Universiteit Leiden

ICT in Business and the Public Sector

Security Challenges in a Smart Home IoT

Name: Falih Ihsan
Student-no: s2742349

Date: 25/04/2022

1st supervisor: Olga Gadyatskaya

2nd supervisor: Nele Mentens

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)

Leiden University

Niels Bohrweg 1

2333 CA Leiden

The Netherlands

Abstract

As smart home automation popularity increases, so does the number of people that are using smart home devices. However, there are some issues regarding the smart home, which are privacy and security concerns as its technology can easily be hacked.

This study analyzes the current state of smart home security, what type of challenges it faces, and who is responsible for the security in smart home IoT.

To identify the security challenges, the existing literature was studied. In addition, an interview with experts and a survey with smart home users were conducted to find out their insights in this regard. The interview and survey results were analyzed and compared with the literature. Furthermore, the limitations of this study are also discussed.

The results showed there are many attack vectors and vulnerabilities in smart home IoT. According to the experts, the most common attack vector is a network attack, and the most dangerous vulnerability is RCE. Security devices in the market could help improve security, although only on the network level. The majority of answers showed manufacturers as responsible for smart home security.

Table of Contents

Table of Figures

Table of Tables

1. Introduction

1.1. Introduction to the Internet of Things and smart home

Internet of Things (IoT) is a system that uses physical objects which is embedded with software, sensors, and other technologies in order to exchange information and data with other devices over the Internet. As a dependency on using the computer network increases, then data becomes more valuable. Therefore, the way the information is protected and its security are now essential [1]. As stated by the website Statista [2], the number of connected devices will increase from 20.35 billion in 2017 to 75.44 billion in 2025 around the world. With this growth, cyber-attacks will be more likely to occur and potentially become a severe threat to IoT devices and applications as IoT grows.

Based on the book “Inside the Smart Home” written by Richard Harper, the word Smart Home was officially used in “1984 by the American Association of House Builders” [3, p. 1]. A smart home is a house that utilizes technology to help human activities at home, and it can be controlled remotely. A smart home uses smart devices and is connected through wireless or wired to communicate and exchange data. According to verified market research [4], the smart home market value is estimated at USD 98.24 billion in 2020 and will increase to USD 495.15 billion in 2028. As the number of market values grows, consumer spending will rise from $86 billion in 2020 to $173 billion by 2025 [5].

However, the presence of smart homes also endangers consumers' or users’ risk of security, privacy, and physical safety [6]. For instance, an attacker can eavesdrop or intercept the wireless transmission of sensors and observe the residents' indoor activities, such as showering and sleeping [7]. Furthermore, attackers can use it to their advantage if they learn the schedule of house inhabitants. For example, attackers can decide to grab valuable items when the owners are not at home, or worse, the attacker can harm the owners’ life by attacking them when they are sleeping.

1.2. Background

As part of the IoT, smart home technologies are operated through the internet, so users are able to monitor and control their devices remotely. However, in the same way, cybercriminals can also easily access smart home devices through the Internet by exploiting the vulnerabilities in the devices. As per an investigation led by Which [8], smart homes

could experience more than 12,000 cyber-attacks in a single week. Furthermore, in 2017, it was reported that DDoS attacks increased 91% because of IoT [9]. The Mirai botnet attack was one example of the most known DDoS attack, which was using smart home devices to attack a DNS provider and several websites in 2016.

There are more instances of incidents that cause privacy issues for smart home users. One of the news about a smart home hack was in 2019 when a Nest system was interceded and distressed the homeowners by changing the room temperature, talking to them via a camera, and playing disturbing music. The issue continued even though users had changed passwords before they finally changed their network ID [10]. Another incident was in 2013 when a hacker said inappropriate words to a baby through a baby camera [11]. In 2016, a bug in a Nest smart thermostat software had drained its battery and eventually turned it off, and it caused a cold midnight for the home user [12]. Another news concerning thermostats was in 2017 when hackers raised the home temperature from 23C to 35C [13]. Such incidents could cause property and economic damage where the heating bills increase.

Questions on what kind of attacks are possible in smart home IoT and who is responsible for smart home security have now arisen. The various news about smart homes getting hacked indicates that the security in smart home devices is required to be improved. As the market value and consumer spending in smart homes will increase, so will the potential for misuse.

1.3. Definitions

The objective of this section is to explain the terms that emerged in discussions with experts about smart home security. A more comprehensive explanation of these terms is written in Chapter 2.

1.3.1. Denial-of-service and Distributed denial-of-service

A denial-of-service (DoS) attack takes place when the original user who owns a system or device cannot access it due to a malicious actor's actions. A DoS attack is accomplished when the target cannot respond or crash, which prevents the actual owner from gaining access by sending the targeted device or network with an overload of traffic. There is a term distributed denial-of-service attack (DDoS) attack. DDoS attacks happen when multiple devices operate to attack a single target. DDoS attackers usually use a botnet, a group of Internet-connected devices that have been hijacked, to make a large-scale attack [14].

1.3.2. Attack vector

Kaspersky describes attack vectors as “the method or means by which cyber-criminals penetrate or crack the target system” [15]. Therefore, a device is considered less secure if it has more number of attack vectors.

1.3.3. Blockchain

Blockchain is a digital ledger that is duplicated and shared across the computer network. Since the data is decentralized, it is considered more secure. The validity of the data will remain intact if one unauthorized actor tries to change data in the network because the rest of the data will not be altered in the network

1.3.4. Ransomware

Ransomware is when an attacker uses malware that employs encryption to lock the victim’s software and then demands some ransom to unlock it.

1.3.5. Artificial Intelligence, machine learning

Artificial Intelligence (AI) is the ability of a machine or digital computer to make decisions and perform intelligent tasks. Machine learning is the sub-field of AI [16].

1.3.6. Encryption

Encryption is the process of converting data into ciphertext to prevent confidential data leaks.

1.3.7. Homomorphic encryption

Homomorphic encryption makes it possible to analyze encrypted data without decrypting the data. Thus, the data can remain confidential while being processed [17].

1.3.8. MITM (Man In The Middle)

MITM is a type of attack where an attacker is positioned in the middle or between two communicating parties to intercept and/or alter the conversation between them [18].

1.3.9. Matter protocol

Matter protocol is a unified standard so that connectivity between smart home devices, mobile apps, and cloud services is more reliable, secure, and easy to use [19].

1.4. Research questions

The objective of this study is to gain insight on what kind of challenges a smart home encounters and it is based on the literature review and interviews with experts. This

research topic is relevant because the smart home market is estimated to increase [4], while smart home technology is still vulnerable to hacking [8].

The main research question is:

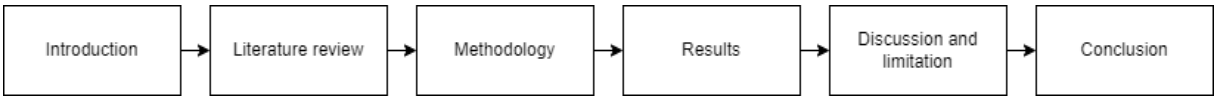
RQ: What are the security challenges in a smart home IoT?

To answer the main research question, sub-questions have been made:

1. What is the most dangerous vulnerability in the smart home?
2. What attack vector is the most common in smart home?
3. What are the advantages and disadvantages of implementing security devices in a smart home?
4. Who is the most responsible for smart home security?

1.5. Thesis structure

In this section, the structure of this thesis will be outlined. The study will be divided into six



phases and the complete structure will be illustrated below.

Figure 1: Schematic overview of the research

1.5.1. Literature Review

The literature is written with a combination of white and gray literature. White literature is research papers, academic books, published journals, and conference proceedings, while gray literature is government reports, corporations, lecturers, associations and sociates, and professional organizations [20].

The research was done using Google Scholar, ResearchGate, and the University of Leiden Database as the primary literature source. The keywords used to search the literature were: SOK, IoT, Smart Home, Security.

1.5.2. Methodology

The methodology is the explanation of how the research was done. Interviews were conducted with many experts. The study used semi-structured interviews to help the interviewee explore critical questions and give a more detailed response.

1.5.3. Results

Based on the interview that has been conducted, an analysis will be designed. In addition, answers from experts will be analyzed to see their opinions and thoughts.

1.5.4. Discussion and limitations

This chapter will discuss the experts' point of view and the limitation of the study will be written.

1.5.5. Conclusion

The study's conclusion and future work will be written in this chapter.

2. Literature review

2.1. Understanding the Internet of Things

The IoT refers to "an extension of the Internet into the physical world for interaction with physical entities from the surroundings" [21]. In other words, it is about connecting physical entities to the Internet and using it to interact with its surrounding. IoT has been implemented in many applications. According to Asghari *et al*. [22], IoT applications can be categorized into six groups which are healthcare, environment, smart city in which smart home IoT is a part of, commercial, industrial, and general aspects.

IoT can be divided into three layers; perception, network, and application [23].

- The perception layer is responsible for collecting data using sensors and actuators [23]. This layer gathers the information from the sensors and actuators and then transmits it to the network layer [24]. Some examples of the sensors in the perception layer are temperature sensors, humidity sensors, etc.
- The network layer is responsible for transmitting data that was acquired from the perception layer to different IoT Hubs and devices in the application layer over the Internet [25]. This is the layer where cloud computing platforms, Internet gateway, routing devices, etc., operate using protocols such as Wi-Fi, 5G, Zigbee, etc.
- The application layer is where the smart environment is achieved. One of the examples is the smart home environment.

2.2. The smart home

The smart home is part of the IoT (Internet of Things). A smart home stated by Aldrich [26, p. 17], is

> "A residence equipped with computing and information technology which anticipates and responds to the needs of the occupants, working to promote their comfort, convenience, security, and entertainment through the management of technology within the home and connections to the world beyond."

To put it more simply, a smart home is a home with IoT devices to provide convenience to the owner. Typically, a smart home consists of many connected devices that function in various areas with different applications. The various applications are generalized into four groups: energy management, entertainment, healthcare, and security [27]. Each group

consists of multiple devices to support its functions, such as entertainment with smart TVs and smart speakers. Smart home devices communicate through the home gateway using wired or radio communication. The end-users control the smart home devices using the smart home controller, such as smartphones or a home assistant. The gateway also serves as an access point for the devices connected to cloud services and the Internet.

The potential of the smart home market is enormous as consumer IoT products become part of daily life. According to a European Commission report in January 2022 [28], European smart home revenue will increase more than double from 2020 to 2025, from approximately €17 billion to about €38.1 billion. The number of smart home devices has been rising over the last few years [29]. Tech giants are also trying to get into the smart home market and offer different smart home devices, such as Google with Nest, Apple with HomeKit, and Samsung with SmartThings.

The concern of cybersecurity and privacy can outweigh the potential of smart home technology because when someone uses the technology, they will also share their private and sensitive information with private companies. The next subsection will discuss more about cyber security.

2.3. Understanding cyber security

Cybersecurity is a term that is used broadly, and its definitions are highly variable and unconcise [30]. The lack of meaning to cybersecurity makes it essential to clarify an issue which, in this case, what does it mean to have cybersecurity? In this case, how to ensure security in smart home technology? Cybersecurity revolves around three main themes, confidentiality, integrity, and availability [31]. The definition is as follows:

- Confidentiality: “assurance that data, programs, and other system resources are protected against disclosure to unauthorized persons, programs, or systems.”[1]
- Integrity: “assurance that programs, or systems protect data, programs, and other system resources are protected against malicious or inadvertent modification or destruction by unauthorized persons, programs, or systems.”[2]
- Availability: “assurance that use of data, programs, and other system resources will not be denied to authorized persons, programs, or systems.”[3]

[1] Arnbak 2015, p.322
[2] Ibid.

In other words, confidentiality is about ensuring that the authorized users' data is private. Integrity is about verifying the data and ensuring that the data is not tampered with by someone not authorized. Finally, availability ensures the data are permitted to be accessed by authorized users. These three attributes are the foundation of cybersecurity in a smart home. If one of these attributes is not functioning correctly, it will create vulnerabilities that will later impose threats to the smart home technology and cause a negative impact.

Implementing IoT in a smart home is risky as smart home suffers from privacy vulnerabilities such as encryption and authentication [32]. In addition, many smart home IoT devices that are commonly used have inadequate configuration settings to change passwords and access permission [33].

2.4. Smart home security problems

2.4.1. Smart home vulnerability

Vulnerabilities mean weakness or gaps in the protection system. There are many vulnerabilities in smart home IoT. Some vulnerabilities even stay in the same system for years even though there are patches. One of the reasons why the vulnerabilities are not fixed is because the administrators do not know which vulnerabilities are the most dangerous [34]. In other words, for manufacturers to fix the vulnerabilities in their devices, they need to know the most dangerous vulnerabilities in the device. Because of the connection with the Internet, smart home devices can be hijacked remotely without having to access the device physically. From the research of Abdullah *et al*. [35], the primary smart home vulnerabilities are heterogeneous architecture, outdated protocols, weak encryption, limited storage and CPU, insecure applications, poor authentication, and firmware failure.

Heterogenous architecture

Heterogeneous architecture means using a wide range of smart home devices that work effectively using different systems. There are many networking protocols that could be used in the smart home, such as Z-Wave, Zigbee, Wi-Fi, Insteon, etc. However, each protocol has its own strength and weaknesses; thus, a different variety of protocols will be difficult to be managed efficiently and securely by non-experts [36]. Due to heterogeneity, many problems arise, such as standardization problems and security issues [37]. Because there are no

[3] Ibid.

standards, it is not straightforward to determine the requirements of how secure the smart devices need to be, which allows hackers to take advantage of any open vulnerabilities [38].

Outdated protocols

Outdated protocols refer to protocols that are not upgraded, which making it possible to be hijacked by attackers. The traditional security protocols and procedures are not enough because the existing IoT devices have limitations in integrity, scalability, and interoperability. In addition, IoT protocols lack security features, and the trust between devices is non-existed [39].

Weak encryption

According to Kaspersky [40], in cyber security, encryption is the process of converting data into an encoded format. The function of encryption is to protect information confidentiality and ensure that the information is not being tampered with [41]. Poor encryption in one data will make the data transparent, thus allowing attackers to exploit it [35]. IoT devices have limited CPU and processing power hence, it affects the efficiency and efficacy of cryptosystems [42] [43]. Many smart home IoT devices are connected to the cloud to provide services such as remote control, notifications, and digital content [33]. However, weak encryption could cause a breach in the cloud system and cause a data breach [44].

Limited Storage and CPU

Smart home devices gather a lot of data to be analyzed, stored, and processed. However, device controllers usually have limited computational and storage resources, thus limiting their ability to implement proper security [36]. Furthermore, IoT devices are also connected to the Internet, thus exposing these devices to numerous types of attacks and making them vulnerable [45].

Insecure applications

There is a lack of privacy protection features in middleware platforms and IoT applications. Many IoT companies take advantage of the Internet to provide features and services that can be controlled using smartphone applications. Smartphone applications can be used to hijack a smart home device such as Max [46]. He found that programming errors in the mobile application of August Smart Lock could lead to a leak of the cloud endpoint of the device and sensitive information. Max used the found sensitive information to obtain the account login username and password and change the true owner of the device to himself

Poor authentication

Authentication is a method validating the true owner of a system or device. The primary risks of network communication come from poor credentials and poor authentication [35]. With insufficient authentication, a device or mobile application becomes vulnerable and can be exploited by a hacker. Once a hacker logs in and pretenses as a user, the hacker can change the password and make it inaccessible to the owner [47].

