Benenson 2016). More specifically, a joining device needs to know the network key to communicate with the rest of the network safely (i.e., use encryption) and, in order to avoid sending this key in plaintext, the ZLL master key encrypts it. Despite the ZLL

master key being solely distributed to certified manufacturers, it was leaked in 2015. The implications of such are that an attacker can decrypt the network key during its transmission, and consequently send arbitrary commands to the devices. Regarding the OWASP Top 10 for IoT, this vulnerability falls under "Weak, Guessable, or Hardcoded Passwords" due to the ZLL master key being hardcoded into every device. Since then, Zigbee 3.0 was announced to replace ZLL while providing backwards compatibility.

Another example can be found in a study conducted to assess the security of Tapo L530E by TP-Link where four vulnerabilities were discovered (Bonaventura, Esposito, and Bella 2023), two of them being classified as "High". Out of those two, the first was named "Lack of authentication of the smart bulb with the Tapo app" (falls under "Insecure Ecosystem Interfaces") given that the app did not require any guarantee about the identity of its peer, and therefore being susceptible to spoofing where anyone can pretend to be the smart bulb. The latter was named "Hard-coded, short shared secret" (falls under "Weak, Guessable, or Hardcoded Passwords") given that the app allows an attacker to obtain the secret used for authentication during the "Bulb Discovery" phase.

In another example, Toutsop, Das, and Kornegay (2021) studied DoS attacks and how to detect them. The authors claim "hackers" might exploit sensor vulnerabilities to gain unauthorized network access. One of the shown DoS attacks was the "Wi-Fi deauthentication attack" (in this context, "deauthentication" and "disassociation" are synonyms), which consists of sending deauthentication frames to the victim, given that these frames do not require encryption nor authentication. A deauthentication frame is essentially a request sent to the access point for disconnection (e.g., if the device is experiencing connectivity issues and decides to reconnect to the network). By simply eavesdropping Wi-Fi traffic the attacker can discover the MAC address of the victim and spoof a deauthentication frame. This will cause the victim to lose connection effectively causing a denial of service.

Furthermore, a technical paper demonstrated the security vulnerabilities in Philips Hue, with one of such vulnerabilities being present in the way the iOS app authenticated to the bridge (Dhanjani 2013). The author developed a malware script that caused the smart bulb to suffer a "sustained blackout". The ability to control the bulb was facilitated by utilizing a whitelist token that was not randomly generated, but derived from the MD5 hash of the owner's MAC address instead. This implied that knowing the MAC address of the assigned owner was enough to control the smart bulb. By calculating and consecutively trying the MD5 hash of every MAC address nearby, the attacker would eventually guess the owner's MAC address, and given that there was no way to unregister a whitelisted token, the access was permanent. With this access, the attacker was able to control the smart bulb, and the sustained blackout was simply a "turn off" command sent to the bridge's API endpoint every half second.

No frameworks specifically concerned with the security of home-based smart bulbs were found. However, there are several frameworks regarding the overall security of consumer IoT devices. Naturally, due to the first domain being a subset of the latter, the latter is still of relevance to this thesis. Akhilesh et al. (2022) developed an automated penetration testing framework with the aim of discovering the 5 most common vulnerabilities that target smart home-based IoT devices. To test their framework,

the authors selected 5 IoT devices for testing, 2 of them being smart bulbs, namely a TP-Link and a LIFX. While the testbed identified the vulnerabilities of "Lack of Transport Encryption" and "Insecure Firmware" in the first smart bulb, it couldn't find any vulnerabilities on the latter. Although the authors acknowledge several limitations regarding the limited number of vulnerabilities and its narrowed scope, I consider the way the authors evaluated each device to not represent the scenario accurately. The authors added the CVSS score of each vulnerability, and associated the final sum with the device being evaluated. However, I believe that a device that has 2 vulnerabilities with the CVSS score of 5.0 has a better security posture than a device that has a single vulnerability with score of 10.0, since the first two vulnerabilities would be classified as "medium" and the latter as "critical".

Ammar, Russello, and Crispo (2018) compare 8 IoT frameworks implemented by different vendors, namely Amazon Web Services IoT (Amazon), ARM Mbed (ARM), Azure IoT Suite (Microsoft), Brillo/Weave (Google), Calvin (Ericsson), HomeKit (Apple), Kura (Eclipse), and SmartThings (Samsung), regarding how each approached security implementations, encompassing the architecture, the third-party smart apps, the compatible hardware, and the security features. The authors claim that there is a gap between the frameworks in terms of compatibility at the hardware level, usually due to specific requirements and dependencies of the other components. The authors also claim that despite this issue being present at the security level, the vendors follow the same trend and enforce the same security standards in some aspects. This article essentially sheds light to the problems with implementation vulnerabilities, since the frameworks share the same "design philosophy" in terms of having a centralized cloud environment, while following different approaches on how to apply it.

Regarding threat modeling, Casola et al. (2019) propose an "almost completely automated process" for threat modeling and risk assessment of an IoT system. To achieve this, the authors designed an ISO-compliant process that extends the IoT Multi-cloud Application Composition Model (IoT MACM) formalism. The identified threats were classified based on the asset they applied to (e.g., gateway, end device), associated with the respective STRIDE category, and with the CIA property they compromised. Then, countermeasures from the NIST Security Control Framework (Force and Initiative 2013) were listed.

Additionally, Rizvi et al. (2020) developed a threat model for securing IoT networks at device-level. The need for the device-level threat analysis was based on the authors' claim that it is a requirement to develop a security scheme that adequately protects a network, while also acknowledging that a device-level analysis can be laborious due to the overwhelming number of devices. The authors designed 3 scenarios, namely healthcare, commerce, and home, and highlighted the primary vulnerabilities, proposed tailored vulnerability scores, detailed threat environments, and recommended security controls, for each scenario.

Dalvi, Maddala, and Suvarna (2018) authored an article that shares similar objectives with this thesis, but takes a different approach by designing three attack trees targeting an IKEA Trådfri bulb, each depicting a different scenario, namely regarding packet spoofing, data modification, and a DoS attack. While the authors' approach shares similar goals, it also had several limitations, such as oversimplified steps and a

lack of depth. Nevertheless, due to its resemblance, this article was included in this thesis.

Regarding analysing an IoT device by its layers, Mira and Alsmadi (2019) evaluate the respective IoT attacks and security vulnerabilities. Due to its wide coverage, it grasped the surface of each category (e.g., network layer) by succinctly describing each subcategory (e.g., DoS, malicious code injection), while providing high-level general countermeasures.

In essence, this chapter provides insights into what has been researched within the academic community. This research ranges from attacks exploiting implementation flaws, hard-coded secrets, or the availability of smart bulbs. Additionally, IoT frameworks and surveys were analyzed, although no frameworks specifically concerned with the security of home-based smart bulbs were found, which is the gap this thesis aims to close. Furthermore, research regarding threat modeling of smart bulbs was gathered and studied. Lastly, a security layer analysis research article was considered. This thesis integrates insights from these areas of research, as it builds its framework upon their contributions.

3. Methodology

This chapter demonstrates the methodology followed in order to perform the research. It starts by presenting and introducing the chosen research design and consequently providing a brief introduction of how it is applied to the study. After that, how the data was gathered and the step-by-step procedures followed during this process are detailed. Consecutively, how the data is analyzed and interpreted, leading to the development of key findings is detailed. In order to validate such findings, the metrics used to evaluate these steps, in terms of validity and reliability, are discussed. Lastly, the chosen approach to threat modeling is justified.

3.1. Design Science Research

There are two complementary paradigms regarding how to acquire knowledge that concerns management of information technology, namely behavioral science and design science. While the first seeks to justify theories that explain or predict phenomena, the latter seeks to solve problems through ideas, practices and technical capabilities (Hevner et al. 2004). Given that this thesis aims to develop a customized framework for smart bulbs targeted towards the research community, design science was considered the most suitable paradigm to follow. With this, a design science research (DSR) approach based on the "Information System Research Framework" (ibid.) was chosen.