Firmware failure

Firmware is a type of software that is embedded in a hardware. IoT operating systems and firmware need to be patched regularly to minimize threats and enhance their functionality features [43]. Unfortunately, many IoT devices have similar firmware, which increases the probability of hacking, and making firmware a significant vulnerability in smart home IoT devices. However, many manufacturers and device vendors spend small investments on providing IoT patches because revenue does not come from the maintenance but the sales of the devices [48]. Therefore, leaving IoT devices with vulnerabilities that attackers could exploit.

2.4.2. Dangerous vulnerabilities

Keromytis [49] researched about vulnerabilities in VoIP. According to the author, VoIP/IMS (Voice over Internet Protocol / Multimedia Subsystems) is a product group that allows advanced communication services to be delivered over the Internet. The communication data can be stored in the cloud or in physical storage. The research is relevant because it has a similar process as smart home IoT as the data could be shared online. According to the researcher, the top five most dangerous vulnerabilities grouped by effect are denial of service, remote control of device, access to service, attack the user, and access to data. According to Kaspersky [50], a denial of service (DoS) attack is an attack that is launched to prevent a website, server, or other network resources from operating normally. Remote control of device means the adversary is taking complete control of the device, whether by default password and services, code injection, or authentication failure. Access to services and access to data are self-explanatory. Finally, attack the user means vulnerabilities that allow attackers to alter the administrator of a device.

On the other hand, Shiaeles *et al*. [47] discussed about the most critical vulnerabilities in IoT. They are arbitrary code execution, injection, broken authentication, cross-site request forgery, server-side request forgery, cross-site scripting, remote code execution, remote

command execution, denial of service, buffer overflow, privilege escalation, arbitrary file manipulation, and directory traversal.

- Arbitrary code execution refers to the execution of any code in a target.
- Injection is an attack that allows cybercriminals to inject malicious code and execute it remotely.
- Broken authentication is a vulnerability that allows an attacker to log in without having to make an account.
- Cross-site request forgery (CSRF) is an attack that occur when a cybercriminal trick the targeted victims into submitting a malicious request to a regular website.
- Server-site request forgery (SSRF) is an attack where attackers trick the server into allowing access to the server.
- Cross-site scripting (XSS) is a vulnerability that enables attackers to execute a malicious script on a trusted website.
- Remote code execution is executing malicious code on a target system over the Internet.
- Remote command execution is similar to remote code execution, where it lets the attacker execute malicious code remotely.
- Denial of service is an attack that is executed to shut down a website or server by sending a lot of traffic.
- Buffer overflow is an attack that aims to send carefully written code as an input to a website.
- Privilege escalation is where an attacker can trick a system into giving them extra privileges, such as an administrator.
- Arbitrary file manipulation is uploading malicious files to a website so that attackers can have access to the website
- Directory traversal is a vulnerability that allows an attacker to access hidden files on the website.

Software vulnerabilities that allow attackers to control a device remotely are the most dangerous attack. Such vulnerabilities are usually exploited by injecting malicious code into the targeted device software, allowing attackers to take control of the system. They are

generally called “arbitrary code vulnerabilities” including dangling pointer references, buffer overflow vulnerabilities, integer errors, and insecure use of format strings [51].

According to Kaspersky [52], Remote Code Execution (RCE) is one of the most dangerous computer vulnerabilities. The attack can be launched remotely without physical access to the device. It allows a cybercriminal to execute malicious code remotely on the victim’s computing device over the Internet or local networks. The impact of RCE vulnerability can lead to losing control of the system and theft of sensitive data. For example, in one of the RCE attacks on Microsoft in 2021 [60], attackers executed arbitrary code on Microsoft Exchange Server and could modify any/all affected files.

Armis Lab [53] has found a new attack vector called BlueBorne which spreads through the air and attacks via Bluetooth. Because it spreads via the air, it is more contagious and could spread with minimum effort. The attack is also hard to detect as traditional protection methods do not protect from airborne threats. BlueBorne allows cybercriminals to gain control of devices, spread malware to other devices, access corporate data and networks, and penetrate a secure network. Armis demonstrated an attack on a mobile phone where it showed that a successful RCE attack on a smartphone enables the attacker to gain full control of the device and take a picture of the owner.

2.4.3. Attack vector

An attack vector is a method of attack to exploit vulnerabilities in hardware or software. Attack vector allows a cybercriminal to gain access to sensitive data by exploiting vulnerabilities in the system. There are many attack vectors in IoT. Furthermore, one smart home device can have multiple attack vectors [54]. One of the causes why smart home devices could have various attack vectors is because manufacturers do not take security as a priority when they produce smart home IoT devices. Gemalto's report [55] showed that manufacturers and service providers spend only 13% of their total IoT budget on security. Because of the lack of support from the manufacturers, it leaves consumers with vulnerable and unsupported devices [56]. Kaspersky [57] reported 105 million attacks targeting IoT devices in the first six months of 2019, which increased significantly from just 12 million attacks in H1 2018. The attacks on IoT devices are mostly not complicated but use a method

that is hard to detect. The Mirai botnet used the unpatched vulnerabilities on smart home devices to easily slip through them and control them.

The threat of an attack in smart home IoT can come from human carelessness and the vulnerabilities in the device itself. Hughes-Lartey *et al*. [58] research stated that the human factor is a significant threat to the organization's cyber security. Furthermore, Breda *et al*. [59] stated that social engineering attacks are the biggest threat in cybersecurity, and it was reported that 98% of cyber-attacks rely on social engineering [60]. Social engineering is the art of manipulating people to gain others' confidential information. Social engineering attacks can be classified into two categories: direct and indirect [61]. A direct attack means it requires a physical contact or an eye contact or a voice interaction, or even the attacker's presence in the victim's working area to perform the attack. On the other hand, an indirect attack means that the attack does not require the attacker's presence to launch an attack.

Examples of social engineering attacks and their definitions are as follows:

- Phishing: phishing attacks aim to extract confidential information from the target through emails or phone calls.
- Baiting: a baiting attack involves creating a trap for the targeted victim.
- Tailgating: a tailgating attack involves physical access as the attacker follows the target with security access to a restricted area to have access to that area.
- Pretexting: a pretexting attack aims to steal the target's personal information by creating fake scenarios

A phishing attack is one of the most common social engineering attacks [62]. A report by ForgeRock [63] stated that the most common attack method was phishing in 2020, with 25% of all attacks in the US. By using phishing, the attacker could make the victims click on the designated website and download malware that could harm their computer [64].

Alrawi *et al*. [33] grouped smart home components into four categories: device, mobile application, cloud endpoint, and communication. In each component, there are different attack vector. In smart home devices, there are three attack vector which is vulnerable services, weak authentication, and default configuration. In mobile application, there are permission, programming, and data protection as attack vector. In cloud endpoint, the

attack vectors are vulnerability services, weak authentication, and encryption. Lastly, there are only two attack vectors in communication: encryption and MITM (man in the middle).

First, the smart home device is an essential part of the smart home, so that is one of the reasons why most of the smart home research focuses on the device.

The definition of each attack vector in a smart home device is as follows:

- Vulnerable services mean vulnerabilities in the running services in the device.
- Weak authentications mean weak credentials that are easy to guess.
- Default configurations mean a device that runs default settings from the factory.

Next is the mobile application, where most smart home IoT devices are being controlled. The definition of each attack vector in a mobile application is as follows:

- Permission means that a mobile application that is over-privileged that violates the user's privacy.
- Programming, in this case, means that mobile application with vulnerable implementation or programming error.
- Data protection, in this case, means hard-coded sensitive information in the mobile application.

Communication is where the smart home devices communicate with each other.

The definition of each attack vector in communication is as follows:

- Encryption, in this case, refers to a lack of encryption or protocols that has weak encryption
- MITM (Man in The Middle) refers to the probability of a man-in-the-middle attack.

Cloud endpoints are the Internet components of smart home IoT. Vendors use the cloud to provide services to the end-users, such as remote control and alerts. Smart home devices and mobile applications work together to create a cohesive smart home IoT. However, it can also act as an additional attack point. The definition of each attack vector in the cloud endpoint is already discussed above.

Overall, Alrawi and colleagues' research [28] does not explicitly mention the most common attack vector in smart home IoT. However, the authors analyzed several kinds of literature

and grouped them into their respective attack vectors. As a result, they found that the most common attack vector in the smart home device and cloud endpoints is vulnerability, data protection is the most common attack vector for mobile applications, and encryption is the most common attack vector in communication.

Other researchers such as Heartfield *et al*. [65] grouped the smart home threat landscape into five main categories: communication medium, supply chain, sensory channel, side channel, and control software. In each of these landscapes, they can be divided into several categories. Communication medium refers to how devices, sensors, actuators, and applications communicate in a smart home. The communication medium can be divided into wired, wireless, and home Internet. Control software refers to how smart home devices are being controlled, monitored, and operated. There are four components of control software: Host OS, third-party apps, firmware, and workflow automation. The sensory channel refers to how data is collected in the smart home. There are three ways of sensory channels used in smart homes: voice, infrared, and ultrasonic. Supply chain attack vector refers to attackers taking advantage of the distribution or delivery of the smart home devices' software and/or hardware. For example, an attacker selling second-hand a smart lock online on Amazon with the device has already been infected with malware. A side-channel attack is launched by an attacker using information leakage from the cryptosystem [66]. The attack uses the electromagnetic emanations from hardware to gain knowledge about its system. There are two parts of the side-channel: EMA (electromagnetic emanations) and EMI (electromagnetic interference).

Capellupo *et al*. [67] mentioned that there are three attack vectors in smart home devices: authentication and authorization, network-based attacks, and malware attacks. First, authentication and authorization refer to the lack of protection in smart home devices. Developers often do not allow the change of default configuration, enabling attackers to brute force the device's password. Furthermore, most end-users set a guessable password on their devices because manufacturers do not enforce password policy. Next, network-based attacks refer to attacks that take advantage of devices connected to the Internet. Because of the lack of processing power and memories that smart home devices have, the data that is being shared is often unsecured. Lastly, malware attacks are malicious software

designed by cybercriminals to steal and damage data or destroy computers and their systems.

Capellupo *et al*. and Heartfield *et al*. showed and described the attack vectors in their research. However, they did not specify what attack vector commonly occurs in a smart home. On the other hand, Kaspersky [68] had listed their findings on common attack vectors on companies' infrastructure, which are:

- Brute force attack is a method where an attacker trying to guess a password by trying all possible combinations of characters [69]. Brute force attack is the highest number percentage in organizations, with 31.58% of reported cases.
- Exploitation of publicly accessible applications is a method of attack that exploits vulnerabilities. The attack is primarily caused by companies' failure to install patches. This type of attack has the same percentage as brute force attack with 31.58% of cases.
- Malicious e-mail attacks can be launched with malware attached or through phishing. It was reported that malicious e-mail has 23.68% of reported cases.
- Drive-by compromise is an attack where an attacker gains access to a system through the website that users visit regularly. To launch this attack, hackers trick the users into downloading the malware or attaching a malicious code on the website that exploits the browser vulnerability. It was reported that drive-by compromise has 7.89% of reported cases.
- Portable drivers and insiders were tied with 2.63% of cases. The use of USB to launch an attack on a company has become rare and not reliable. Insiders mean employees that want to harm their own companies.

2.4.4. Proof-of-concept attacks

In Li's book [70], he mentioned that there are many ways to attack smart home devices. Some attacks require physical access to the smart home device, making it difficult to attack. However, other attacks can happen without having the requirement of physical access, meaning they can be done remotely.

There are many examples of attacks done by researchers to exploit smart home vulnerabilities. Some researchers tried to exploit the security of smart home devices from

the hardware itself. One researcher named Chapman researched a LIFX light bulb. LIFX light bulb is a light bulb that can be controlled via Wi-Fi equipped devices such as a smartphone. He tried to hack into the light bulb by obtaining the firmware from the physical chip [71]. Another researcher also made a similar attack on the LIFX light bulb. A researcher named LimitedResults tried to get the firmware of LIFX from the chip stored inside the bulb [72]. He and Chapman found that the LIFX light bulb could be hacked and obtain Wi-Fi credentials.

Ur *et al.* [73] did a research on Philips Hue. Philips Hue's lighting system can be controlled via smartphone or website because it is connected to the Internet. Ur and his colleague have proven that guests of the owner of the Philips Hue that have physical access to the Hue and the home's Wi-Fi network can control the Hue without the owner noticing [73]. A guest only needs to download the Hue app and "simply needs to press a button on the base station to pair that instance of the app with the Hue system permanently" [73, p. 3]. August smart lock also had a similar vulnerability as guests can take control of the smart lock. Wollerton [74] proves that by having physical access to the smart lock, a guest can enroll in a new key and gain full access to the smart lock.

The positive side of physical access attack is that the attacker needs to gain physical access to the device. However, it is still dangerous as once an attacker gains access to the physical device, they can further escalate the attack. Kavalaris and Serrelis [75] proved that in their research. They found that you can alter the firmware of a device to spread malicious viruses or leave a backdoor [75].

Next, Bitdefender [76] tried to hack into the August smart lock. August smart lock is a lock that is connected to Wi-Fi and can be controlled with a smartphone or smartwatch, similar to a LIFX light bulb. Bitdefender found that the smart lock is unencrypted, causing it to be easy to get its Wi-Fi credentials. A similar case also happened in Ring Doorbell. Bitdefender [77] also hacked into Ring Doorbell. Ring Doorbell Wi-Fi connection was unencrypted, so it was easy to get the Wi-Fi credentials.

Obermaier and Hutle [78] did a research on cloud-based surveillance systems. They research on four types of cameras that are connected to the cloud server and offer video streaming features using the Internet. The authors found that camera A and B credentials are not disclosed to the users and cannot be configured unless users access it through the cloud

service, while cameras C and D require login credentials. Furthermore, there was no authentication needed from cameras A and B when they were trying to connect to the cloud server, which indicates a big security design flaw in both cameras because it enables remote attacks.

Other researchers, Kavalaris and Serrelis [75], found that Sonos Wi-Fi access is vulnerable to attack. They found that they could obtain the Wi-Fi password and its hidden SSID by using a rooted android device. However, one specific attack is really dangerous, called key reinstallation attacks (KRACKs). One researcher stated that KRACKs is dangerous because "the attack works against all modern protected Wi-Fi networks" [79], meaning that a Wi-Fi network in a smart home could be exploited using KRACKs. Furthermore, the researcher stated that "if your device supports Wi-Fi, it is most likely affected" [79]. This means that the wireless access point could be affected, and all the smart home devices that could connect to the Wi-Fi network.

2.4.5. Reported attack incidents

According to ForgeRock [63], unauthorized access was the most common type of breach in the US, with 43% breaches and an increase of 450% attacks involving username/password totaling 1.48 billion in 2020. Furthermore, according to a report by Avast in 2019 [80], a security camera is one of the top five most vulnerable smart home devices in the US, Canada, and Australia.

Smart cameras are a great tool to keep an eye on the surrounding of the user's home. However, the cameras can also be hacked by an attacker through the Internet. According to Statista [81], 28% of the US participants were worried that they were being spied on through smart home devices. In January 2019 [82], a NEST camera was hacked and caused panic in the family as the attacker trolled the homeowners by saying that North Korea had launched missile attacks at the US. The most recent report about a hacked camera was in April 2022 [83] when an attacker hacked into a Ring camera and disturbed a 3-year-old child.