Design science research involves the design and the development of an artifact, and revolves around addressing two fundamental questions: "What purpose does the new artifact serve?" and "How can we demonstrate the utility it provides?". The core of this approach lies in presenting strong evidence to address these questions. In order to follow this framework, three domains must be identified: the environment, the Information Systems (IS) research, and the knowledge base. The environment defines the problem space, which refers to the people (e.g., their roles, capabilities, characteristics), the organizations (e.g., their strategies, culture, processes) and to the technology (e.g., infrastructure, applications, development capabilities). In essence, it contains the goals, problems, and opportunities that define business needs as they are understood by those working for the company. The knowledge base provides the tools from which the IS research is conducted, and is complemented by the artifact that is being produced. It is composed of foundations (e.g., theories, frameworks, models) and methodologies (e.g., data analysis techniques, validation criteria). Lastly, the IS research is concerned with the development of theories and artifacts that originate from business needs, while adding content to the knowledge base for further research and practice. These theories and artifacts assess, and simultaneously are refined by, case studies, simulations and similar experiments (ibid.). In order to build an artifact that respects the DSR methodology, Hevner et al. (ibid.) lay down a set of guidelines so that the artifact has certain properties, such as being viable in its form of construct, providing clear and verifiable contributions, or being presented effectively. This thesis relates to IS Research by making a contribution to the research community's body of

knowledge, by providing a framework that identifies threats, highlights challenges, and states requirements, regarding the security of smart bulbs, while following the DSR methodology.

3.2. Data Collection

This work aims to create a threat model in order to assess and improve a smart bulb's security posture beyond the mere examination of the device itself, by recognizing the versatile vulnerabilities and inherent complexities of its broaden attack surface. As in any study, the data collection process is paramount not only regarding its reliability but also regarding its reproducibility, with the latter being one of the foundational pillars of research. In order to build a solid knowledge foundation, sources that contain relevant information respective to the security of smart bulbs were taken into consideration, such as existing frameworks, case studies and known vulnerabilities (CVEs). Regarding the data gathering methods, relevant scientific articles will be meticulously collected from diverse sources, including the university's library database and reputable scientific platforms such as ACM, Science Direct, Springer, IEEE Xplore, ResearchGate, and Google Scholar.

In order to find the relevant articles, keywords such as "IoT security" and "smart bulb security" were used, along with backward snowballing, which refers to the practice of parsing and following the references of the article being analyzed in an attempt to find additional relevant work. While there is not much research regarding smart bulb security specifically, IoT security has been researched extensively. Given that the latter is an expansive topic that yields excessive results, the "relevance" metric of databases was leveraged to accelerate the data collection process. Although specifics may differ across databases, the "relevance" metric typically has several factors, such as "term frequency" (indicating how many times the search term appears in asset fields) or "inverse document frequency" (the number of assets containing the search term; the higher the count, the lower the term's importance). With this, the articles were organized based on the "relevance" metric offered by the database system. If the search yielded an excessive number of results, the search process was halted when several consecutive articles were found to be outside of the thesis' scope.

In order for an article to be included, it generally has to be peer reviewed, published in journals or conferences, be written in English, published between 2014 and 2024, and be relevant to the topic. There are some exceptions to the rule, especially given that the cybersecurity community produces a significant amount of relevant content that is not academically published. Exclusion criteria encompassed articles that failed to meet the inclusion criteria, that were inaccessible due to being behind a paywall, that were duplicates of other articles or lacked relevance. To assess if an article was relevant, different sections were analyzed, namely title, abstract, introduction and conclusion, and the full article. If an article failed to meet the relevance criteria in one of these sections, progression to the next section was halted, signaling that the article was likely outside the intended scope.

Additionally, the word "bulb" was replaced by "light" and "lamp" as they are often synonyms in this context. Furthermore, keywords respective to their section

were appended to the search term, such as "threat model" for Chapter 4 and "zigbee" for Section 2.1.4, to enhance the search's specificity.

3.3. Data Analysis

In order to analyse the collected data, (Hevner et al. 2004) provide "Design Evaluation Methods" from which "informed argument" and "scenarios" were selected. These methods belong to the "descriptive" category, which was chosen given the time and resource constraints of this work. The informed argument method consists on leveraging research and relevant information to construct a compelling case for the artifact's usefulness, which is achieved by building the artifact upon relevant literature and addressing the identified research gap. The scenarios method consists on constructing detailed scenarios around the artifact to demonstrate its utility, which is achieved by collecting, analysing, and evaluating events to illustrate how the framework could have helped protect the smart bulbs.

3.4. Threat Modeling

Although there are numerous techniques for threat modeling, this thesis introduces a distinctive approach by combining existing methods to offer a more comprehensive understanding of the threat landscape. Popular techniques such as DREAD, PASTA and TARA were excluded due to being risk-centric, given that the risk is the product of probability and impact, which are components that are dependent of the environment that encompasses the object being analyzed, which is out of scope for this thesis. Attack trees were excluded due to being used for specific scenarios which goes against the objective of this work of being comprehensive. Due to data flow diagrams (DFDs) being "arguably the most common approach" (OWASP 2024), they were selected to illustrate the presented threat model. Additionally, STRIDE is used in order to help identify and analyze threats due to its popularity and suitability.

4. Threat modeling

This chapter contains a tailored threat model towards smart bulbs that intends to guide the development of countermeasures. The first step in threat modeling is to understand the system in order to understand what threats are most applicable to it (OWASP 2024). Although smart bulbs can use several communication protocols, the most prevalent is Wi-Fi, despite some using Zigbee (usually in cases where power efficiency and scalability are important factors). Figure 1 depicts a scenario in which "Smart bulb 1" represents a smart bulb connected to the network via Wi-Fi, while "Smart bulb 2" is connected via Zigbee. In this scenario, the user controls both smart bulbs "indirectly" through a mobile application. That is, the cloud server acts as a middleman between the mobile application and the smart bulbs and for every request or response, to or from them. It is important to note that, depending on the smart bulb, this is not always the case. In some instances, the cloud is used for initial setup, firmware updates, and features such as integration with voice assistants. Smart bulbs can perform basic operations (e.g., turning on/off, adjusting colour and brightness) without Internet, using protocols such as Zigbee or Z-Wave and communicating with a local hub, Bluetooth by pairing directly with the smart bulb, or via infrared or radio frequency commanded by a remote control. As mentioned in Section 1.3, this thesis focuses on the most popular controller, the mobile application.

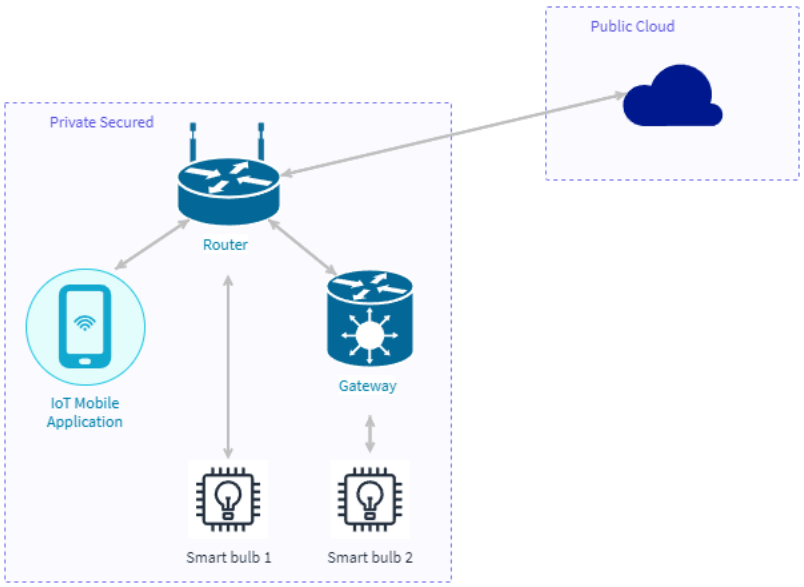

Figure 1: Network topology of a home network with smart bulbs

Figure 1 depicts a common network topology regarding smart bulbs in a home environment. Based on Figure 1, a data flow diagram was developed, which is displayed in Figure 2.