Forbes reported a case of a family getting insulted through the baby monitor [11]. The family used an IP camera from Foscam, and it has two-way audio and is compatible with a smartphone. However, the camera had a vulnerability in its firmware, as proven by Shekyan and Harutyunyan [84] in their research, and a random stranger took advantage of it. The

camera owned by the family had a feature called “remote internet monitoring from anywhere in the world” and a proven vulnerability by researchers means that thousands of cameras in the United States (U.S) were vulnerable to the same attack.

One method known to be used to infect multiple devices in a smart home is using a botnet. Botnet is one of the primary ways to launch a DDoS attack. According to NetScout threat intelligence report [85], there was a total of 9.7 million DDoS attacks in 2021. Furthermore, the number of botnet attacks increased by 23%, from 2,656 in Q3 to 3,271 in Q4 of 2021 [86]. There are two ways of how botnet spreads: first is through brute-forcing weak credentials, and second through unpatched vulnerabilities devices [87]. Many poor-quality IoT devices come with hard-coded credentials from the factory or default passwords that the end-users do not change, and even if the end-users change their passwords, they will most likely use passwords that are easy to guess. Moreover, many manufacturers do not spend a lot of money on security, with only 13% of the total budget spent by IoT organizations in 2018 [55].

In 2016, a botnet called Mirai took advantage of some insecurities in IoT devices and infected them [88]. Many IoT devices infected were unpatched older devices [64] and devices that still use default credentials from the factory or default username and password [89]. Mirai botnet used the infected IoT devices to run a DDoS attack on Krebs on Security, OVH, and Dyn. It was estimated that the Mirai botnet infected up to 600K devices, making it one of the biggest DDoS attacks ever. Wired [89] reported that the Mirai botnet was created by three people that wanted to make some money by hosting a gaming server in a game called Minecraft. Using the Mirai botnet, they can shut down competitors’ servers so that players would join their servers instead. However, the creators did not know that the botnet would grow so big and infect many devices.

In 2021, a new botnet emerged called Meris. Meris botnet primarily consists of networking devices such as IoT gateways, Wi-Fi access points, routers, switches, and mobile network equipment [90]. Meris was not as big as Mirai, but it was able to attack Yandex, one of the largest technology companies in Russia [91].

2.5. Mitigations and Solutions

The LIFX light bulb research done by Chapman [71] and LimitedResults [72] was sent to the LIFX company. As a result, LIFX made some adjustments to mitigate the attack from ever happening again.

Many of the problems stated in this literature review were already fixed by the manufacturers' update patch, such as the August smart lock case [74] and the Ring doorbell case [92]. In addition, Norton released 12 tips on how to make a more secure smart home: give your router a name, use a robust encryption method for Wi-Fi, set up a guest network, change default usernames and passwords, and use strong and unique passwords for Wi-Fi networks and device accounts, check the setting for your devices, disable features you may not need, keep your software up to date, audit the IoT devices already on your home network, do the two-step (two-factor authentication), avoid public Wi-Fi networks, and watch out for outages [93]. Smart home devices and networks should be more secure by following these tips.

Another solution is to use third-party security companies such as Kaspersky and Bitdefender. For example, Kaspersky announced a new product to protect smart home devices called “Kaspersky Smart Home Security” [94]. It has features such as detecting vulnerable network ports, protecting against brute-force attacks, blocking dangerous links and downloads, checking password strength, and restricting the Internet use [95]. To use Kaspersky smart home security, users need to contact their ISP and ask if they offer it.

Another company that offers smart home security is Bitdefender with its Bitdefender Box product. Bitdefender Box secures devices that are connected to the home network. Bitdefender Box filters the outgoing and incoming traffic to block the access of threats that may harm the user’s network. In addition, Bitdefender Box offers web scanning, on-demand vulnerability assessment, brute force detection, anomaly detection, sensitive data protection, device management, exploit prevention, parental control, and local protection [96]. There are three ways of installing Bitdefender Box [97]. First, it can be hooked up to the user’s ISP modem and act as a router. Second, replace the existing router by turning off the router’s Wi-Fi network and use the Bitdefender Box instead. The third method is by using bridge mode, meaning users still use their router’s network, but the Box added protective measures on top.

Another example of smart home security devices offered by security companies is Norton Core [98]. Norton Core is a wireless router that protects the home network. Norton Core offer features such as network security, device security, parental control, etc. Norton Core can be installed by connecting it with the existing router, or it can act as a router.

Trimananda *et al*. [99] investigated Norton Core and Bitdefender Box. The authors found that Norton Core and Bitdefender Box only defend against attacks that come from outside. Norton Core and Bitdefender Box considered devices inside the local network safe and trusted, allowing them to generate traffic with one another in the local network. Therefore, they do not defend against attacks that come from compromised local devices.

2.6. Smart home security responsibility

It is difficult to determine who is responsible for smart home security because many parties contribute to the technology. The attack that happened in the smart home can be blamed on cybercriminals because they keep exploiting the system. However, attackers exploit the design flaw because of manufacturers' sloppiness and the tardiness of consumers in updating their software [100]. Some of the defects in IoT devices come from bad design, such as devices that do not have a standard user interface that lets users change passwords easily [101]. There is also a survey on where the government should put IoT security regulations, such as the security method that is used for data storage [55]. So, it is not that simple to determine who is responsible for the security in the smart home. To further compare the results of this thesis, related research will be discussed about the general security and privacy responsibility.

Gross and Rosson [102] did a research and asked who was responsible for securing IT to 12 participants. The answers given by participants could be grouped into three categories which are technical, organizational, and social. The technical answers believed that the security responsibility falls on the IT professionals that work in an IT company, and there were 7 participants that thought so. There are 4 participants that believed the organizations or manufacturers are responsible for the IT security. The social perspective is a balance between technical and organizational while also putting end-users as an essential role in security. There was only 1 participant that answered with a social perspective.

Mozilla [103] conducted a survey in 2017 and got almost 190,000 respondents around the globe and asked, “Who is most responsible for protecting the online safety, privacy, and security of the connected apps and devices you own?". The results showed that 34.5% of people believed that the responsibility is in the individuals, and roughly the same amount with 34% believed it’s the manufacturers' responsibility. With 20.5% of respondents thought that the government was responsible, while 11% were unsure who was responsible.

Haney *et al*. [104] did a research on smart home responsibility with 40 smart home users. Regarding personal responsibility for the smart home security, the authors found that there was a total of 28 participants that believed that users had personal responsibility for security, with 21 respondents believing that the responsibility is shared with other parties such as the manufacturers and government. 30 participants felt that manufacturers had responsibility for security with 24 of them believed that its shared responsibilities with other parties such as the government and users. Finally, 5 participants thought that the government is responsible for security shared with other parties.

Overall, a lot of results showed that manufacturers are the most responsible. Research by Mozilla and Haney *et al*. showed that users are the second most responsible for security. However, no participants in the discussed study were found as experts in cybersecurity in IoT. Asking experts in cybersecurity in IoT would add more perspective and insight to this discussion. So, further interviews will be needed.

3. Methodology

3.1. Methodology approach

This study uses different types of information, which is from literature, interviews with experts, and a survey. Theoretical knowledge is already existing knowledge and can be found in the literature and the review has been done in chapter 2. It gives information on the research scope and helps provide direction for the interview questions. Then, experts were interviewed to ask for their opinion and insights. Additionally, a survey was conducted to see users' opinions on smart home security.

An interview is one of the methods in qualitative research. Interviews are used as the data source because they contain the interviewee's thoughts and opinions. There are three types of interviews for research: structured, semi-structured, and unstructured [105]. The semi-structured interview method is chosen because it allows "both interviewer and interviewee to discuss some topics in more detail" [105, p. 2]. In addition, the interviewer has the freedom to ask further questions and clarifications about the interviewee's initial response.

A survey is one of the primary methods in quantitative research. Quantitative research focuses on collecting data and generalizing it across groups of people [106]. In addition, the data gathered from the survey could be used to compare the data from the interview.

3.2. Data-collection method

3.2.1. Interview

The expertise that is required for the interviewees was either individuals who work in IoT companies as cybersecurity experts or researchers who had done research about smart home IoT security. Experts' contacts were found from LinkedIn, references of used literature, and personal contact of interviewed experts. Before conducting the interview, the researcher sent an e-mail to experts to ask if they would like to participate in the interview. Furthermore, the list of questions was sent with the e-mail so that the participants know what to expect from the interview and will have time to prepare to answer. The questions asked will be the same for every expert, thus allowing consistent data to be analyzed. If the participants were willing to participate, the interview date would be decided. The interviews were conducted via Zoom and MS Teams due to geographical limitations.

16 respondents agreed to be interviewed. At the beginning of the interview, the researcher read the interview procedure, such as the research topic, duration of the interview, how the data will be processed, and the confidentiality of the data. The language used for the interview was English, as many of the participants were from different countries.

The questions that were asked in this interview:

1. How many years of experience do you have in cyber security or in IoT?
2. What is your role in your organization or company?
3. What is your opinion on the current state of smart home technology?
    a. How did smart home technology change over the last five years?
    b. What changes have you observed in the field with respect to smart home security?
4. What developments do you foresee in the smart home security area in the next 5 years?
    a. Which of these developments would you consider most relevant to your own role, and why?
5. What do you think is currently the most likely attack vector in a smart home?
6. Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? For example, August smart lock, LIFX, and Foscam
    a. Why or why not?
7. What are the most frequently reported security incidents that you know of, or you've experienced?
8. What vulnerability do you think is the most dangerous in the smart home systems?
9. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box
10. Who is more responsible for smart home security?
    a. Manufacturers
    b. Consumers
    c. Government

d. Security industry

11. Would you like to add something?

The first two questions are about the experts' background, years of experience, and roles in their organizations. Question 3 inquires the experts' opinion about the current state of smart home, how the technology changes, and what changes they have observed. Question 4 is to ask experts about smart home security in the future. Question 5 is to answer the sub-question number 2 as to be precise, "What attack vector is the most common in smart home?". Question 6 asks if some attack done by researchers could emerge in real development. Question 7 asks experts about any incident they have experienced or their knowledge about an attack incident.

Question 8 is to answer the sub-question number 1 as to be precise, "What is the most dangerous vulnerability in the smart home? ". Question 9 asks experts how a third-party security company could improve smart home security and help answer the sub-question number 3 as to be precise, "What are the advantages and disadvantages of implementing security devices in a smart home?". Question 10 is the same as the sub-question number 4: "Who is the most responsible for smart home security." The last question is asked to experts if they wanted to express other ideas or opinions but could not because it is was not explicitly requested.

The main research question of this study is, 'What are the security challenges in a smart home IoT?' To answer the main research question, vulnerabilities in the smart home need to be explored. The literature review has already been given about types of attacks and vulnerabilities. However, expert insights are required to provide a more practical perspective. After that, solutions can be proposed based on the experts' opinions and literature.

Interview analysis

The interview research method is iterative, so the data is analyzed several times and better understood.

The interviews were recorded using Nvidia Share. During an interview, notes were written at the same time as experts answered the questions. After that, the data was organized and stored securely. The data was labeled without attaching the interviewees' names and stored

securely to maintain confidentiality. The recorded interview sessions were transcribed manually by the interviewer. After transcribing each interview and reading the transcript, they will be analyzed. QDA Miner, a qualitative analysis software, was used to help with analyzing the transcript.

3.2.2. Survey

Participants required for the survey were users with smart home devices installed in their homes. The survey questions were created using Qualtrics[4] and logged in using the researcher's Leiden University account. After that, the survey was conducted online through multiple platforms. First, the survey was sent to a website called SurveyCircle[5] for approximately two days to be answered by the public, from June 10, 2022, to June 11, 2022. Then, the researcher paid a considerable sum of money to a website called CloudResearch[6] for it to be answered by the public for roughly two days, from June 11, 2022, to June 12, 2022. These websites are two of many websites where researchers could submit their surveys and have them answered by the public or by specific participants that the researchers set.

The list of questions for the survey can be seen below:

1. What is your gender?
    a. Male
    b. Female
    c. Other
    d. Prefer not to say
2. What is your age?
    a. Under 18
    b. 18-30
    c. 31-45
    d. 46-60
    e. Above 60
3. What is your education level?
    a. Middle school diploma
    b. High school diploma
    c. Bachelor's degree
    d. Master's degree
    e. PhD or other similar

[4] https://www.qualtrics.com/uk/
[5] https://www.surveycircle.com/en/
[6] https://www.cloudresearch.com/

4. What industry are you working in or studying for?
    a. Telecommunication
    b. Education
    c. Health care
    d. Other industry
5. Which country do you currently reside?
6. How long have you been using smart home technology?
   By smart home technology, we mean devices that could communicate with each other and connected to the internet to help you in your daily activities, such as Smart TV, home assistants (Google Home, Alexa, etc.), smart thermostats, smart light, smart cameras, etc.
    a. Less than 1 year
    b. 1-3 years
    c. 3-6 years
    d. More than 6 years
7. Have you ever got hacked?
    a. Yes
    b. No
8. If you ever got hacked, what device(s) got hacked?
   You can select multiple answers
    a. Camera
    b. Thermostat
    c. Light
    d. Smart assistant
    e. Others
9. There are security devices (Bitdefender Box 2, Norton Core, and Kaspersky smart home security) that could improve the security in smart home devices but still lacking because it could only detect the connection to the internet but not connection between devices in a smart home. Knowing that, would you still buy one?

    a. Yes, why?
    b. No, why?
10. Who do you think is responsible for the security in smart home?
    a. Manufacturers, why?
    b. Users / owners, why?
    c. Security industry (security companies, researchers, etc.), why?
    d. Government, why?
    e. Others, why?

A total of 129 participants entered the survey, but 111 finished the survey. Some of the answers had less than 111 respondents in some questions. Mainly in question 10 where there were only 72 participants. The questions consist of 10 questions. The first five questions were general questions about the respondents' demographic: gender, age, education level, working industry, and country of residence. Question six asked how long the participants had used smart home technology. Question seven asked if the participants ever got hacked, and question eight asked what devices got hacked. Questions seven and eight were asked to see if they could support the interview question number seven from the experts: "What are the most frequently reported security incidents that you know of, or you've experienced?". Question nine asked if they would buy security devices or services to install in their home even though they know if it has limitations. Question ten asked who is responsible for smart home security. This question is essential to see if the survey answers are the same as the interview with experts.

Survey analysis

The survey analysis was performed using the method of filtering on the Qualtrics website. In addition, Qualtrics has the visualization of the survey, which helps in understanding the data.

3.3. Ethical consideration

For this thesis, no smart homes or any devices were hacked. However, some experts that were interviewed have experience in this field.

All interviews were recorded using Nvidia Share, and all participants gave consent. Experts will stay anonymous even after the interview is finished. The interviews lasted from 30 to 60 minutes, and all recorded interviews will remain confidential.

The transcripts can be found in the Appendix 1 without personal information.

4. Results

This chapter will show the results of the semi-structured interviews and survey.

4.1. Interview

4.1.1. Interview demographic

The 16 participants were interviewed online because of demography. The semi-structured interviews lasted an average of 43 minutes. Most of the participants were researchers that had done research on IoT security. The minimum level of education of the participants was a master's degree. All of the experts that were interviewed were male. The minimum level of experience in cybersecurity or in IoT are five years. The experts that were interviewed are from USA, Italy, Australia, Ecuador, Netherlands, UK, and Belgium.

Here is the table of participants with a code name, years of experience, positions, and country

Code Name	Years Of Experience	Role	Country
INT 1	7 years	researcher	USA
INT 2	6 years	researcher	Italy
INT 3	6 years	researcher	UK
INT 4	8 years	researcher	UK
INT 5	6 years	researcher	Australia
INT 6	5 years	researcher	Ecuador
INT 7	10 years	researcher	Australia
INT 8	10 years	researcher	Sweden
INT 9	10 years	researcher	Ecuador
INT 10	6 years	product owner	Netherlands
INT 11	15 years	researcher, consultant	UK
INT 12	20 years	retired researcher	Australia
INT 13	11 years	researcher	USA
INT 14	6 years	researcher	Belgium
INT 15	20 years	managing director	Belgium
INT 16	13 years	application security engineer	USA

Table 1. Research Participants

4.1.2. Interview findings

This section will explain each question and the answers given by participants.

Experts' opinion on the current state of smart home technology

a. How did smart home technology change over the last five years?

The smart home has changed a lot over the last five years, and more devices have come out with different functions and features. Expert number 3 added that the smart home devices change for the better and not as clunky as 5 years ago. However, the smart home technology itself is still not mature yet because the smart home devices can only control a few parts of the house instead of full automation of the home. Interviewee 15 stated, "*[the smart home devices] are like some kind of gadgets. They have some limited functionality, […] [and] it's not integrated in the whole building*".

b. What changes have you observed in the field with respect to smart home security?

Some experts believed that manufacturers focused on making new devices with new features and did not take security as a primary priority, as stated by expert number 7 "*[manufacturers] far more focus on features and new product releases, and far less focus on security*". There was also a gap in smart home security as big manufacturers can build a more secure device because they have the money and resources. In contrast, smaller manufacturers do not have as much money and resources. Interviewee 13 stated, "*the big companies have hundreds of engineers that are dedicated to work on the product […] but start-ups do not have those resources*". On the other hand, there was an increase in awareness of security and privacy concern, as stated by interviewee 1 "*there are more awareness of security and privacy*". Interviewee 14 supports this idea by saying "*people are more concerned about the security and privacy*".

Experts' opinion on future development in the smart home security are in the next 5 years

a. Which of these developments would you consider most relevant to your own role, and why?

The answers given by experts were varied. Some experts say there will be security standards and requirements in the future, implementation of blockchain, homomorphic encryption, the use of 5G as smart home security, and new security rules and policies from the government. Interviewee four pointed out that there will be more products for cyber security in IoT in the future, particularly from big companies. Moreover, expert 6 believed that password-less security would be implemented in smart home devices. Some experts believe that security awareness will increase, thus forcing manufacturers to build more

secure devices, which stated by interviewee 10, "*[consumers] will demand security on smart home devices*". Furthermore, expert 15 believed that users need to be educated by stating "educate the users to make sure that they [do] not buy devices recklessly ". Some interviewees believed that security would get better, and the quality would improve. However, interviewee 13 argued that security would not improve significantly by stating, "*I do not know if the security will improve. I think, for some devices it will improve […] For start-up company getting a product out in the market, having it visible in front of the customer is a higher priority than actually securing it*".

Experts' opinion on the most likely attack vector in a smart home

The answers given by experts were varied. Multiple experts pointed out that smart home devices have bad security design, thus enabling large-scale attacks such as a botnet attack as stated by one of the experts, "*[manufacturers] do not consider the security that much. So, it's causing a lot of problems such as Mirai botnet* ". Other experts mentioned unpatched vulnerabilities in older devices and cheap uncertified devices.

Another attack vector mentioned by experts was network access or wireless access. Expert 2 was one of the participants that answered wireless access because "*no physical medium that the attacker needs to access to be able to launch attacks*". Other experts mentioned that the human factor is the weakest link. Expert 8 stated, "*I think the most common one is the human factor*" and he answered the reason is because of weak passwords. Interview 6 supports this argument as he pointed out that users put too much trust in unknown people thus, he answered the question with social engineering. Expert 11 agreed with the view of participants 8 and 6 by stated "*I say that the attack in smart home nowadays is through the users because of the lack of education or guidance to the users*" Interviewee 9 could come up with a concrete answer and stated, "*I think in smart home, it's difficult to define the most common attack vector because in IoT*".

Experts' opinion on if some attacks reported by security researchers in the lab that they could think of emerge in real development. Given examples are, August smart lock, LIFX, and Foscam

All of the experts agreed that it could happen. Some experts believed that some attacks that could happen in the lab are not common to occur in actual development because they are hard to replicate in real life. However, expert 2 believed that it can act as a warning so that

countermeasures can be found. Furthermore, some experts believed that attack on smart home devices depend on how committed and what budget the attacker has so attacker can earn some money. Expert 1 pointed out that there are two perspectives in this field; first, the vulnerabilities are not known until the researchers find them, and the attackers exploit the vulnerabilities after that. Second, the vulnerabilities are already being exploited by attackers but were not known by the public until researchers found them. Additionally, participant 14 believed that when researchers found vulnerabilities and disclosed them to the manufacturer, there is a possibility that the manufacturer will not fix the vulnerabilities because it's too expensive as he stated "*Sometimes, research communities found about vulnerabilities and found solutions to improve the security but unfortunately, most of the manufacturers do not implement on what researchers found in the lab*"

Experts' opinion on the most frequently reported security incidents that they know of, or they've experienced

The answers given by experts were varied. Multiple experts mentioned Denial-of-Service, where attackers make the smart home devices stop working. Furthermore, some experts mentioned the use of botnet to launch a DoS attack, such as Mirai botnet. Other experts said cameras are the most reported security incidents as expert 12 stated the reason, "*it's pretty easy to see what people are doing in their smart home [using] the cameras*". Expert 1 pointed out that users complain about privacy more than security as he stated the reason "*a lot of these devices collecting personal information*". Other experts also mentioned about ransomware, unauthorized user, services that run on the device, banking fraud, and hardcoded credentials in the device itself.

Experts' opinion on vulnerability that is the most dangerous in a smart home systems

The answers given by experts were varied. Multiple experts said that Remote Code Execution (RCE) type of attack is the most dangerous. Expert number 5 mentioned the reason why RCE is dangerous by stating, "*I [can] just send you some package and then I can have full control of your devices*". Some experts mentioned any attack that could lead to physical consequences because nothing is more critical than safety risks. Others stated poor credentials or lack of authentication, not updated firmware, and privacy concerns.

Experts' opinion if a third-party security company devices could help consumers improve security. Given examples, Norton core, Kaspersky smart home security, Bitdefender box

Most experts support the production of security devices. However, expert 1 mentioned that one of the reasons smart home devices do not have anti-virus is because they are small devices with limited resources, so it's hard to program them. He further argued that it uses a blacklisting method, which is not a new solution, and the blacklists need to be updated regularly. Furthermore, participant 2 added that security companies need to invest in research because attackers are getting smarter and can find new ways of attack. However, some experts agreed that the security that the devices offer is lacking because those devices can only monitor on a network level and not the smart home devices themselves. Furthermore, security devices can also be hacked as they are also considered smart devices. Many experts also mentioned privacy concerns because the security companies could also collect users' private data by connecting to smart home devices.

Experts' opinion on who is more responsible for smart home security and rank them. Given options; manufacturers, consumers, government, security industry

Most of the experts agreed that manufacturers should be the most responsible as they are the ones that build smart home devices. The security industry comes second as they should support manufacturers. Interviewee 11 stated, "*the security industry is the one that proposed security solutions to the devices*". Government comes third. Many experts believed that government needs to push manufacturers to produce smart home devices with better security by imposing minimum security standards. In addition, privacy policies should be implemented so that manufacturers know what kind of data they can collect. Finally, consumers ranked fourth as they mostly do not have technical knowledge. However, three experts answered without any ranking and stated that everyone should be responsible.

Experts' additional opinion

Some experts said people need to be more careful about what we share online as privacy and security are both critical. There are no easy solutions to problems regarding smart home security. Although, a lot of people think that smart home attack is not a real issue. It is suggested that Blockchain and AI will be used a lot in the future. Interviewee 5 added that the smart home security is a good ecosystem as it keeps researchers have a job by researching attacks and consumers buying security devices to be more secure.

4.2. Survey

4.2.1. Survey demographic

There were 111 complete answers, and the researcher decided to also analyze incomplete answers, which had 129 participants in the survey. The average time spent by respondents to complete the survey was 5 minutes. Most of the participants were women aged 18 to 30 years old. The majority of respondents' education levels were high school graduates, and most of them were not working in the given options industry. Finally, the majority of the respondents were from the USA. Further details of the demographics can be seen in Table 2.

	Percentage
Gender	
Male	27.91%
Female	72.09%
Age	
Under 18	0.78%
18-30	40.63%
31-45	35.16%
46-60	12.50%
Above 60	10.93%
Education level	
Middle school	3.91%
High school	64.84%
Bachelor’s degree	24.22%
Master’s degree	6.25%
PhD or other similar	0.78%
Work industry	
Telecommunication	3.13%
Education	9.38%
Health care	17.19%
Other industry	53.91%
Retired	16.41%
Country of residence	
Azerbaijan	0.78%
Bangladesh	0.78%
Benin	0.78%
New Zeeland	0.78%
Turkey	0.78%
United States of America	96.12%

Table 2. Survey participants’ demographics

4.2.2. Survey findings

This section will explain the answers given by participants.

Duration of participants' have been using smart home technology

Respondents were asked how long they had been using smart home technology. The possible answers were less than 1 year, 1-3 years, 3-6 years, and more than 6 years. As shown in Figure 2, most of the respondents were users that had been using smart home technology for 1-3 years with 42.31%, followed by users that had been using it for more than 6 years, less than 1 year, and 3-6 years with 26.92%, 18.46%, and 12.31% respectively.

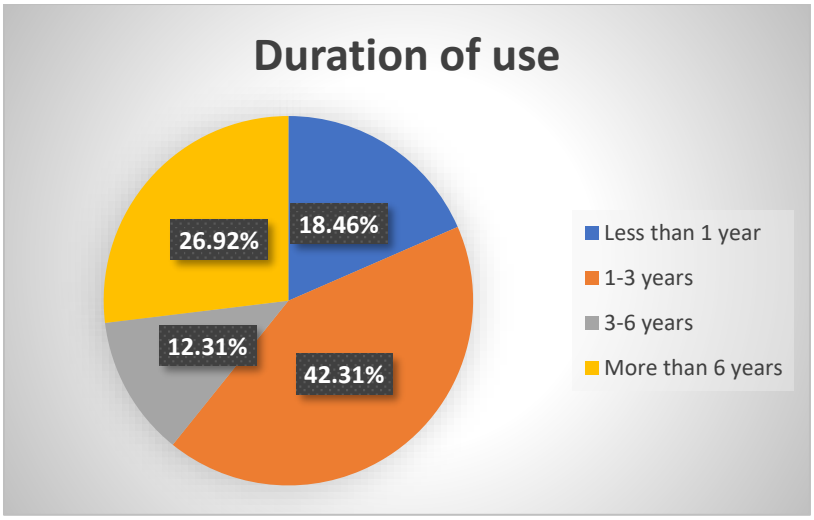


Figure 2. Duration of use

Hacked incident

Participants were asked if they ever experienced getting hacked using smart home devices. 65% of participants answered with 'no', while 35% answered 'yes' as seen in Figure 3.

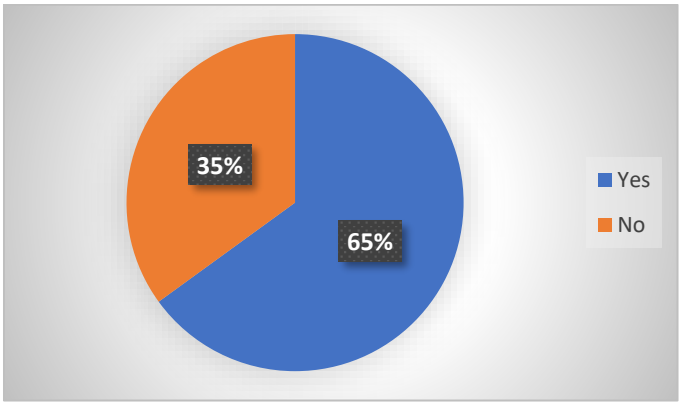


Figure 3. Experience hacked

For participants that had been hacked, they could select multiple answers about what device(s) that got hacked. Most of the answers were cameras and smart assistants, with both getting 24.56%. The thermostat and light each also got 10.53%. Lastly, 29.82%

answered with others and wrote smartphones, computers, tablets, and social media accounts. Figure 4 shows the graph of devices that got hacked.

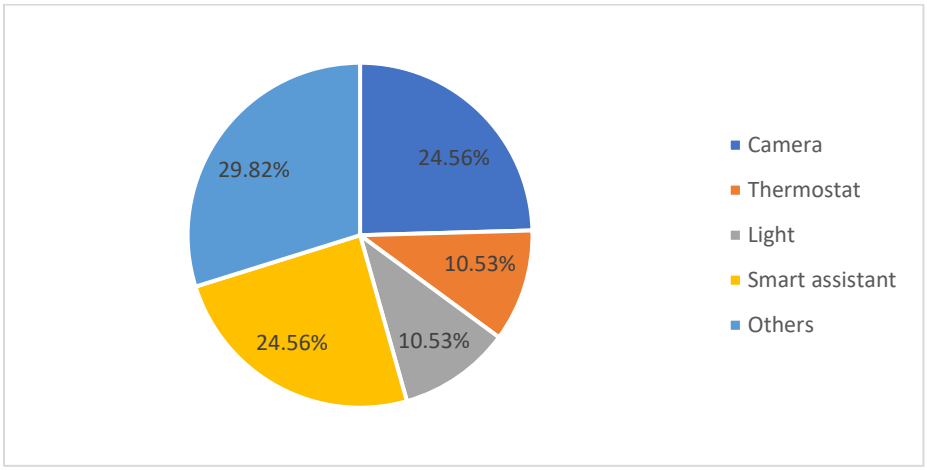


Figure 4. Devices that got hacked

Security devices

Participants were asked if they would buy security devices even though the security devices still need improvements, the responds was 47.59% '*yes*' and 52.41% '*no*' as shown in Figure 6. The main reason for the answer '*yes*' was that it still added security. Some respondents said that they need further information about the product to make a clear decision, but they still chose '*yes*'. On the other hand, participants answered with '*no*' because they do not really need it. One of the respondents that answered with '*no*' gave a reason with "I need more information to fully make a decision and trust [the security devices]"

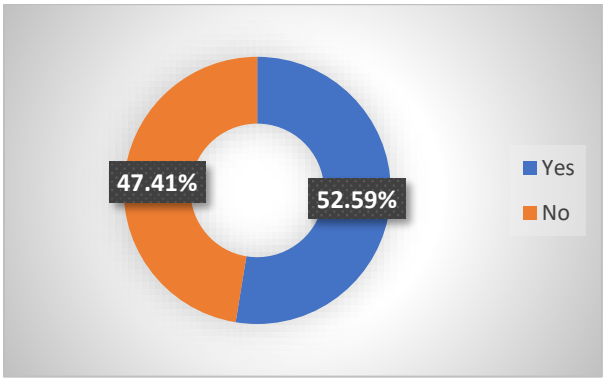


Figure 5. Security devices

Smart home security responsibility

The survey results showed that many participants believed manufacturers are responsible for smart home security, with 43%. The primary reason is that they are the ones that produced the smart devices. On the other hand, 28% of respondents believed that users are

responsible because they are the owner of the devices. 22% of participants chose the security industry as the one who is responsible because they are knowledgeable about security. 3% of respondents chose government, and 0% chose others. Figure 7 shows the graph of smart home security responsibility.