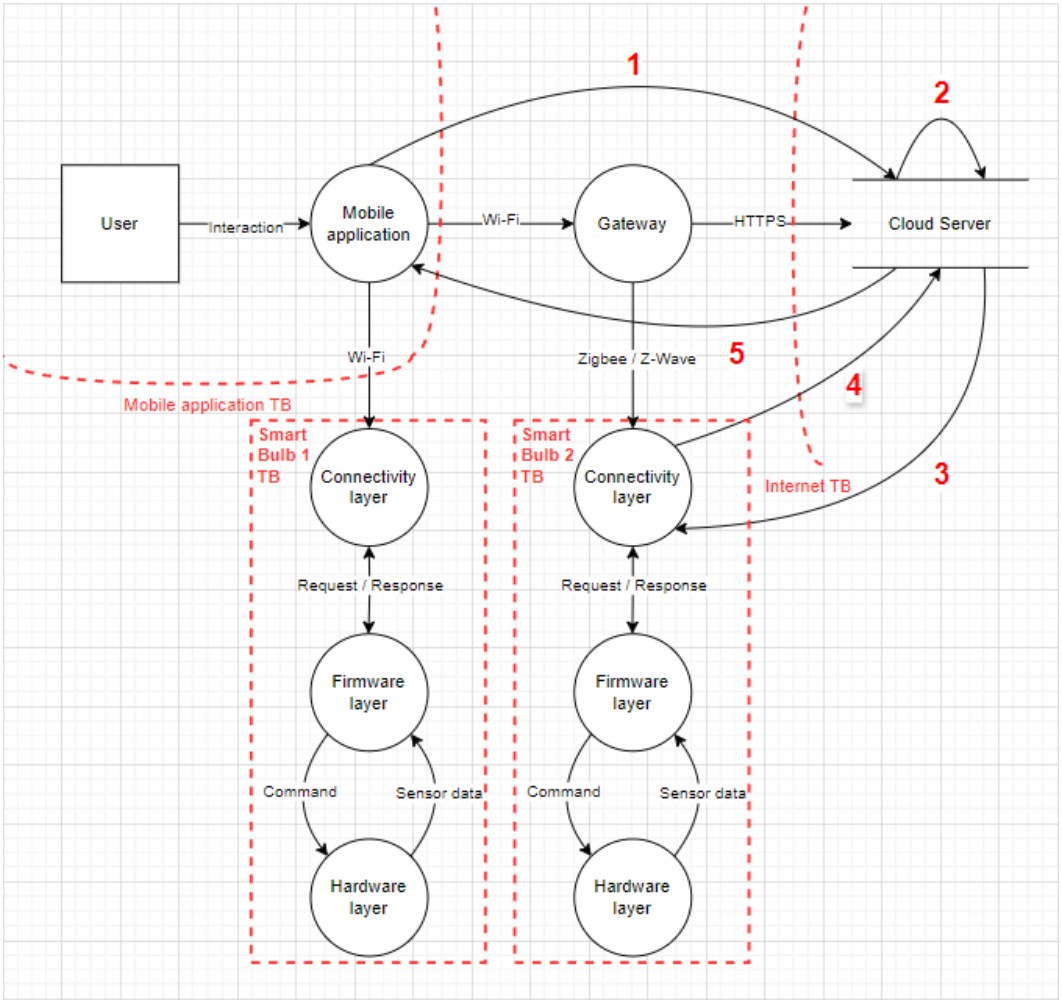

Figure 2: Data flow diagram of a home network with smart bulbs

In Figure 2, the term "Gateway" serves as an abstraction denoting the device facilitating communication with the mobile application or smart bulb. In the former scenario, it denotes the router, acting as the gateway for the mobile application. In the latter, it indicates the hub, serving as the gateway for Zigbee and Z-Wave-operated smart bulbs.

An example of a sequence of data traffic, which steps are numbered in Figure 2, could look like the following:

1. **Mobile application sends a command to the cloud**
   The mobile app encapsulates the command and sends it over the internet to the designated cloud service endpoint over HTTPS (Hypertext Transfer Protocol Secure).

2. **Cloud service processes the command**
   The cloud service verifies the user's authorization, interprets the command, and if the request passes all checks, the cloud service prepares it for transmission to the smart bulb.

3. **Cloud service sends the command to the smart bulb**

This transmission can occur using various communication protocols, depending on the specific implementation.

4. **Smart bulb executes the command and sends status update to cloud**
   After executing the command, the smart bulb sends a status update to the cloud service. This update is sent via the designated communication protocol.

5. **Cloud service forwards status update to mobile application**
   When the cloud service is notified of the smart bulb's new state, it processes that data and sends the status update to the mobile application. This update is sent over the Internet to the mobile application's endpoint. The mobile app receives the status update and updates its user interface accordingly.

By applying STRIDE to this macro perspective data flow, a few potential attacks of threats that can be identified. These attacks are detailed in Table 2.

Threat	**Potential attack**
Spoofing	Taking the identity of the smartphone app to control the smart bulb.
Tampering	Intercepting and modifying communication between the smartphone app and the cloud service.
Repudiation	Absence of proper logging and auditing, making it impossible to identify the source of security breaches.
Information Disclosure	Lack of proper encryption in communication between the smartphone app and the cloud service, leading to disclosure of sensitive information.
Denial of Service	Flooding the cloud service with requests, rendering it unresponsive and preventing legitimate users from controlling the smart bulb.
Elevation of Privilege	Exploiting vulnerabilities in the smart bulb's firmware to gain unauthorized access and execute commands.

Table 2: STRIDE applied to the macro perspective

The threats outlined in Table 2 grasp the surface of smart bulb attacks and do not represent the whole landscape. This chapter conducts a similar analysis, delving deeper into the various layers of the smart bulb. These layers were tailored to the specific ecosystem of the smart bulb, by basing them on existing research and industry practices. In order to draw the boundaries between the layers, the overall behaviour of the smart bulb was analyzed and layers were subsequently assigned based on their function and importance. In order to contextualise this study to the smart bulb's environment, and due to its popularity, the 3-layer architecture (Perception, Network, Application) was expanded. Due to its importance and the unique challenges it faces, the firmware layer was extracted from the perception layer. Additionally, given the scenario in Figure 1, the cloud layer was extracted from the application layer due to its unique nature. Not only does it act as a middleman between the smart bulb and the mobile application, but it is also owned by a third-party. With this, a 5-layer architecture was formulated with the following layers: "Hardware", "Firmware", "Connectivity", "Application", and "Cloud".

The hardware layer consists of the physical components of the smart bulb, and it is a subset of the perception layer when contrasting with the 3-layer architecture. This layer controls the bulb's actions through actuators that receive commands from the firmware, while providing real world data through its sensors in return. The firmware layer consists of the low-level code that controls the hardware, and it is also a subset of the perception layer in the 3-layer architecture. This layer receives commands from the cloud layer through the connectivity layer. The connectivity layer is concerned with the communication between the smart bulb and the other entity. It is the equivalent of the network layer in the 3-layer architecture. It encompasses the communication protocols used and how they are implemented. This layer serves as a medium to connect the mobile application and the cloud layer to the smart bulb. The application layer is concerned with the security of the mobile application that issues commands to the smart bulb. The cloud layer acts as a middleman between the mobile application and the smart bulb.

4.1. Hardware layer

The hardware layer is the first layer of the smart bulb. It contains the smart bulb's physical components and it communicates with the firmware layer. This layer has two primary functions: to execute the commands sent by the firmware, and to provide data that is collected from the sensors. As mentioned in Section 2.1.1, the key components of a smart bulb are LEDs, or other forms of light emitters, a connectivity module, a power supply module, integrated circuits and a heatsink. Given the nature of this layer, the attacks conducted usually require physical access to the smart bulb. A non-comprehensive list of attacks that target this layer includes physical tampering, side-channel, micro-probing, fault injection, power attacks, hardware trojans, supply chain attacks, electromagnetic interference, and reverse engineering.

A common way an attacker attempts to gain access to an IoT device is by trying to connect to an administration physical port. With this in mind, manufacturers must secure this access by using robust authentication mechanisms (e.g., SSH over Telnet) (IoTSF 2019b). Other strong preventive measures include disabling unnecessary physical ports, pins, and circuit tracks, thus reducing the attack surface; epoxying chips that manage critical functions, so that if an attacker attempts to tamper one, the chip gets destroyed in the process of removal; and lastly, the entire system can be submerged in a block of resin, hindering its accessibility to all but the most determined (ibid.). While preventive measures aim to prevent threat actors from conducting their attacks, detective measures aim to detect whether an attack happened. An example of a detective measure could involve using a physical casing that exhibits damage when tampered with (i.e., when it is opened). Table 3 contains a potential attack for each STRIDE threat and the respective countermeasure at the hardware layer.

Threat	**Potential Attack**	**Countermeasure**
Spoofing	Spoofing the MAC address by identifying and modifying it within the EEPROM chip.	Leverage the security of trusted platform modules (TPMs) to encrypt EEPROM data.
Tampering	Opening the casing and modifying internal circuits in order to insert rogue devices, trojans, or backdoors.	Design the smart bulb with tamper-resistant physical features.
Repudiation	Lacking proper logging mechanisms, events and actions performed by the smart bulb's hardware components can not be reliably recorded.	Implement hardware-level logging mechanisms to record critical events and interactions.
Information Disclosure	Storing or processing sensitive information, such as encryption keys or configuration data, that can be exposed to unauthorized access.	Employ hardware-level encryption and secure storage mechanisms to protect sensitive information.
Denial of Service	Overloading the power supply module, using an electromagnetic pulse to damage the circuitry, or by simply physically damaging the smart bulb.	Design the smart bulb with resilient hardware components and redundancy measures to mitigate the impact of DoS attacks.
Elevation of Privilege	Exploiting a vulnerability in the microcontroller that allows overwriting the device's firmware.	Regularly update the firmware and implementing security measures such as secure boot or firmware validation.

Table 3: STRIDE applied to the Hardware layer

Table 3 shows potential attacks of how STRIDE can identify threats at the hardware layer. In this table, several examples of threats are highlighted with their respective countermeasures. In this layer, data at rest in non-volatile memory is a common target since it is usually unencrypted in Electrically Erasable Programmable Read-Only Memory (EEPROM) chips. If this is the case, combined with physical access to the smart bulb, a threat actor could extract sensitive information, such as the Wi-Fi password or the MAC address. With the first, the attackers can infiltrate the network and, with the latter, the attackers can spoof the MAC address, bypassing potential network security features such as MAC filters. Regarding the tampering threat, the usage of Secure Elements (SE), or a device that is capable of providing a layer of security at the hardware level, is recommended. Secure elements refer to tamper-resistant processor chips or secure components. However, Jaouhari and Bouvet (2022) claim that this is not implemented in most IoT devices due to the increase in financial costs and resource requirements, and thus smart bulbs are no exception. Additionally, IoTSF (2019a) recommend using a "hardware-based tamper-resistant capability" to store crucial data items (e.g., cryptographic keys) required for the boot process. Again, due to the cost constraint, smart bulbs usually have no physical logging, let alone redundancy components, and therefore lack non-repudiation and are prone to DoS, respectively. The elevation of privileges threat is usually associated with higher level code (e.g., misconfigurations in firmware, applications).

Overall, the security of this layer depends heavily on its implementation, and thereby its manufacturer, as the consumer usually has little to no effect over it. Therefore, the main requirements to secure this layer are to:

HW1 Disable all unnecessary ports (e.g., debugging, unused communication, and configuration ports);

HW2 Design the bulb's casing with tamper-resistant features (e.g., tamper-evident seals);

HW3 Epoxy chips that execute critical functions (e.g., microcontroller, integrated circuits that store critical information such as cryptographic keys or configuration data);

HW4 Encrypt sensitive data at rest (e.g., network key, user credentials).

4.2. Firmware layer

The firmware layer lies between the hardware layer and the connectivity layer, and it is concerned with the low-level software code that controls the hardware of the smart bulb. Exploits regarding this layer usually stem from implementation flaws or outdated firmware versions. Examples of the first can be found, for example, when the hardcoded global ZLL master key was leaked (Morgner, Mattejat, and Benenson 2016), or when the usage of weak cryptographic functions, or hardcoded passwords and API keys, is found by reverse engineering the firmware (De La Cruz and Bradley 2021).

In order to mitigate the latter, firmware over-the-air (FoTA) updates are issued. Jaouhari and Bouvet (2022) claim this is a complicated task given that there is a lack of consensus regarding how to implement it, combined with the challenges these devices already face. In order to support this claim, the authors list several attacks that target updating firmware, such as the "Rollback attack" where the threat actor sends an "update" to the device that is in fact an old and vulnerable version; the "Repeated update requests attack" where the threat actor sends multiple update requests, either with valid or invalid firmware, in order to attempt a DoS attack; or the "Mismatched firmware" where the threat actor sends valid firmware, but for a different type of IoT device. Table 4 contains a potential attack for each STRIDE threat and the respective countermeasure at the firmware layer.

Threat	**Potential Attack**	**Countermeasure**
Spoofing	Spoofing the firmware update server, sending malicious firmware updates to the smart bulb.	Implement strong authentication mechanisms to ensure that only legitimate updates are accepted (e.g., use digital signatures).
Tampering	Modifying the firmware of the smart bulb to disable security features or introduce backdoors.	Employ secure boot mechanisms to verify the integrity of the firmware before execution.
Repudiation	Compromising the firmware of a smart bulb to manipulate its logging functionality, if there is one.	Implement secure logging within the firmware, recording all significant actions and events.
Information Disclosure	Vulnerabilities in the firmware can allow for the leak of sensitive information stored or processed by the smart bulb (e.g., network credentials, user data).	Employ secure coding practices to minimize the risk of vulnerabilities in the firmware (e.g., encrypt sensitive information, use access controls).
Denial of Service	Flooding the smart bulb with malformed firmware update requests, overwhelming its processing capabilities and causing it to become unresponsive.	Implement firmware update request validation mechanisms to filter out malicious or malformed requests (e.g., rate limiting).
Elevation of Privilege	Exploiting a vulnerability in the firmware that allows for the execution of code within the bulb's memory with elevated privileges.	Apply the principle of least privilege, and regularly update the firmware to address known vulnerabilities and mitigate the risk of privilege escalation attacks.

Table 4: STRIDE applied to the Firmware layer

Table 4 shows potential attacks of how STRIDE can identify threats at the firmware layer. In this table, several examples of threats are highlighted with their respective countermeasures. The main attacks targeting this layer usually focus on finding vulnerabilities via reverse engineering the firmware (e.g., dumping, modifying, and flashing the firmware), or finding vulnerabilities in the firmware's update process.

For example, in order to preserve the integrity of the boot code, IoTSF (2019a) advise to check for the validity and trust worthiness of each stage of it immediately before running that code so that the risk of TOCTOU attacks (time-of-check to time-of-use) is reduced. Additionally, Arakadakis et al. (2021) analyze the challenges and limitations of over-the-air programming (OTAP) for IoT devices in respect to the firmware update process, in modern IoT networks. The authors claim that an adversary can launch both external and insider attacks, with the first being perpetrated when the attacker forges packets, launches replay attacks or impersonates nodes that disseminate the updates, and the latter being perpetrated when the attacker has managed to control a node. The authors also claim that a successful insider attack can gain complete control over the network by compromising a single node, by leveraging the dissemination nature of the system. These nodes are used so that manufacturers can use "incremental programming" schemes, which consist on issuing delta scripts (patches) in order to avoid sending the whole firmware image every time a new update is released. Despite incremental programming improving the efficiency and security of firmware updates, Toutsop, Das, and Kornegay (2021) claim that most IoT devices that a user purchases are not secure "out of the box". This implies that the user needs to update the firmware and configure the device to operate securely before connecting it to the network.

Similarly to the previous layer, there are usually no non-repudiation mechanisms to ensure the ownership of actions. The common non-repudiation technique is to check for the validity of the signature of the firmware image or of a new patch. Regarding redundancy, this layer usually stores a "golden image" to provide fail-safe updates (Jaouhari and Bouvet 2022).