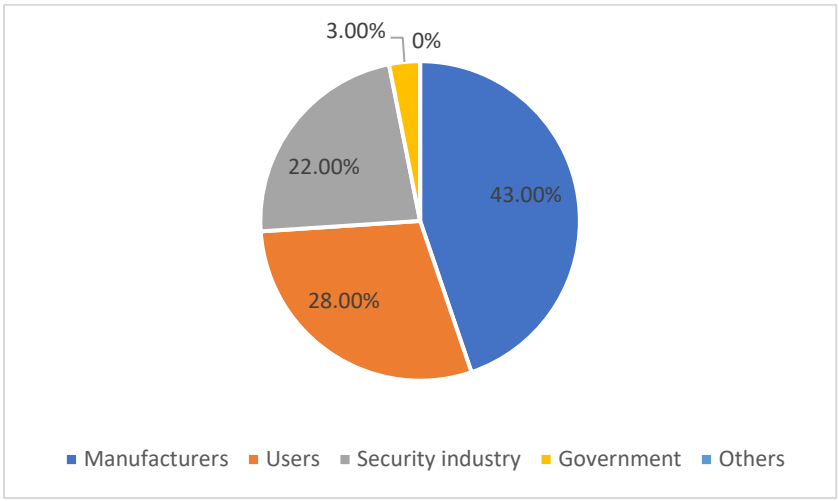


Figure 6. Smart home security responsibility

5. Discussion and limitation

5.1. Discussion

In this section, we will discuss further about the interview results posted to experts and break down into different topics following the sequence of the questions.

When experts were inquired about the most dangerous vulnerability, most of them mentioned RCE (Remote Code Execution) as it allows attackers to access and have complete control of the affected machine. RCE is part of arbitrary code execution, which is an attack that could be executed by injecting malicious code or malware into the device. A successful injection could lead to RCE attack and enables hackers to control a device remotely, such as a smartphone, as proven by Armis Lab [53]. One of the experts also mentioned that RCE type attack could also be a botnet attack. Mirai botnet is one of the botnet attacks where it compromised up to 600K devices, including smart home devices [88]. On the other hand, other experts believed that the most dangerous vulnerabilities are any attacks that could lead to a life-threatening impact. They said that nothing is more dangerous than safety risks. There were multiple reported attacks that took control security cameras and caused anxiety, such as the hack on Nest camera [82]. However, as of writing this thesis, no research that proved smart home devices could cause harm to human life. To answer the sub-question number 1, the answer would be RCE.

During interview sessions, experts were also requested to express their views about which attack vector is the most likely to take place in a smart home, and the provided answers by experts were varied. Attack in a smart home could happen because of many vectors. However, most of the answers alluded to network attack because it does not require a medium to launch. Experts also mentioned about attack vector that is caused by the human factor, such as social engineering. Phishing is one of the common examples of social engineering attacks because most users are susceptible to phishing attacks. If consumers fall for phishing attacks, then they are actually exposing themselves to remote control attack (RCE). Examples of RCE can be referred to in the previous paragraph (see discussion on sub-question number 1).

Similar to the views shared by experts, Kaspersky [68] also reported that the most frequent attack vector in organizations are brute force attacks and vulnerable applications. These types of attacks are carried out via network.

However, it is worth noting that not all brute force attacks have to be exploited through the Internet since they could also be performed offline [106]. On the other hand, vulnerable applications enable attackers to exploit a device remotely because the manufacturers are not patching the vulnerabilities. A botnet could take advantage of the unpatched vulnerabilities in a device and exploit the device. This is supported by some experts who stated that the most common attack was caused by companies that are not taking security as priority, further risking the security of the devices. To answer the sub-question number 2, the answer would be inconclusive, because there is no concrete evidence on what the most likely attack vector in a smart home is.

Discussion was reviewed together with experts about whether or not findings in the lab can also take place in real development. They all agreed that it could happen, especially in remote attacks that do not require physical access. The example of attacks found by researchers that could emerge in real development, such as August smart lock [74] and LIFX lightbulb [71], however, the possibility is relatively low because it requires attackers to have physical access to the device. There are slight differences in the experts' opinions on the manner and why the attack can happen. For an attack in real development to occur, there is a need for a business case where attackers will gain something from launching the attack, such as the Mirai botnet in 2016 [89], which was created to earn some money. Furthermore, experts pointed out that security cameras that researchers exploited in the lab could occur in real life. Forbes [11] proves this opinion, where the attacker took advantage of the published research to exploit a security camera. Multiple reported incidents of cameras getting hijacked summarized that the attackers' motive was to cause disturbance to the owners.

The experts had different answers when they were talking over the most frequently reported security incident they knew or experienced, and it can be concluded that Denial-Of-Service attacks are the most widely known ones. It was reported that there were 9.7 million DDoS attacks in 2021 [85]. Experts think that a DDoS attack is most likely to happen because many smart home devices utilize cloud services. Another example on reported incident as

per experts is hacked cameras. Avast [78] reported that cameras are the top 5 most vulnerable devices in smart homes in the US, Canada, and Australia. The attack on security cameras is supposedly very common as it is easy to do because there is a search engine called Shodan[7] that can find vulnerable cameras online with ease. The survey showed that 35% of users had experienced getting hacked. Furthermore, devices that got hacked the most are cameras and smart assistants as the most hacked devices with 24.56% each. In other words, experts' opinions about cameras as the most hacked devices are supported with the survey from the users.

From the interviews, experts also agreed that third-party security company products or services could improve smart home security and offer a great security solution to users with limited knowledge. However, they also admit that the security offered in these devices is very limited to just protecting the network traffic from the Internet and cannot monitor the connection traffic among the smart home devices. Research by Trimananda et al. [99] supports this opinion, where Norton Core and Bitdefender Box did not detect the traffic among devices in the local network. Furthermore, experts pointed out that since these security devices are smart themselves, then they are vulnerable to getting hacked. However, as of writing this thesis, no research supported that these devices could be hijacked. To sum up the answer to the sub-question number 3, there are advantages of protecting users and devices from the Internet, but there are still some issues since the local connection cannot be secured, and it has the possibility of being hacked. When users were asked if they would use security devices knowing they still need improvement, more than 50% of them would like to use them because it has added security value.

When experts were asked who is responsible for smart home security, the answers can be ranked into manufacturers, security industry, government, and consumers. The interviewees chose manufacturers as the most responsible because they are the ones that made the products. The responses provided by experts correlate with the previous research done by Gross & Rosson [101] and Haney et al. [103] because the manufacturers and third-party are the most responsible for the security and the government is partly responsible. However, there is a difference in experts' opinions with some previous research. A survey by Mozilla [102] and research by Haney et al. [103] showed that the consumers are one of the most

[7] https://www.shodan.io/

responsible about security, but experts thought that consumers do not have a high responsibility in smart home security because they have minimal knowledge about security. Furthermore, the result of the survey with users found that 43% of them said that manufacturers are responsible for the security of smart homes. The primary reason users gave was similar to experts' opinion, which is that they produced the smart devices. To answer sub-question number 4, it can be concluded that the literature does not support the answers given by experts and the survey with owners.

5.2. Limitations

One of the limitations of the interview in this study was the experts' background. Most of the experts were experienced in cyber security and IoT. Because of this, there is a possible bias towards the viewpoint of cyber security experts in the results. Furthermore, with a relatively small sample size of only 16 participants, there is a possibility of assuming as true a false premise [107]. The results could be different with a more significant sample and more participants with diverse backgrounds.

Another limitation is that the discussed attacks and solutions were not tested on a real smart home. Therefore, it implies that there is no proof if the attacks and solutions provided by literature or discussed by experts are accurate or not.

There is an ambiguity in some of the interview questions in questions 7 and 8. Question 8 stated, "What vulnerability do you think is the most dangerous in the smart home systems?" and some experts understood the word 'dangerous' as the impact it could bring to human life, and not the vulnerability of the device itself. In addition, question 7 asked about the opinions of the experts in the smart home. One expert answered beyond this research's scope, indicating an ambiguity in the question. Thus, there is a need to change of the wording of the questions to make sure that there is no ambiguity.

Question number 9 asked about third-party security company devices, and the researcher gave a few examples. However, it caused an issue where experts focused on the examples given, notably Bitdefender Box.

It is decided not to do a second round of interviews because of the availability of professionals for the interview, time limitations, and the amount of work to be done.

Furthermore, if a second interview round is conducted, the data will need to be analyzed and double-check where misconceptions could occur.

Some of the questions in the survey were not answered completely or left empty. For example, 129 participants answered question number one, but there were only 72 respondents in question ten. Therefore, the number of participants in some questions was not the same.

Some of the answers given by participants from the survey were not serious or left empty, such as “Jajszhjx”, and “Turn around like the one that says it is like the same height as you and your gay”. Thereby, the analysis of data was complicated.

There was a need for a further explanation in question 9 of the survey. Some of the respondents said they needed additional information to be able to give proper reasons.

5.3. Recommended solutions

The recommended solutions are provided by literature and interviews with experts. The following recommended solutions are aimed at manufacturers, users, and third-parties. Implementing the provided recommendation will improve the general security in the smart home.

5.3.1. Recommendation to manufacturers

- Expert number two stated that manufacturers need to invest in IoT security research to help find threat vectors so countermeasures can be developed.
- Vulnerabilities will inevitably discovered. Therefore, manufacturers should provide patches or firmware updates [48].
- Provide guidance to users. Manufacturers should give tips and guidance on how to configure their devices securely [104].

5.3.2. Recommendation to users

- Many experts mentioned that users need to change the default password when they buy smart devices.
- Botnet could exploit unpatched vulnerabilities, so users need to update their device regularly.

5.3.3. Recommendation to third-parties (security industry and government)

- Security companies and researchers could create a universal consensus or certification program for manufacturers to follow. IEEE [48] provided elements that the certification body should verify, which are:
    - Devices should not have weak protection or insufficient resources.
    - Follow the already proven protocols and use strong authentications.
    - The gathered data are handled and shared with care.
    - The used protocols should not leak information about the users beyond the limit of the intended use.
    - Certified providers should respond immediately to privacy issues
    - Provide devices with identifying labels where consumers could check the certification status of the device and device description.
- The government penalized manufacturers that did not follow the certification program.
- Government creates regulations that protect consumers' privacy and security and support manufacturers [104].

6. Conclusion and future work

6.1. Conclusion

In this conclusion, the main research question in the first chapter will be revisited and answers will be explained thoroughly. The main research question is

"What are the security challenges in smart home IoT?"

This research aimed to understand what challenges smart home IoT faces. There are many attack vectors and vulnerabilities in smart home IoT. This is caused by two factors: human carelessness and the flaws in the technology itself. First, end-users tend not to change the default passwords, or even if they change them, they usually reuse passwords or credentials that are easy to guess. The flaws in the technology itself are caused by manufacturers that do not take security as a priority and limit the budget for security during production. The most common attack vector is network attacks because it is easy to do as attackers can do it remotely from around the world. Furthermore, cameras can be hacked through the Internet to monitor users' activities or create a disturbance. The most dangerous vulnerability in a smart home system is RCE because attackers could take complete control of a device. Attackers could exploit a device because of the vulnerabilities in the device, such as weak credentials and poor authentication.

Security devices offered by security companies could help consumers secure their smart home devices. However, security devices have its limitation. It can only secure on the network level because the security devices only scan the traffic that is going in and out of the gateway. Furthermore, some experts believed the security devices could also be hacked as they are smart devices connected to the Internet. Additionally, there was a privacy concern pointed out by experts because the security devices read all the traffic that is in the home gateway. Thereby, some experts did not want to use the security devices personally in their homes, but they recommended it for consumers that do not have knowledge about security as long as users understand the privacy and security risks. However, more than half of the respondents from the survey want to use the security devices even though it is still lacking in security. The main reason was that the devices still added additional protection.

As to who is responsible for security in smart homes, the answers given by experts fall into manufacturers as number one, two is security industry, third is the government, and fourth is the consumers. Furthermore, the survey showed that manufacturers as the ones responsible for security, followed by users, the security industry, the government, and others. However, the answers given by experts and survey did not correlate with the literature as consumers should be one of the most responsible for the security in the smart home, according to Mozilla [103] and Haney *et al*. [104].

6.2. Future work

Based on the limitations of this study, there are a few points that are needed to improve it. These were

1. Interview extension
2. Survey extension
3. Practical validation of the findings

As mentioned in the limitations, some of the interview questions were ambiguous. Furthermore, the experts invited for the interview were from the same background. So, there is a need to conduct a second interview to address the ambiguity of the questions and conduct interviews with people from different backgrounds, for example, users who own smart home devices and government employees who know about IoT security, to generate additional insights.

Just as the interview needs an extension, so does the survey. There needs to be an additional option in a 'yes or no' question, which is 'I don't know'. Some respondents that could not make a clear answer could choose that option. Furthermore, as mentioned in the limitations, some answers given by participants were not serious, so a survey with a more serious audience would be better. Finally, the additional survey could be conducted to a more specific audience, such as smart home users that partnered with manufacturers or audience that works in security companies.

This study focused on analyzing the already existing literature and interviews with professionals. To understand better about the challenges in smart home, there is a need to conduct a practical test to see if some of the attack vectors and vulnerabilities in the discussed smart home devices still exist or not. Furthermore, there was no literature that

supports the sub-question number 2, so this could be a research question that could be done for further work. Additionally, there is a need to research the security devices to prove a point from the experts that security devices could also be hacked because they are also smart devices.

References

[1] K. S. Young, "Internet Addiction: The Emergence of a New Clinical Disorder," vol. 1, no. 3, pp. 237-244, 2009.

[2] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025," Statista, 27 November 2016. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Accessed 12 December 2021].

[3] R. Harper, Inside the smart home, London: Springer, 2003.

[4] Verified Market Research, "Smart Home Market Size And Forecast," Verified Market Research, [Online]. Available: https://www.verifiedmarketresearch.com/product/global-smart-home-market-size-and-forecast-to-2025/. [Accessed 12 December 2021].

[5] W. Ablondi, "2021 Global Smart Home Forecast - June 2021," Strategy Analytics, 29 June 2021. [Online]. Available: https://www.strategyanalytics.com/access-services/devices/connected-home/smart-home/market-data/report-detail/2021-global-smart-home-forecast. [Accessed 1 October 2021].

[6] K. Fu, T. Kohno, D. Lopresti, E. Mynatt, K. Nahrstedt, S. Patel, D. Richardson and B. Zorn, "Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things," *Computing Community Consortium,* 2017.

[7] V. Srinivasan, J. Stankovic and K. Whitehouse, "Protecting your Daily In-Home Activity Information from a Wireless Snooping Attack," *10th international conference on Ubiquitous,* pp. 202-211, 2008.

[8] A. Laughlin, "How a smart home could be at risk from hackers," Which?, 2 July 2021. [Online]. Available: https://www.which.co.uk/news/2021/07/how-the-smart-home-could-be-at-risk-from-hackers/. [Accessed 4 April 2022].

[9] A. D. Rayome, "DDoS attacks increased 91% in 2017 thanks to IoT," TechRepublic, 20 November 2017. [Online]. Available: https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/. [Accessed 16 May 2022].

[10] CISOMAG, "Hackers take over Smart Home," CISOMAG, 26 September 2019. [Online]. Available: https://cisomag.eccouncil.org/hackers-take-over-smart-home/. [Accessed 4 April 2022].