Overall, the security of this layer depends heavily on its implementation. However, unlike the previous layer, the user is required to have an active approach and update the firmware to remain secure. Therefore, the main requirements to secure this layer are to:

FW1 Update the firmware regularly;

FW2 Require all firmware updates to be digitally signed with a trusted certificate;

FW3 Ensure that each firmware update is the latest;

FW4 Utilize hardware-based secure boot mechanisms combined with a root of trust to ensure that only authenticated and unmodified firmware is loaded during boot-up.

4.3. Connectivity layer

The connectivity layer lies between the firmware layer and the application layer, and it is concerned with the communication between the smart bulb and the other party, which is usually the mobile application or the cloud server. From a security perspective, this layer is in charge of providing the security that is necessary to communicate safely. Popular communication protocols used in this layer include Wi-Fi, Zigbee, and Z-Wave.

A common approach to find vulnerabilities and consequently improve the security of this layer lies in fuzzing, given the difficulty in emulating IoT devices, mainly due to the lack of scalability. Fuzzing consists of providing invalid, unexpected, or random data as input to a program. With this method, Ma et al. (2023) created a hub fuzzing tool was tested against 21 IoT devices and uncovered 23 zero-day vulnerabilities, resulting in the assignment of 4 CVEs. Notably, CVE-2022-47100 was identified concerning smart bulbs. Ren et al. (2021) developed a device-agnostic fuzzing tool in order to detect implementation vulnerabilities regarding Zigbee. With this tool, the authors found 3 vulnerabilities in Z-Stack, the mainstream code implementation of Zigbee. Additionally, Check Point (2020) demonstrated a notable attack when, by posing as an authentic ZigBee light bulb, the authors managed to capitalize on weaknesses detected within the bridge, granting them access to penetrate the "internal" network through a remote ZigBee exploit conducted over-the-air.

Table 5 contains a potential attack for each STRIDE threat and the respective countermeasure at the connectivity layer.

Threat	**Potential Attack**	**Countermeasure**
Spoofing	Spoofing the identity of the smart bulb by sending false commands to the central hub, or the identity of the user to the smart bulb.	Implement strong authentication mechanisms such as cryptographic protocols (e.g., TLS) to ensure the identity of both the smart bulb and users.
Tampering	Modifying data packets in transit to alter commands.	Use message integrity checks to ensure the integrity of transmitted data.
Repudiation	Lacking logging mechanisms may lead to repudiation issues.	Implement comprehensive logging to record relevant actions taken by users and devices, making it possible to trace and verify actions.
Information Disclosure	Intercepting unencrypted, or weakly encrypted, data packets to obtain sensitive information.	Encrypt all sensitive data in transit using strong encryption algorithms.
Denial of Service	Flooding the network with excessive traffic to overwhelm the smart bulb.	Implement DoS mitigation techniques such as rate limiting or traffic filtering.
Elevation of Privilege	Exploiting vulnerabilities in network protocols or configurations to gain unauthorized access to the smart bulb.	Regularly update firmware and implement least privilege.

Table 5: STRIDE applied to the Connectivity layer

Table 5 shows potential attacks of how STRIDE can identify threats at the connectivity layer. In this table, several examples of threats are highlighted with their respective countermeasures. The main attacks targeting this layer usually rely on fuzzing tools that exploit implementation flaws. Therefore, the usage of frameworks that provide such features is recommended (e.g., Killerbee to fuzz Zigbee (River Loop Security 2024)).

Overall, this layer is similar to the hardware layer in the sense that the security depends heavily on its implementation. With this, the main requirements to secure this layer are to:

CO1 Implement robust authentication mechanisms (e.g., TLS) to verify the identity of both the smart bulb and users;

CO2 Use message integrity checks to verify the integrity of data packets transmitted between the smart bulb and other parties;

CO3 Encrypt all sensitive data transmitted between the smart bulb, mobile application, and cloud server using strong encryption algorithms.

4.4. Application layer

The application layer lies between the connectivity layer and the cloud layer, and it is concerned with the security of the mobile application that issues commands to the smart bulb.

Securing mobile applications is no easy task and several attacks can be conducted in order to compromise the security of the communication between the smart bulb or the cloud. These attacks range from installing malicious versions of the application, to installing malicious updates, or by having the device responsible for controlling the smart bulb infected.

Table 6 contains a potential attack for each STRIDE threat and the respective countermeasure at the application level.

Threat	Potential Attack	Countermeasure
Spoofing	Spoofing the original application in order to harvest user credentials.	Implement robust authentication mechanisms (e.g., multi-factor authentication).
Tampering	Malicious modifications to the app's code alter bulb settings without user consent.	Employ code signing and integrity checks to detect unauthorized modifications to the application code.
Repudiation	Inadequate logging in the app leads to disputes as users deny making bulb control changes.	Implement comprehensive logging of user actions and changes to bulb settings.
Information Disclosure	Poor security practices expose user data stored insecurely or transmitted without encryption.	Encrypt sensitive data at rest and in transit.
Denial of Service	Floods of requests overwhelm the app's servers, rendering it unusable for legitimate users.	Implement rate limiting and request throttling mechanisms to mitigate the impact of excessive requests.
Elevation of Privilege	Exploiting vulnerabilities grants users unauthorized administrative access, leading to control over all bulbs or disruptions.	Enforce least privilege principles by granting users only the permissions necessary to perform their intended tasks.

Table 6: STRIDE applied to the Application layer

Table 6 shows potential attacks of how STRIDE can identify threats at the application layer. In this table, several examples of threats are highlighted with their respective countermeasures. Although some may argue that code obfuscation is "security by obscurity", it is still advisable. This not only obstructs competitors, but also threat actors who seek to exploit, by reverse engineering for example, the smart bulb for their own purpose. The main attacks targeting this layer usually rely on implementation flaws from the developers or a low level of security from the user. Therefore, the main requirements to secure this layer are to:

AP1 Implement robust authentication mechanisms (e.g, MFA);

AP2 Regularly update and patch the mobile application to address known vulnerabilities and emerging threats;

AP3 Implement secure device enrollment procedures that authenticate and verify the identity of smart bulbs before they are added to the user's account;

AP4 Implement tamper detection mechanisms to detect and respond to unauthorized modifications or tampering attempts on the mobile application.

4.5. Cloud layer

This layer lies at the top of the layer list and, in some scenarios, acts as a middleman between the mobile application and the smart bulb. The security of this layer is concerned with the data that is stored in the cloud and the commands that are sent to the smart bulb.

Cloud environments are targeted by attackers due to the fact that they hold data from multiple users in a centralized service. Thus, it is paramount these services are secured and protected against various threats. Attackers frequently target cloud environments for the valuable data they contain. As such, securing these services is crucial not only for the protection of individual users but also for the integrity and trustworthiness of the entire system.

Table 7 contains a potential attack for each STRIDE threat and the respective countermeasure at the cloud level.

Threat	**Potential Attack**	**Countermeasure**
Spoofing	Attackers might attempt to impersonate legitimate cloud services to gain unauthorized access to the smart bulb's data or control.	Implement strong authentication mechanisms (e.g., MFA) for accessing cloud services.
Tampering	Unauthorized modification of data stored in the cloud, such as device configurations or user credentials.	Employ data integrity checks such as cryptographic hashing to detect unauthorized modifications to data stored in the cloud.
Repudiation	Lack of proper logging or auditing mechanisms in the cloud infrastructure might lead to repudiation issues.	Implement comprehensive logging mechanisms to record all actions performed on the cloud infrastructure.
Information Disclosure	Unauthorized access to sensitive data stored in the cloud, such as user profiles or device usage patterns.	Encrypt sensitive data stored in the cloud to prevent unauthorized access.
Denial of Service	Overloading cloud servers or services with excessive requests to disrupt service availability.	Implement rate limiting and throttling mechanisms to mitigate excessive requests and prevent service overload.
Elevation of Privilege	Exploiting vulnerabilities in cloud infrastructure or authentication mechanisms to gain unauthorized access or control over the smart bulb.	Implement access controls to restrict modification privileges to authorized users only, while following least privilege principles.

Table 7: STRIDE applied to the Cloud layer

Table 7 shows potential attacks of how STRIDE can identify threats at the cloud layer. In this table, several examples of threats are highlighted with their respective countermeasures. This layer is unique in the sense that the user has no control over the data that is processed. Therefore, the main attacks targeting this layer target the cloud provider (the communication to the cloud is addressed in Section 4.3), and consequently its infrastructure. With this, the main requirements to secure this layer are to:

CL1 Implement MFA for all users accessing cloud services;

CL2 Encrypt all sensitive data stored in the cloud;

CL3 Maintain comprehensive logs of all actions performed on the cloud infrastructure, and digitally sign them;

CL4 Implement rate limiting and throttling mechanisms to mitigate excessive requests and prevent service overload.

5. Framework

A framework was developed in order to encapsulate the conducted threat modeling. This framework is displayed in Figure 3, and it proposes an iteration approach in order to refine the general understanding of threats towards smart bulbs. The iterations shall continue until no new knowledge is gathered, as new knowledge indicates an incomplete knowledge base.

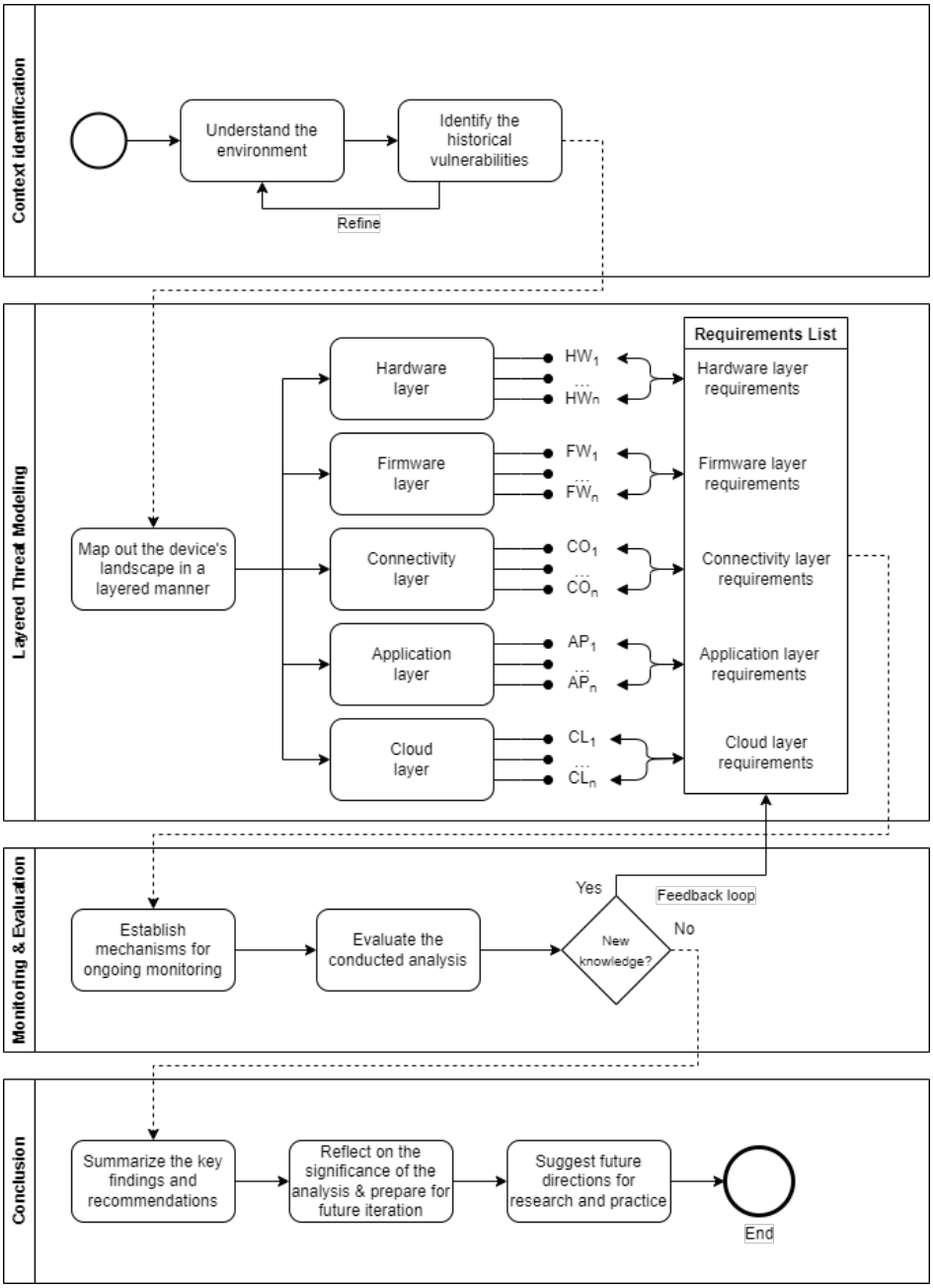

Figure 3: Threat Modeling Framework

As it can be seen in Figure 3, this framework comprises of four sections, namely:

- **Context Identification:** where the environment is understood (i.e., how does the smart bulb work, what are its components, how does it communicate) and the historical vulnerabilities are analyzed. This section aims to build the pillars from which further knowledge will be based upon;
- **Layered Threat Modeling:** consists of identifying threats, through a layered approach. To do so, the current landscape is mapped with the knowledge gathered from the previous section. After mapping the landscape, layers are assigned, and for each layer, threats, countermeasures, and requirements are identified. Consequently, the requirements are merged in a requirements list;
- **Monitoring & Evaluation:** consists on monitoring and evaluating the current understanding of smart bulbs. This is done by establishing mechanisms for ongoing monitoring that are based on the requirements list, and by evaluating the conducted analysis. As new knowledge is gathered, the requirements for each layer, and consequently the requirements list, are reassessed;
- **Conclusion:** where the key finding are summarized, the significance of the analysis is reflected, and future directions are suggested.

This framework is analyzed and discussed in Sections 6 and 7.

6. Implementation & Results

This section highlights in detail how the selected methods were applied during the conducted research. As previously mentioned, this thesis relies on design science research in order to guide the approach taken, and to design an artifact.

6.1. Design Evaluation Methods

As described in Section 3.1, in order to follow the "Information Systems Research Framework" (Hevner et al. 2004), one needs to identify the environment, the IS research, and the knowledge base. In the context of this thesis, the environment is the research community, which can utilize this study as a comprehensive resource on smart bulb security. The knowledge base comprises of the public academic databases, from which this artifact is built upon and intends to contribute to, further enhancing the understanding of this area. The IS research artifact is this thesis, mainly relating to the framework provided, as it is main contribution of this thesis.

In order to evaluate an artifact, Hevner et al. (ibid.) suggest several design evaluation methods. As mentioned in Section 3.3, the two methods chosen were "informed argument" and "scenarios", with both belonging to the "descriptive" category, due to their applicability to this work.

The informed argument method consists on using information from the knowledge base to build convincing arguments for the artifact's utility. Given that this work identifies and proposes an approach to close a research gap, is built upon relevant literature, and shows a deep understanding of the problem's domain, it stands as a significant contribution to the field.

The scenarios method consists on constructing detailed scenarios around the artifact to demonstrate its utility. To do so, events were collected, analyzed, and evaluated in order to illustrate how the framework can help prevent incidents and protect smart bulbs. The events were collected from news and blog articles, since the public academic databases yielded no new results when querying for "smart bulb" and keywords such as "incident", "hack", or "news".

Nardi (2019) shows, through a blog article, that it is possible to extract the Wi-Fi SSID and encryption key from the smart bulb's memory. The author was also able to dump the firmware image and extract sensitive information, such as a root certificate and an RSA private key. While requirement HW4 (Encrypt sensitive data at rest) would have mitigated the former extraction, the latter extraction could only be mitigated through a firmware update, which relates to requirement FW3 (Ensure that each firmware update is the latest). Muravitsky, Dashchenko, and Sako (2018) show similar findings, but in this case it was not only the network credentials of the Wi-Fi network, but the list of all credentials of every Wi-Fi network to which the bulb had connected before.