[11] K. Hill, "How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old," Forbes, 13 August 2013. [Online]. Available: https://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/?sh=178a2bfaaad6. [Accessed 12 November 2021].

[12] N. Bilton, "Nest Thermostat Glitch Leaves Users in the Cold," The New York Times, 13 January 2016. [Online]. Available: https://www.nytimes.com/2016/01/14/fashion/nest-

thermostat-glitch-battery-dies-software-freeze.html. [Accessed 16 May 2022].

[13] M. Hughes, "Hacker remotely raises home temperature 12ºC (22ºF) on smart thermostat," TNW, 21 July 2017. [Online]. Available: https://thenextweb.com/news/hacker-remotely-raises-home-temperature-12oc-22of-smart-thermostat. [Accessed 16 May 2022].

[14] CISA, "Understanding Denial-of-Service Attacks," Cybersecurity & infrastructure security agency, 20 November 2019. [Online]. Available: https://www.cisa.gov/uscert/ncas/tips/ST04-015. [Accessed 4 April 2022].

[15] Kaspersky, "Attack Vector," Kaspersky, [Online]. Available: https://encyclopedia.kaspersky.com/glossary/attack-vector/. [Accessed 14 December 2021].

[16] IBM, "Artificial Intelligence (AI)," IBM, 3 June 2020. [Online]. Available: https://www.ibm.com/nl-en/cloud/learn/what-is-artificial-intelligence. [Accessed 8 April 2022].

[17] A. Arampatzis, "Homomorphic Encryption: What Is It and How Is It Used," Venafi, 22 January 2020. [Online]. Available: https://www.venafi.com/blog/homomorphic-encryption-what-it-and-how-it-used. [Accessed 8 April 2022].

[18] NIST, "man-in-the-middle attack (MitM)," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/man_in_the_middle_attack. [Accessed 5 May 2022].

[19] CSA, "Matter," CSA, [Online]. Available: https://csa-iot.org/all-solutions/matter/. [Accessed 8 April 2022].

[20] Kansas State University, "Overview of Grey Literature and White Papers," Kansas State University, [Online]. Available: https://guides.lib.k-state.edu/c.php?g=181814&p=6804869. [Accessed 1 October 2021].

[21] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security and Mobility,* vol. 4, no. 1, pp. 65-88, 2015.

[22] P. Asghari, A. M. Rahmani and H. H. S. Javadi, "Internet of Things applications: A systematic review," *Computer Networks,* vol. 148, pp. 241-261, 2019.

[23] Y. Jie, J. Y. Pei, L. Jun, G. Yun and X. Wei, "Smart Home System based on IOT Technologies," *2013 International Conference on Computational and Information Sciences,* pp. 1789-1791, 2013.

[24] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures," *The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015),* pp. 336-341, 2015.

[25] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST),* 2015.

[26] F. K. Aldrich, "Smart Homes: past, present, and future," in *Inside the smart home*, London, 2003, pp. 17-39.

[27] T. D. P. Mendes, R. Godina, E. M. G. Rodrigues, J. C. O. Matias and J. P. S. Catalão, "Smart Home Communication Technologies and Applications: Wireless Protocol Assessment for Home Area Network Resources," *Energies, Vol 8,* pp. 7279-7311, 2015.

[28] European Commission, "REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT," Brussels, 2022.

[29] E. Zeng, S. Mare and F. Roesner, "End User Security & Privacy Concerns with Smart Homes," *the Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017),* pp. 65-80, 2017.

[30] D. Craigen, N. Diakun-Thibault and R. Purse, "Defining Cybersecurity," *Technology Innovation Management Review,* pp. 13-21, 2014.

[31] A. Arnbak, "Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives," 2015.

[32] A. Gerber and S. Kansal, "Top 10 IoT security challenges," IBM, 16 November 2017. [Online]. Available: https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/. [Accessed 4 May 2022].

[33] O. Alrawi, C. Lever, M. Antonakakis and F. Monrose, "SoK: Security Evaluation of Home-Based IoT," *2019 IEEE Symposium on Security and Privacy (SP),* 2019.

[34] J. M. Kizza , "Introduction to Computer Network Vulnerabilities," in *Guide to Computer Network Security*, Springer, 2017, pp. 87-103.

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

[36] H. Lin and N. W. Bergmann, "IoT Privacy and Security Challenges for Smart Home Environments," vol. 7, no. 3, p. 44, 2016.

[37] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman and M. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," *The Journal of Supercomputing,* p. 14053–14089, 2021.

[38] A. Gainer, "Smart devices could leave your home vulnerable to security threats," CBS News, 19 April 2022. [Online]. Available: https://www.cbsnews.com/newyork/news/smart-devices-hacked-security-threats/. [Accessed 21 May 2022].

[39] D. Bastos, M. Shackleton and F. El-Moussa, "Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments," *Living in the Internet of Things: Cybersecurity of the IoT - 2018,* 2018.

[40] Kaspersky, "What is Data Encryption?," Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/definitions/encryption. [Accessed 20 May

2022].

[41] S. Gürses and B. Preneel, "cryptology and privacy in the context of big data," *Exploring the Boundaries of Big Data,* pp. 49-85.

[42] W. Z. Khan, M. Zahid, M. Y. Aalsalem, H. M. Zangoti and Q. Arshad, "Ethical Aspects of Internet of Things from Islamic Perspective," 2018.

[43] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 3, pp. 2702-2733, 2019.

[44] A. Patel, N. Shah, D. Ramoliya and A. Nayak, "A detailed review of Cloud Security: Issues,Threats & Attacks," *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA),* pp. 758-764, 2020.

[45] M. A. Azzawi, R. Hassan and K. A. A. Bakar, "A Review on Internet of Things (IoT) in Healthcare," *International Journal of Applied Engineering Research,* vol. 11, no. 20, pp. 10216-10221, 2016.

[46] J. Max, "Backdooring the Frontdoor Hacking a "perfectly secure" smart lock.".

[47] S. Shiaeles, N. Kolokotronis and E. Bellini, "IoT Vulnerability Data Crawling and Analysis," *2019 IEEE World Congress on Services (SERVICES),* pp. 78-83, 2019.

[48] IEEE, "INTERNET OF THINGS (IOT) SECURITY BEST PRACTICES," IEEE, 2017.

[49] A. Keromytis, "a look at VoIP vulnerabilities," pp. 41-50, 2010.

[50] Kaspersky, "DoS (Denial of Service) attack," Kaspersky, [Online]. Available: https://encyclopedia.kaspersky.com/glossary/dos-denial-of-service-attack/. [Accessed 23 May 2022].

[51] T. Sommestad, H. Holm and M. Ekstedt, "Estimates of success rates of remote arbitrary code execution attacks," *Information Management & Computer Security,* vol. 20, no. 2, pp. 107-122, 2012.

[52] Kaspersky, "Remote Code Execution (RCE)," Kaspersky, [Online]. Available: https://encyclopedia.kaspersky.com/glossary/remote-code-execution-rce/#:~:text=One%20of%20the%20most%20dangerous,the%20device%20is%20not%20required.. [Accessed 14 May 2022].

[53] B. Seri and G. Vishnepolsky, "The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks," Armis, 2017.

[54] Kaspersky, "How we hacked our colleague's smart home, or morning drum & bass," Kaspersky, 1 July 2019. [Online]. Available: https://ics-cert.kaspersky.com/reports/2019/07/01/fibaro-smart-home/. [Accessed 12 December 2021].

[55] Gemalto, "The State Of IOT Security," 2019.

[56] B. Schneier, "The Internet of Things Is Wildly Insecure — And Often Unpatchable," Wired, 6 January 2014. [Online]. Available: https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/. [Accessed 8 May 2022].

[57] Kaspersky, "IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019," Kaspersky, 15 October 2019. [Online]. Available: https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019. [Accessed 8 May 2022].

[58] K. Hughes-Lartey, M. Li, F. E. Botchey and Z. Qin, "Human factor, a critical weak point in the information security of an organization's Internet of things," *Heliyon,* vol. 7, no. 3, 2021.

[59] F. Breda, H. Barbosa and T. Morais, "SOCIAL ENGINEERING AND CYBER SECURITY," pp. 4204-4211, 2017.

[60] M. Swanagan, "How To Prevent The Top Cyber Attacks In 2022," Purplesec, 27 November 2021. [Online]. Available: https://purplesec.us/prevent-cyber-attacks/. [Accessed 12 May 2022].

[61] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet,* vol. 11, no. 4, 2019.

[62] S. Gupta, A. Singhal and A. Kapoor, "A Literature Survey on Social Engineering Attacks: Phishing attack," *International Conference on Computing, Communication and Automation (ICCCA2016),* pp. 537-540, 2016.

[63] ForgeRock, "2021 ForgeRock Consumer Identity Breach Report," 2021.

[64] Kaspersky, "What is Social Engineering?," Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering. [Accessed 2 May 2022].

[65] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J. R. J. Fontaine, A. Filippoupolitis and E. Roesch, "A taxonomy of cyber-physical threats and impact in the smart home," *Computers & Security ,* vol. 78, pp. 398-428, 2018.

[66] NIST, "Side-Channel Attack," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/side_channel_attack. [Accessed 3 May 2022].

[67] M. Capellupo, J. Liranzo, M. Z. A. Bhuiyan, T. Hayajneh and G. Wang, "Security and Attack Vector Analysis," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, Springer International Publishing, 2017, pp. 593-606.

[68] Kaspersky, "Common initial attack vectors," Kaspersky, 7 October 2021. [Online]. Available: https://www.kaspersky.com/blog/most-common-initial-attack-vectors/42379/. [Accessed 3 May 2022].

[69] Kaspersky, "Brute-force," Kaspersky, [Online]. Available:

https://encyclopedia.kaspersky.com/glossary/brute-force/. [Accessed 27 May 2022].

[70] S. Li, "Security Architecture in the Internet of Things," in *Securing the Internet of Things*, United States, Todd Green, 2017, pp. 27-48.

[71] A. Chapman, "Hacking into Internet Connected Light Bulbs," contextis, 4 July 2014. [Online]. Available: https://www.contextis.com/us/blog/hacking-into-internet-connected-light-bulbs. [Accessed 1 October 2021].

[72] LimitedResults, "Pwn the LIFX Mini white," LimitedResults, 23 January 2019. [Online]. Available: https://limitedresults.com/2019/01/pwn-the-lifx-mini-white/. [Accessed 12 November 2021].

[73] B. Ur, J. Jung and S. Schechter, "The Current State of Access Control for Smart Devices in Homes," *Workshop on Home Usable Privacy and Security (HUPS),* 2013.

[74] M. Wollerton, "Here's what happened when someone hacked the August Smart Lock," cnet, 25 August 2016. [Online]. Available: https://www.cnet.com/home/smart-home/august-smart-lock-hacked/. [Accessed 12 November 2021].

[75] S. P. Kavalaris and E. Serrelis, "Security Issues of Contemporary Multimedia Implementations: The Case of Sonos and SonosNet," *The Proceedings of the International Conference in Information Security and Digital Forensics, Thessaloniki, Greece,* pp. 63-74, 2014.

[76] Bitdefender, "Cracking the August SmartLock: WiFi Password Eavesdropping Made Easy," Bitdefender, 2020.

[77] Bitdefender, "Ring Video Doorbell Pro Under the Scope," 2019.

[78] J. Obermaier and M. Hutle, "Analyzing the Security and Privacy of," *IoTPTS '16: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security,* pp. 22-28, 2016.

[79] M. Vanhoef, "Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse," 2017. [Online]. Available: https://www.krackattacks.com/. [Accessed 12 November 2021].

[80] Avast, "Avast Smart Home Security Report 2019," Avast, 2019.

[81] Statista, "Importance of smart home security & safety / Worried about being spied on through smart home devices 2021, by country," Statista, April 2021. [Online]. Available: https://www.statista.com/forecasts/1227824/smart-home-security-safety-vs-privacy-concerns. [Accessed 10 May 2022].

[82] M. Gafni, "“5 minutes of sheer terror”: Hackers infiltrate East Bay family’s Nest surveillance camera, send warning of incoming North Korea missile attack," Mercury News, 21 January 2019. [Online]. Available: https://www.mercurynews.com/2019/01/21/it-was-five-minutes-of-sheer-terror-hackers-infiltrate-east-bay-familys-nest-surveillance-camera-send-warning-of-incoming-north-korea-missile-attack/. [Accessed 12 May 2022].

[83] B. Linder, "Parents say they ditched their Ring camera after their 3-year-old son claimed a voice kept asking if he ‘wanted ice cream’ at night," Penn Live, 6 April 2022. [Online].

Available: https://www.pennlive.com/news/2022/04/parents-say-they-ditched-their-ring-camera-after-their-3-year-old-son-claimed-a-voice-kept-asking-if-he-wanted-ice-cream-at-night.html. [Accessed 12 May 2022].

[84] S. Shekyan and A. Harutyunyan, "To Watch Or To Be Watched Turning your surveillance camera against you," 2013.

[85] NetScout, "NETSCOUT THREAT INTELLIGENCE REPORT," NetScout, 2021.

[86] Spamhaus, "Spamhaus Botnet Threat update," Spamhaus, 2021.

[87] D. Palotay, "IoT Botnet Report 2021: Malware and Vulnerabilities Targeted," CujoAI, 17 December 2021. [Online]. Available: https://cujo.com/iot-botnet-report-2021-malware-and-vulnerabilities-targeted/. [Accessed 9 May 2022].

[88] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas and Y. Zhou, "Understanding the Mirai Botnet," *the Proceedings of the 26th USENIX Security Symposium,* pp. 1093-1110, 2017.

[89] G. M. Graff, "How a Dorm Room Minecraft Scam Brought Down the Internet," Wired, 13 December 2017. [Online]. Available: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/. [Accessed 9 May 2022].

[90] C. Cimpanu, "Meet Meris, the new 250,000-strong DDoS botnet terrorizing the internet," 9 September 2021. [Online]. Available: https://therecord.media/meet-meris-the-new-250000-strong-ddos-botnet-terrorizing-the-internet/. [Accessed 1 December 2021].

[91] Economist, "Yandex, Russia's biggest technology company, celebrates 20 years," The economist, 30 September 2017. [Online]. Available: https://www.economist.com/business/2017/09/30/yandex-russias-biggest-technology-company-celebrates-20-years. [Accessed 12 December 2021].

[92] N. J. Rubenking and M. Eddy, "Exclusive: Bitdefender Discovers Ring Doorbell Vulnerability," PCMag, 7 November 2019. [Online]. Available: https://www.pcmag.com/news/exclusive-bitdefender-discovers-ring-doorbell-vulnerability. [Accessed 30 November 2021].

[93] S. Symanovich, "12 tips to help secure your smart home and IoT devices," Norton, 28 August 2019. [Online]. Available: https://us.norton.com/internetsecurity-iot-smart-home-security-core.html. [Accessed 30 November 2021].

[94] Kaspersky, "Kaspersky Smart Home Security: the company announces new product to protect connected devices at home," Kaspersky, 6 September 2021. [Online]. Available: https://www.kaspersky.com/about/press-releases/2021_kaspersky-smart-home-security-the-company-announces-new-product-to-protect-connected-devices-at-home. [Accessed 30 November 2021].

[95] Kaspersky, "Protect smart home devices from hacking," Kaspersky, 6 September 2021. [Online]. Available: https://www.kaspersky.com/blog/how-to-protect-smart-home-devices/41617/. [Accessed 30 November 2021].