List (2020) also describes an event in which a researcher managed to reverse engineer and upload custom firmware to an Fcmila branded smart bulb that contained a "relatively unknown Chinese SoC" Opulinks OPL1000. Although in this case the firmware modification is used to improve the user's experience, one should also consider a supply chain attack where a threat actor modifies the firmware of smart bulbs intended for distribution, which is addressed by requirements FW2 and FW4.

Notselwyn (2023) details through a blog article how he hacked his smart lights with CVE-2022-47758. This CVE's description is "Nanoleaf firmware v7.1.1 and below is missing TLS verification, allowing attackers to execute arbitrary code via a DNS hijacking attack". In the author's example, rogue DHCP, DNS, and MQTT servers were used in order to trick the smart bulb into believing it was receiving debug commands from the official debugging endpoint. It must be acknowledged that, prior to the update which patched this vulnerability, the framework would not have protected against this attack. This is due to the fact that the CVE does not contain any of the searched keywords in its description, and therefore not initially being taken into consideration. Nonetheless, given that the nature of this vulnerability lies in an implementation flaw where TLS verification is missing, the framework would have prevented the attack with the corresponding patch by following requirement FW3, that ensures each firmware update is the latest.

These examples show that, despite not protecting the smart bulb against every scenario, the framework is effective in addressing most of the attacks described. It is also important to remember the iterative nature of this framework, as it is still in its first iteration. Scenarios that generate requirements that are not initially in the knowledge base are important, since they identify needed requirements that were not previously accounted for, thereby increasing the framework's robustness.

7. Discussion

There will always be trade-offs in the world of technology and IoT devices are no exception to the rule. The constraints of low processing power and limited memory present inherent challenges that impede the seamless integration of robust security measures. These restrictions make it more difficult to apply complex security procedures and increase the susceptibility of equipment to outside attackers. Striking a balance between functionality, efficiency, and security becomes a delicate task. A task which threat actors that advantage of by exploiting these challenges to their own benefit.

The proposed framework helps addressing the aforementioned problem when considering smart bulb security. One major limitation of this framework is that it has not been tested against a physical device due to time constraints. Although this would contribute greatly to the reliability of the framework, the contributions provided from the analysis and conducted threat modeling should not be underestimated.

When comparing with other frameworks, this work provides a different approach by splitting the smart bulb device into its layers. Despite the concepts of splitting an IoT device into its layers or the concept of developing a framework to improve the security of IoT devices not being new, the novelty of this work lies in combining both, along with threat modeling, to achieve a more comprehensive approach. Additionally, by using threat modeling at its core and by listing requirements, this framework's results are straightforward, while other frameworks usually use threat modeling as a tool to build a quick and simple understanding of the attack surface with the goal of building an artifact with different purposes.

Regarding the followed methodology, most of the information was collected from academic databases, with some exceptions to the rule, given that the cybersecurity community produces a significant amount of relevant content that is not academically published. This thesis serves as the basis, and therefore the first iteration of the framework, for further research regarding the security of smart bulbs. Without performing a second iteration, or testing the framework technically, it becomes hard to assess how well this framework performs systematically. Nonetheless, the first iteration provided a good understanding of the smart bulb's environment, namely the threats they face, along with countermeasures to mitigate them.

Threat modeling precedes risk management, with the latter being highly context dependent. Therefore, when reflecting on the chosen research problem, the framework would ideally support the risk management efforts of organizations who are concerned about the security of their smart bulbs. In an extreme scenario, this organization might even be a critical infrastructure. In order to enhance the insights threat modeling provides, a better understanding of the device being examined is required, which falls under the "Context Identification" stage of the framework. Despite this iteration mainly relying on identifying historical vulnerabilities, this can also be achieved through other methods that enhance the understanding of the smart bulbs threat landscape. In order to improve the conducted threat modeling, other methods should also

be considered.

7.1. Ethical and societal aspects

Although it is impossible to rule out the possibility that those with bad intentions could use some of this work for nefarious purposes, which is transversal to everything related to security, it is thought that researchers would benefit from a project that assists in assessing the security posture of smart bulbs, with the latter being the ultimate goal of this thesis. Additionally, since all the gathered data originates from publicly accessible sources, there are no privacy or GDPR concerns associated with this research.

Regarding the societal aspects, it is thought that this framework can help researchers assessing and evaluating the security posture of smart bulbs. Despite being based on a diagrams regarding a home-based network, this work can be extended and applied to different types of networks where smart bulbs may exist, such as public of critical infrastructure, and therefore help protecting them.

7.2. Limitations

A crucial limitation shared by all projects is the limitation of time. The research community is continuously developing and publishing articles, which makes it hard to claim to have researched "all" the existing literature. Furthermore, when researching for the security of smart bulbs, it was common to find articles that mainly focused on IoT security that briefly mentioned smart bulbs, usually in an example, by bundling them with other home-based IoT devices such as smart outlets or smart thermostats. Nonetheless, an extensive research was conducted with the aim of accurately depicting the landscape of smart bulbs while being as thorough as possible.

Lastly, a notable limitation stems from the nature of this thesis as an individual work. Like all individual projects, it presents a challenge for peer reviewing the literature review. Furthermore, the same limitation applies to the threat modeling section, where the absence of a collaborative environment may limit the depth of threat identification and analysis.

8. Conclusion

In this thesis, an overview of the challenges that smart bulbs face was provided, along with the reasons for widespread adoption of such devices. The research problem was highlighted, and the research question formulated. To answer the first half of the research question, the challenges that smart bulbs face were detailed, along with the historical vulnerabilities found in these devices. To answer the second half of the research question, a tailored framework, with threat modeling at its core, was developed.

In order to build the foundational knowledge needed to conduct the threat modeling, along with developing the framework, data was gathered regarding the state of IoT devices. The data gathered includes their landscape, applicable current legislation, cyber attacks, defense mechanisms, and vulnerabilities. Then, a network topology and its respective data flow diagram of a home network with smart bulbs, was developed. The smart bulb was then split into its layers, with each being analysed thoroughly with threat modeling. A first iteration of potential attacks, respective countermeasures, and requirements was listed, allowing for a deeper understanding of the underlying threats to smart bulbs. This procedure was then formalized and encapsulated with a framework that assesses the security posture of a smart bulb.

Overall, it is believed that this thesis contributes to the community's body of knowledge. Through the developed framework, this thesis provides valuable insights into detailing the smart bulb's landscape.

8.1. Future work

In order to refine the conducted threat modeling, more research regarding the security of smart bulbs should be performed. With new requirements being added to the knowledge base, the robustness of the framework is consequently increased. Building on this thesis, further iterations and applications of the framework in real-world scenarios would be a significant contribution.

Topics that were excluded from the scope of this thesis, such as privacy or artificial intelligence, can be explored to further support the research community. Additionally, considering the increasing integration of smart bulbs into smart home ecosystems, examining the broader security implications of interconnected smart devices (e.g., cross-device exploitation) could provide valuable insights.

Bibliography

Affinito, Antonia et al. (2023). "The evolution of Mirai botnet scans over a six-year period". In: *Journal of Information Security and Applications* 79, p. 103629. ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2023.103629. URL: https://www.sciencedirect.com/science/article/pii/S2214212623002132.

Akhilesh, Rohit et al. (2022). "Automated Penetration Testing Framework for Smart-Home-Based IoT Devices". In: *Future Internet* 14.10. ISSN: 1999-5903. DOI: 10.3390/fi14100276. URL: https://www.mdpi.com/1999-5903/14/10/276.

Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo (2018). "Internet of Things: A survey on the security of IoT frameworks". In: *Journal of Information Security and Applications* 38, pp. 8–27. ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2017.11.002. URL: https://www.sciencedirect.com/science/article/pii/S2214212617302934.

Arakadakis, Konstantinos et al. (Oct. 2021). "Firmware Over-the-air Programming Techniques for IoT Networks - A Survey". In: *ACM Comput. Surv.* 54.9. ISSN: 0360-0300. DOI: 10.1145/3472292. URL: https://doi.org/10.1145/3472292.