[96] Bitdefender, "Manual - Bitdefender Box," 16 January 2019. [Online]. Available: https://download.bitdefender.com/resources/media/materials/box/v2/user_guide/2020/BOX_UserGuide_v2_en.pdf?adobe_mc=MCMID%3D19000064854589797877726807793705579949%7CMCORGID%3D0E920C0F53DA9E9B0A490D45%2540AdobeOrg%7CTS%3D1641600000. [Accessed 13 May 2022].

[97] D. Allan, "What is Bitdefender Box and what can it do?," Techradar, 18 June 2021. [Online]. Available: https://www.techradar.com/news/bitdefender-box-explained. [Accessed 4 May 2022].

[98] Norton, "Norton Core," [Online]. Available: https://support.norton.com/sp/static/ftpdata/english_us_canada/manuals/NortonCore_UG.pdf. [Accessed 12 May 2022].

[99] R. Trimananda, A. Younis, B. Wang, B. Xu, B. Demsky and G. Xu, "Vigilia: Securing Smart Home Edge Computing," *2018 IEEE/ACM Symposium on Edge Computing (SEC),* 2018.

[100] "Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure," *Albany Law Journal of Science & Technology ,* vol. 13, pp. 43-82, 2002.

[101] M. Fagan, M. Yang, A. Tan, L. Randolph and K. Scarfone, "Security Review of Consumer Home Internet of Things (IoT) Products," 2019.

[102] J. B. Gross and M. B. Rosson, "Looking for Trouble: Understanding End-User Security Management," 2007.

[103] J. Caltrider, "10 Fascinating Things We Learned When We Asked The World 'How Connected Are You?'," Mozilla, 1 November 2017. [Online]. Available: https://blog.mozilla.org/en/mozilla/10-fascinating-things-we-learned-when-we-asked-the-world-how-connected-are-you/. [Accessed 3 May 2022].

[104] J. Haney, Y. Acar and S. Furman, "“It's the Company, the Government, You and I”: User Perceptions of Responsibility for Smart Home Privacy and Security," *USENIX Security Symposium 2021,* pp. 411-428, 2021.

[105] N. Mathers, N. Fox and A. Hunn, "Using Interviews in a Research Project," Trent Focus Group, 1998.

[106] LeTourneau University, "Quantitative Research and Analysis: Quantitative Methods Overview," LeTourneau University, 10 January 2022. [Online]. Available: https://lib-guides.letu.edu/quantresearch#:~:text=Quantitative%20research%20methods%20emphasize%20objective,statistical%20data%20using%20computational%20techniques.. [Accessed 13 June 2022].

[107] J. Faber and L. M. Fonseca, "How sample size influences research outcomes," *Dental Press Journal of Orthodontics,* vol. 19, no. 4, pp. 27-29, 2014.

[108] E. Ronen, C. O'Flynn, A. Shamir and A.-O. Weingarten, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," *2017 IEEE Symposium on Security and Privacy,* pp. 195-212, 2017.

[109] Statista, "Smart Home - revenue forecast in the World from 2017 to 2025," 15 June 2021. [Online]. Available: https://www.statista.com/forecasts/887554/revenue-in-the-smart-home-market-in-the-world.

[110] "IoT under fire: Kaspersky detects more than 100 million attacks on smart devices in H1 2019," 15 October 2019. [Online]. Available: https://www.kaspersky.com/about/press-releases/2019_iot-under-fire-kaspersky-detects-more-than-100-million-attacks-on-smart-devices-in-h1-2019.

[111] R. D. Adams, "IoT device attacks double in the first half of 2021, and remote work may shoulder some of the blame," 13 September 2021. [Online]. Available: https://www.techrepublic.com/article/iot-device-attacks-double-in-the-first-half-of-2021-and-remote-work-may-shoulder-some-of-the-blame/.

[112] A. Brauchli and D. Li, "A Solution Based Analysis of Attack Vectors on Smart Home Systems," *2015 International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC,* 2015.

[113] "Envista Forensics," 2015. [Online]. Available: http://www.envistaforensics.com/news/the-most-hackable-cars-on-the-road-1.

[114] "Business Insider," 25 September 2019. [Online]. Available: https://www.businessinsider.nl/hacker-breaks-into-smart-home-google-nest-devices-terrorizes-couple-2019-9?international=true&r=US.

[115] "My Alarm Center," [Online]. Available: https://myalarmcenter.com/blog/the-history-of-home-automation/#:~:text=1966%3A%20ECHO%20IV,turn%20appliances%20on%20or%20off..

[116] G. Ye, "IoT_reaper: A Rappid Spreading New IoT Botnet," 20 October 2017. [Online]. Available: https://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/.

[117] B. Krebs, "Did the Mirai Botnet Really Take Liberia Offline?," 4 November 2016. [Online]. Available: https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-really-take-liberia-offline/.

[118] O. Klaba, "Octave klaba Twitter," [Online]. Available: https://twitter.com/olesovhcom/status/778830571677978624.

[119] "Connected Home 2.0," [Online]. Available: https://www.pwc.co.uk/industries/power-utilities/insights/connected-home.html.

[120] J. Bugeja, A. Jacobsson and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," *2016 European Intelligence and Security Informatics Conference,* pp. 172-175, 2016.

[121] Jmaxxz, "Backdooring the Frontdoor Hacking a "perfectly secure" smart lock.".

[122] D. Oberhaus, "This Hacker Showed How a Smart Lightbulb Could Leak Your Wi-Fi Password," 31 January 2019. [Online]. Available: https://www.vice.com/en/article/kzdwp9/this-hacker-

showed-how-a-smart-lightbulb-could-leak-your-wi-fi-password.

[123] D. Winder, "Confirmed: 2 Billion Records Exposed In Massive Smart Home Device Breach," 2 July 2019. [Online]. Available: https://www.forbes.com/sites/daveywinder/2019/07/02/confirmed-2-billion-records-exposed-in-massive-smart-home-device-breach/?sh=1a6a646411c2.

[124] L. C. D. Silva, C. Morikawa and I. M. Petra, "State of the art of smart homes," *Engineering Applications of Artificial Intelligence,* vol. 25, no. 7, pp. 1313-1321, 2012.

[125] "SmartHomeUSA.com," [Online]. Available: http://www.smarthomeusa.com/info/smarthome/. [Accessed 30 September 2021].

[126] B. Rodrigues, "LuaBot: Malware targeting cable modems," 2016. [Online]. Available: https://w00tsec.blogspot.com/2016/09/luabot-malware-targeting-cable-modems.html. [Accessed 1 October 2021].

[127] Qrator, "Mēris botnet, climbing to the record," Qrator, 9 September 2021. [Online]. Available: https://blog.qrator.net/en/meris-botnet-climbing-to-the-record_142/. [Accessed 12 December 2021].

[128] S. U. Rehman and S. Manickam, "A Study of Smart Home Environment and its Security Threats," *International Journal of Reliability, Quality and Safety Engineering,* vol. 23, 2016.

[129] J. Teel, "Comparison of Wireless Technologies: Bluetooth, WiFi, BLE, Zigbee, Z-Wave, 6LoWPAN, NFC, WiFi Direct, GSM, LTE, LoRa, NB-IoT, and LTE-M," Predictable Design, [Online]. Available: https://predictabledesigns.com/wireless_technologies_bluetooth_wifi_zigbee_gsm_lte_lora_nb-iot_lte-m/. [Accessed 7 April 2022].

[130] Bitdefender, "Bitdefender BOX," Bitdefender, [Online]. Available: https://www.bitdefender.com/box/. [Accessed 30 November 2021].

[131] LIFX, "Privacy & Security: Responsible Disclosure of Security Vulnerabilities," LIFX, [Online]. Available: https://www.lifx.com/pages/privacy-security-responsible-disclosure-of-security-vulnerabilities. [Accessed 30 November 2021].

[132] Oracle, "What is IoT?," [Online]. Available: https://www.oracle.com/internet-of-things/what-is-iot/.

[133] A. Dorri, S. S. Kanhere, R. Jurdak and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case," 2017.

[134] B. Krebs, "Lizard Stresser Runs on Hacked Home Routers," Krebs on Security, 9 January 2015. [Online]. Available: https://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/. [Accessed 4 April 2022].

[135] B. Krebs, "Cowards Attack Sony PlayStation, Microsoft xBox Networks," Krebs on Security, 26 December 2014. [Online]. Available: https://krebsonsecurity.com/2014/12/cowards-attack-sony-playstation-microsoft-xbox-networks/. [Accessed 12 December 2021].

[136] H. Tschabitscher, "How Base64 Encoding Works," Lifewire, 13 November 2020. [Online]. Available: https://www.lifewire.com/base64-encoding-overview-1166412. [Accessed 30 April 2022].

[137] Kaspersky, "Cryptography Definition," Kaspersky, [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography. [Accessed 30 April 2022].

[138] Smarthome, "Insteon," Smarthome, [Online]. Available: https://www.smarthome.com/collections/insteon. [Accessed 5 May 2022].

[139] Microsoft, "CVE-2021-34473," Microsoft, 13 July 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473. [Accessed 14 May 2022].

[140] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton and H. Chen, "Assessing Medical Device Vulnerabilities on the Internet of Things," *2017 IEEE International Conference on Intelligence and Security Informatics (ISI),* pp. 176-178, 2017.

[141] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri and G. Baldini, "Security and privacy issues for an IoT based smart home," *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),* 2017.

[142] M. Ryan, "Bluetooth Smart: The Good, The Bad, The Ugly... and The Fix," 2013.

[143] D. Wroclawski, "How to Keep Your Home Security Cameras From Being Hacked," Yahoo! News, 4 May 2022. [Online]. Available: https://news.yahoo.com/keep-home-security-cameras-being-120340393.html. [Accessed 10 May 2022].

[144] M. Lesk, "Cybersecurity and Economics," *IEEE Security & Privacy ,* vol. 9, no. 6, pp. 76-79, 2011.

[145] N. Bridges, Interviewee, *Smart devices could leave your home vulnerable to security threats.* [Interview]. 19 April 2022.

[146] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif and R. Budiarto, "Investigating Brute Force Attack Patterns in IoT Network," *Journal of Electrical and Computer Engineering,* vol. 2019, pp. 1-13, 2019.

[147] B. Bouwmeester, E. Rodríguez, C. Gañán, M. v. Eeten and S. Parkin, "“The Thing Doesn’t Have a Name”: Learning from Emergent Real-World Interventions in Smart Home Security," pp. 493-512, 2021.

Appendix 1

Interview 1

3. What is your opinion on the current state of smart home technology?

a. How did smart home technology change over the last five years?

b. What changes have you observed in the field with respect to smart home security?

So, I've been working on smart home security and privacy for the last 7 years, what I've seen that change for the last 5 years is people were not aware that security and privacy are real issues. For example, there was no awareness that smart home devices collecting users' data, it can be hacked, and as powerful as regular computers. Now, I'm feeling there are more awareness of security and privacy. For example, when consumers talk to Alexa, a smart home device, they know that this device are also recording their voice. On the other hand, attackers also getting more knowledge in this area. As far as I remember, in 2017, there was Mirai botnet attack, which was one of the biggest attacks in IoT security. After that, there was a lot of follow-up attacks which follow Mirai botnet's code that they adapted it in some way. So, what I can say is that there is more awareness from the users side and more cyber security researchers focusing on IoT security and privacy. But, on the other hand, attackers also improving their knowledge as well as their attack surface

4. What developments do you foresee in the smart home security area in the next 5 years?

5.1.1. Which of these developments would you consider most relevant to your own role, and why?

So, there are these new attacks such as ransomwares, or crypto-miner attackers, so they come up with new techniques from the attackers which mean could be more dangerous when use in a smart home environment. On the other hand, the vendors are very diverse, the communication protocols used in smart home are very diverse, there are a lot of different protocols that different vendors use. When it comes to the solutions side, there is no unified solution such as there is no unified defense mechanism use in smart home devices. So, I think in the next 5 years, there will be some communities that are coming together that propose a new protocol such as, new communication protocols, security standards for this purposes. For example, I've seen a niche standard that they are working on lightweight crypto algorithms to be utilized on IoT devices. It shows that vendors are coming together. Maybe the government also will be coming as well to create better defensive solutions

6. What do you think is currently the most likely attack vector in a smart home?

So, one of the biggest issues with smart home devices is the security weaknesses. They are mostly created by the purpose of marketing. So, something like, there is a raspberry pie inside a box which is nicely shaped and then they maybe put a nice machine learning algorithm and they put it in the market. However, they don't consider the security that much. So, it's causing a lot of problems such as Mirai botnet which is one of the cases that shows the security weaknesses of these devices. So, I think that's still the biggest issue in this sector because they don't take security as a priority. So that's why botnet is one of the biggest attackers in this sector. The way a botnet work is that there is one bot master and general operating, the control-end command server, and then attacking to local devices. Then exploiting already well-known security issues such as default password issue. Most of the devices, they don't change the password. So, there is a list of passwords that you can try and if

one of them works, then you get into the device and that device become your bot. So, you can utilize it for different purposes such as to create a DDoS attack or you can utilize it for crypto mining where it can mine the crypto on behalf of you, not the user. So, they can be utilize for several purposes but the basic security problem in those devices still remain and it can be use by the attacker.

7. **Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam**

I think there are 2 perspectives on this subject. One, the vulnerability never known, and the researcher found it in the lab, then the attacker exploit them later. The second, the vulnerabilities are always there, it's being exploited by the attacker but it's not known by the public and then the researchers found that it's being exploited and can be exploited. I don't know which one because it's a bit sophisticated but it can be both of them. Also, I think I've seen one malware paper that claiming that most vulnerabilities, even though its being responsibly disclosure by researchers, there are more vulnerabilities in the public than the one shared to the public. So, sometimes the vulnerabilities are already being exploited and we don't know them. Then, the researchers found that the vulnerabilities are being exploited. That doesn't mean the researchers are the one that exploit it. That's why it's important to know the danger of these devices. So, when you have these devices, you should be aware of the danger such as what they are recording, what they are collecting, and what they are doing at your home. Because we now have physical interaction with these devices, physical communication, they are recording everything not only what we search on YouTube but they also recording the time when we come home, the things that we do at home. As long as we know that we are being recorded, or we know the danger of these devices that it can be exploited, we're going to ask, as a user, to the vendor and the researchers to do research and to secure these devices. So, the security awareness is very important in this perspective. So, it is possible to happen. When the devices are being exploited and publish by the researchers, then it can be use by the attackers as well. So that's possible. I'm not aware of any specific case that I can give you but it's possible that these devices can be easily exploited, like the smart lock, and the cameras. The cameras are a well-known case because when the attacker hacked the cameras, they can see what you do easily. Compared to other devices, the cameras are much more fruitful for the attackers. In general, all of the devices can be hacked and exploited by the attackers. So, we should be careful and as a cyber security researcher, that's why we work on them on the behalf of the users to protect the users. That's why we need more researchers to work on them so it can be disclose to the vendors. So, there are a lot of vendors, a lot of apps, a lot of communications protocols that need to be investigated by the researchers. When you buy a device, most of them, they require you install their own app. As a user, you see the permission but it's not easy to understand what is going on in the back or in the app. At least people don't check every app. We check around 140 apps and most of them collecting very sensitive private information. Some of the vendors are not even famous, so you don't even know what they are doing with your data. You just have to accept the term to use the app. So, there are a lot of vendors, a lot of apps, a lot of communication protocols, and these need to be investigated by the researchers. The users' job on this ecosystem is to understand the risks and aware of the risks.