Bonaventura, Davide, Sergio Esposito, and Giampaolo Bella (2023). "Smart Bulbs can be Hacked to Hack into your Household". In: *arXiv preprint arXiv:2308.09019*.

Casola, Valentina et al. (2019). "Toward the automation of threat modeling and risk assessment in IoT systems". In: *Internet of Things* 7, p. 100056. ISSN: 2542-6605. DOI: https://doi.org/10.1016/j.iot.2019.100056. URL: https://www.sciencedirect.com/science/article/pii/S2542660519300290.

Check Point (2020). *Don't Be Silly - It's Only a Lightbulb*. URL: https://research.checkpoint.com/2020/dont-be-silly-its-only-a-lightbulb/.

Dalvi, Ashwini, Saraswati Maddala, and Divya Suvarna (2018). "Threat Modelling of Smart Light Bulb". In: *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, pp. 1–4. DOI: 10.1109/ICCUBEA.2018.8697723.

De La Cruz, Junibel and Matt Bradley (Sept. 2021). "Philips Hue Bulb & IoT App Security". In.

Dhanjani, N (2013). "Hacking lightbulbs: Security evaluation of the philips hue personal wireless lighting system". In: *Internet of Things Security Evaluation Series*, pp. 1–46.

ENISA (2023). *Glossary (Risk Management)*. URL: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary.

European Commission and Directorate-General for Communications Networks, Content and Technology (2022). *Cyber resilience act – New EU cybersecurity rules ensure more secure hardware and software products*. European Commission. DOI: doi/10.2759/543836.

Fan, Xu et al. (2017). "Security Analysis of Zigbee". In: URL: https://api.semanticscholar.org/CorpusID:37828092.

Force, Joint Task and Transformation Initiative (2013). "Security and privacy controls for federal information systems and organizations". In: *NIST Special Publication* 800.53, pp. 8–13.

Hevner, Alan R. et al. (2004). "Design Science in Information Systems Research". In: *MIS Quarterly* 28.1, pp. 75–105. ISSN: 02767783. (Visited on 03/06/2024).

IoTSF (2019a). *Device Secure Boot*. URL: https://iotsecurityfoundation.org/best-practice-guide-articles/device-secure-boot/.

– (2019b). *Physical Security*. URL: https://iotsecurityfoundation.org/best-practice-guide-articles/physical-security/.

Jaouhari, Saad El and Eric Bouvet (2022). "Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions". In: *Internet of Things* 18, p. 100508. ISSN: 2542-6605. DOI: https://doi.org/10.1016/j.iot.2022.100508. URL: https://www.sciencedirect.com/science/article/pii/S2542660522000142.

Karie, Nickson M. et al. (2021). "A Review of Security Standards and Frameworks for IoT-Based Smart Environments". In: *IEEE Access* 9, pp. 121975–121995. DOI: 10.1109/ACCESS.2021.3109886.

Lins, Fernando A. Aires and Marco Vieira (2021). "Security Requirements and Solutions for IoT Gateways: A Comprehensive Study". In: *IEEE Internet of Things Journal* 8.11, pp. 8667–8679. DOI: 10.1109/JIOT.2020.3041049.

List, Jenny (2020). *A brain transplant for an uncommon smart bulb*. URL: https://hackaday.com/2020/12/07/a-brain-transplant-for-an-uncommon-smart-bulb/.

Lockheed Martin (2024). *Cyber Kill Chain*. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Ma, Xiaoyue et al. (2023). "No More Companion Apps Hacking but One Dongle: Hub-Based Blackbox Fuzzing of IoT Firmware". In: *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*. MobiSys '23. Helsinki, Finland: Association for Computing Machinery, pp. 205–218. ISBN: 9798400701108. DOI: 10.1145/3581791.3596857. URL: https://doi.org/10.1145/3581791.3596857.

Microsoft (2022). *Microsoft Threat Modeling Tool threats - STRIDE model*. URL: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats.

Mira, Fahad and Izzat Alsmadi (2019). "Review of Analysis on IoT Components, Devices and Layers Security". In: *2019 International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 1–6. DOI: 10.1109/ICISCT47635.2019.9012037.

MITRE (2024). *CVE - Common Vulnerabilities and Exposures*. URL: https://cve.mitre.org/cve/search_cve_list.html.

Morgner, Philipp, Stephan Mattejat, and Zinaida Benenson (2016). "All Your Bulbs Are Belong to Us: Investigating the Current State of Security in Connected Lighting Systems". In: *ArXiv* abs/1608.03732. URL: https://api.semanticscholar.org/CorpusID:14408535.

Muravitsky, Andrey, Vladimir Dashchenko, and Roland Sako (2018). *IoT hack: how to break a smart home... again*. URL: https://securelist.com/iot-hack-how-to-break-a-smart-home-again/84092/.

Nardi, Tom (2019). *Don't Toss That Bulb, It Knows Your Password*. URL: https://hackaday.com/2019/01/29/dont-toss-that-bulb-it-knows-your-password/.
NIST (2024a). *Cyber Attack*. URL: https://csrc.nist.gov/glossary/term/cyber_attack.
– (2024b). *National Vulnerability Database*. URL: https://nvd.nist.gov/vuln/search.
Notselwyn, Lau (2023). *How I hacked smart lights: the story behind CVE-2022-47758*. URL: https://pwning.tech/cve-2022-47758/.
OWASP (2018). *OWASP Top 10 Internet of Things*. URL: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf.
– (2024). *Threat Modeling Cheat Sheet*. URL: https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html.
Al-Qaseemi, Sarah A. et al. (2016). "IoT architecture challenges and issues: Lack of standardization". In: *2016 Future Technologies Conference (FTC)*, pp. 731–738. DOI: 10.1109/FTC.2016.7821686. URL: https://api.semanticscholar.org/CorpusID:25623880.
Reedy, Paul (2023). "Interpol review of digital evidence for 2019–2022". In: *Forensic Science International: Synergy* 6, p. 100313. ISSN: 2589-871X. DOI: https://doi.org/10.1016/j.fsisyn.2022.100313.
Ren, Mengfei et al. (2021). "Z-Fuzzer: device-agnostic fuzzing of Zigbee protocol implementation". In: *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec '21. Abu Dhabi, United Arab Emirates: Association for Computing Machinery, pp. 347–358. ISBN: 9781450383493. DOI: 10.1145/3448300.3468296. URL: https://doi.org/10.1145/3448300.3468296.
River Loop Security (2024). *IEEE 802.15.4/ZigBee Security Research Toolkit*. URL: https://github.com/riverloopsec/killerbee.
Rizvi, Syed et al. (2020). "Threat model for securing internet of things (IoT) network at device-level". In: *Internet of Things* 11, p. 100240. ISSN: 2542-6605. DOI: https://doi.org/10.1016/j.iot.2020.100240. URL: https://www.sciencedirect.com/science/article/pii/S2542660520300731.
Ronen, Eyal and Adi Shamir (2016). "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights". In: *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 3–12. DOI: 10.1109/EuroSP.2016.13.
Ronen, Eyal, Adi Shamir, et al. (2017). "IoT Goes Nuclear: Creating a ZigBee Chain Reaction". In: *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 195–212. DOI: 10.1109/SP.2017.14.
Statista (2023). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030*. URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.
Stellios, Ioannis, Kostas Mokos, and Panayiotis Kotzanikolaou (2021). "Assessing Vulnerabilities and IoT-Enabled Attacks on Smart Lighting Systems". In: *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers*. Darmstadt, Germany: Springer-Verlag, pp. 199–217. ISBN: 978-3-030-95483-3. DOI: 10.1007/978-3-030-95484-0_13. URL: https://doi.org/10.1007/978-3-030-95484-0_13.

Toutsop, Otily, Sanchari Das, and Kevin Kornegay (2021). "Exploring The Security Issues in Home-Based IoT Devices Through Denial of Service Attacks". In: *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, pp. 407–415. DOI: 10.1109/SWC50871.2021.00062.

Victor, P. et al. (2023). "IoT malware: An attribute-based taxonomy, detection mechanisms and challenges". In: *Peer-to-Peer Netw. Appl.* 16, pp. 1380–1431. DOI: 10.1007/s12083-023-01478-w.