8. **What are the most frequently reported security incidents that you know of or you've experienced?**

In general, people complain about privacy more than the security because a lot of these devices collecting personal information. One of the most famous one is Amazon Alexa. I think it was on the news as well, such as it was collecting conversations, not only when I call it but just normal conversation such as when speak something near Alexa or having a phone call conversation, that's what I heard from a lot of users. So, people complaining a lot about this rather than the security issues. In my experience, people complain more about the privacy like what kind of data these devices are collecting. They are more suspicious about it more than the security incidence.

9. What vulnerability do you think is the most dangerous in a smart home systems?

I think is the lack of or the miss authentication protocol of these devices. Some of the devices don't have authentication. When you install a device, you have to be in a physical range of the device and then you can hard reset the device, you can take control of it. So basically, the device is yours when you have physical access to the device. That's why these devices require a good initial authentication. Also, after the setup, it also needs continuous authentication in the smart environment because we use these devices all the time. So, I think the most dangerous vulnerability is the lack of authentication of these devices.

10. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box

From what I've seen here is the method use in the Bitdefender Box is not new method such as they have built-in VPN for extra privacy. They also put extra additional security that already known but they put it in the box to sell this new device. I think you can have these security measures by modifying the already existing routers. I think they trying to help the end users because they don't have advance security knowledge to install the security in their devices. It's a good step and can help the users. The Bitdefender Box could also improve more things with the new security measures. For example, I'm not sure about the 'block malware, stolen password', probably these are based on the blacklisting method. I'm not sure those blacklists are regularly updated. They need to be updated because attackers are changing their domain name and their IPs all the time. So, it needs to be updated with new malwares, new attackers, and new methods. On the other hand, the reason why smart home devices don't run anti-virus because they are small devices and cannot really programmed them. There is not much you can do on the device. What I like about this method is that they run on the router, so it means that you don't have to configure smart home devices. It's a good thing but it needs to use a more advance method and this method needs to be up-to-date. On the other hand, not to the third party but from what could be done is we need more standards for the companies. They should not be able to just put it in a box and sell it to the market. They should not be able to do that. There is a need of a standard in this perspective. So, from the security company perspective, this is a good step. But overall, it needs to be better. So, to summarize, it can help in some way but not everything.

11. Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry

First of all, the one that is most responsible is the consumers because we are living in the age of data and you have to know what you bringing to your home. There are some old people that are not technical people but at least you need to have some basic level of knowledge in this perspective. If you rely on others, there will always something that will coming up that is new then will be some

other flaws, I think. But what I'm talking about is just basic knowledge of security and basic knowledge of digital world. Because you have to save your password somewhere secure, this should known. Otherwise, even the most secure system will be exploited if you just give them the password and they can just get in the system. For example, when you just write your password on your computer, anybody who can access the computer can get in the system. You can create the most secure system in a genius way but it will not help. So, the consumers at least need to have basic knowledge of digital devices and basic security knowledge. The second is the manufacturers. The manufacturers need to be aware of the devices that they are selling in the market. They need to consider security as a priority and not just another expense in their business. When you give these devices to the consumers, the devices are connected to the internet all the time. These devices have to be connected to the internet for real time access and remote access. So, the second most responsible is the manufacturers because they need to consider the security of these devices before they sell them to the people. Then I put the security industry last. The reason is that the security industry already does what they can do but there needs to be an effort from the others like manufacturers, the consumers, and the government. They need to put more effort. That's why they are more responsible than the security industry. The security industry comes last after the government. The government comes third. The reason is the government needs to check these devices before they are being distributed to the millions of people. So, it's not just a small business environment. When they put these devices in the market, they are selling a lot of people so it could affect everything such as critical infrastructure of the whole country.

12. Would you like to add something?

Some people such as in academia don't think that this is a real issue. The reason for that, in the academia, they are looking for novelty. For example, botnet and we've known them for 20 years and the solutions is "this, this, this". But what we've seen in real life is there are attacks happening and there is no solution right now on this issue. So, there's have been a solution on real computers but we don't see that the computers are being part of the botnet attacks because they pass through a lot of security defenses. But these smart home devices, they don't have interface so how are you going to put firewall in them, and how you going to modify it to defend from an attack. So, the solutions are there for the computers but these smart home devices are still vulnerable. So, this was an issue for the academia but I think it's getting better and a lot of researchers are working on it. So, in the academia, they look for the novelty. They're looking at new problems and they're defending that these are old problems. But what I believe, even though the attacks are old, there are defenses that have been found in the academia but they are not there so the attacks are happening. So, it's a real problem that we have to work on it.

Interview 2

3. What is your opinion on the current state of smart home technology?

- **a. How did smart home technology change over the last five years?**
- **b. What changes have you observed in the field with respect to smart home security?**

One thing that I think is really important in the last years is the introduction of the Artificial Intelligence (AI) everywhere. So, we're talking a lot about devices that are connected and they need to learn about the user habits or what the user needs. This means we need to gather all the data. Not

only these devices need to learn how the user behaves but they also need to learn how to interact with other components or devices. This is the most prominent evolution in this domain because of the introduction of machine learning and artificial intelligence everywhere. This also means different network architectures because we need to process data in different ways. We have this machine learning or artificial intelligence models, we have different requirements both in terms of storing data, data that we need, but also in terms of how to exchange this data and how to manage the data in the network. So, this has huge implication in terms of security because we are collecting a lot of data that we need to make IoT devices more compliant to the user needs. But this means gathering a lot of sensitive data regarding the users. If you want to make the devices respondent to the users need based on the users' habit, it means that we need to learn the users habit. This also means that a malicious attacker or a malicious user may get access to this data and then profile a user or maybe track user and know that a user is inside the house. They don't have to rely on looking at the light on the windows and they can do this by looking at the data. So, data usually exchange through wireless technology, and this means that it's open to everyone unless there is good security solutions there. But usually it's easy to get access to all this data.

4. What developments do you foresee in the smart home security area in the next 5 years?

a. Which of these developments would you consider most relevant to your own role, and why?

Of course, this artificial intelligence is not at the end of its road but it's still at the beginning. We can gather more and more data from the user. There are smarter ways to use this data and higher capabilities for IoT devices to act based on this data. Another thing that I think would be very important also for smart home and IoT security in general is the application of the blockchain technology. So, instead of having centralize system, there is a trend of moving towards highly distributed networks where there is no central entity that manage the whole network. But all entities have their share in managing the whole network. I guess this is one of the roads towards more secure IoT network and more secure smart home services. Because, the fact that we will not have a centralize network entities that manage the whole network, but there will be highly decentralize network. I think this is more relevant to my role because of the fact that I'm actively doing research on this kind of technologies so the application of blockchain and the impact of blockchain technology on different domain among which is IoT. So, when we want to merge the IoT board and the blockchain board, we need to count for the network demands of IoT. IoT generate a lot of package but it's a lot of small package which have time constrain because we need to deliver this package fast. Although, blockchain provides the security guarantees that we may want for a smart home, we need to be able to deliver the quality-of-service requirements of IoT. So, I think this is very important and also for a technological point of view could be revolutionary.

5. What do you think is currently the most likely attack vector in a smart home?

So, I think the main problem is the fact that we are dealing with wireless technology. So, there is no physical medium that the attacker needs to access to be able to launch attacks. Now everyone can access the wireless instantly. So, this provides a huge attack surface for attackers for different types of attack. For example, we might be able to get sensitive users' information from the wireless instantly because the medium is open so everyone that captured a package, maybe able to inverse the sensitive information. Or, in so many cases, attackers can inject data in this type of networks again, because there is no physical medium that the attacker needs to access. For example, if the

attacker is outside the house, the attacker might inject some package inside the house because again, we are using wireless technology. The basic wireless word, you don't care where the package comes from. You just see the package in the network, so you need to act upon that. So, this represents how huge attacks surface and therefore provides a lot of attack vectors. For different attacks, might be privacy concerns for the users or the disruption of the network and service unavailability.

6. **Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam**

Yes, I think so. One of your examples already shows why it can happen. When you work in a research domain in security and privacy, it's always important to do a responsible disclosure. So, you found a vulnerability, you inform the company that produces the devices like "so we found these vulnerabilities, be aware of the fact that attackers will be able to exploit that". There are some attacks which might be a bit cumbersome such as attacks that took too many steps or hackers that are not properly trained so might not be able to exploit the vulnerability. Since we are dealing with the internet, everyone gets access to all the information what they want. So, it's totally feasible for anyone to get access to all the information needed to launch an attack. I think some attack that has been shown in the literature didn't actually happen, but it is still important to have them there because it acts as a warning. So, it's up to producers to implement the countermeasures to those attacks because it might happen any minute that someone exploits the disclose attack vector.

7. **What are the most frequently reported security incidents that you know of or you've experienced?**

One of the things that has been proven many times is regarding the security cameras. Security cameras have been hacked a lot both in terms of DoS attack or in terms of force information injected inside the camera such as you don't recognize the user or recognize another user as legitimate or don't see the video of the situations that are currently happening. This is one of the things. The other thing that I witness a lot is the gathering of sensitive users' information. So, back in the day people thought that encryption was sufficient to protect users' data. Now, we are dealing with a lot of data regarding users activities. So, let's imagine a lightbulb. Although a lightbulb is made with encrypted information and share it with some server, still you are able to get whether the user is inside the house or not based on the fact that the lightbulb is emitting any package or not. This is stupid but again this is privacy concern because you are able to get whether the user is inside or not. So, all of this privacy guarantees have been hacked a lot in smart homes because encryption may not be sufficient in protecting users.

8. **What vulnerability do you think is the most dangerous in a smart home systems?**

This is the same as the one I talked before, the fact you get a lot of sensitive user's information. I'm very concern about privacy guarantees to be honest. This is one of the things that I'm focusing on my research. In a sense that you can get a lot of information from IoT data. You are able to profile a user, you know the user habits, what kind of service they want, you can have dedicated ads to users. There was this stupid example that someone at a certain time needed to search for a coffin for someone that died. Then, the coffin ads keep coming for an entire week and this is annoying because you don't want to remember the fact that someone that you know died. So, this is all kind of things that you

can retrieve from IoT data regarding the users' activities. So, I guess this is one of the most dangerous because you may impact the live of a user. It's not just the fact that you cause a DoS attack, it's the fact that you are messing with the user's live and it's not good.

9. **How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box**

These devices that you showed me are really interesting and may help the users. The users cannot be aware of every single security concerns. So, providing the users with proper technology to defend at least against the most common attack is already something good. These companies still need to invest in research because one of the problems with security is that there is always someone that comes up with new attacks. You cannot imagine everything. You can have some security guarantees, but you cannot provide full security. Again, there will always someone that manages to break into something new and know new attack vectors. So, I guess this is one of the most important things. These companies develop the tools for users to be secure against cyber-attack, but they also need to continue investing in research to provide more and more secure devices to the users.

10. **Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry**

I would put the manufacturers and government at the first place. Nowadays, seems like a lot of people know about security but they are not security experts. One thing is saying "okay I know in order to secure a communication, I need to use some certificate". But the serious thing is how do you manage those certificates, how do you provide a concrete infrastructure to manage those certificates. The point is that the fact manufacturers and government may know something about security but they should rely on someone that is really expert in security. It's something like a pride. For example, I'm a producer and I know my device is secure because I read something about security and I know this is the way to do it. As I told you before, there are always people in the security field that manage to break new devices because that's their job as security researcher. So, the first place I would put manufacturers and government because they need to realize, and they need the security experts and not people that know about security but security experts. Then, second place is security industry because there is a need for research in this field for the same reason where someone always manage to break into devices in new ways to jeopardize the privacy of users. So, security industry should invest in research, develop new methodologies, find new threat vectors because if the security industry finds these threat vectors, it means they also able to develop countermeasures before attackers actually exploit those attack vectors. Although, I don't like it very much, but I put consumers in the last place. I don't like it very much because consumers need to realize that their security also depends on their actions. A very stupid example is imagined I don't have a smart home and I have a classic old house with key. I put my key inside the keyhole and I open the door then I left the key outside and close the door. I mean that is my fault if someone manages to break in. So, from the users side it's important to have updated password for instance or don't have the password written on the wall just so everyone can access their devices.

So, you have manufacturers and government as the first rank, second is security industry and last is consumers. Just to clarify, I'm confused about the government in the first place the same as manufacturers. So, what do you mean government should know about security as well?

So, when you design new regulations, it should also come with the new technology. These two things cannot be separated because what you can provide from a law point of view also depends on what you can provide from technological point of view. One cannot dealing with issue without the other. From law point of view, you need to provide users with the best guarantees you can but you cannot limit the technology because without the proper technology, you cannot have those guarantees. So, there's a need to be a collaboration between manufacturers and government to agree on what can be provided and the way it can be provided. So, that the devices that sell in the market is up to standards and the government is not providing any limitations to the manufacturers. Because there might be the case where you have regulations that limits the technology that you can use because maybe you have too strict privacy guarantees on the manufacturers side in order to provide users with a stricter privacy guarantees. But then, these two things do not get along that well because you are limiting the technology that you can use. So, there is a need of collaboration between the two side.

11. Would you like to add something?

No, I don't think so.

Interview 3

3. What is your opinion on the current state of smart home technology?
   a. How did smart home technology change over the last five years?
   b. What changes have you observed in the field with respect to smart home security?

It has change definitely. In 2015 when we started bridging psychology and cyber security, there were not many devices to begin with. The usability of the devices was very clunky, and I used to thought that the best cyber security measure was that the devices didn't work. One of the best devices on the market was some Samsung light, I think, and the device suffered from bugs, it was difficult to upgrade, and it wouldn't hook up very well with different services that existed. So, the best cyber security measure was the fact that it was already difficult to make it work even if you have access to the credentials. I think, things have probably changed a little bit. There has been a lot of effort to translate and make the technology a bit easier for users. There have been these online platforms like IFTTT or Stringify where you can easily hook up your devices and make them do smart things. I think that had been a good thing. But I do think that the manufacturers could do more for the cyber security generally and particularly in training the users on how to do things.

4. What developments do you foresee in the smart home security area in the next 5 years?
   a. Which of these developments would you consider most relevant to your own role, and why?

I hope that there will be a push for more from policy side of things. You have seen it last year that the US government has put up a bill to say that there should be some cyber security and IoT things going on. The point is that there is an understanding from the government that smart home technology or IoT technology is here to stay and that it was lacking in terms of cyber security. So, I hope that in the next 5 years, these constraints impose on to the manufacturers, on to the devices, will produce

better devices that are a bit easier to manage. Now, I think there is a risk related to the general surveillance agenda. If you go to the extreme, related to the Snowden and NSA type of leagues. Also, the use of private information for other things like using the Facebook personality questionnaires to harvest data by people and try to influence elections for example which is bad. So, I'm hoping in the next 5 years, the policies, the governments, will manage to prevent these things from happening. As I was explaining, I think it will not necessarily be easy because many features are based on sharing data with other people and harvesting data. For example, the recommendation like Netflix recommends that many people like the same movie as you also like 'that' movie that you haven't seen. So, this is a really interesting features and I use it all the time. There is a bit of a gray area where this information can actually be use in other ways, unforeseen ways. I don't have a TV, but I'm told that in some devices, there is a feature that tries to recognize what you're watching and I think it's called ACR or Automatic Content Recognition or something like that which is a tick-box that you can untick from the settings. So basically, the manufacturer of the device, of the TV, has access to what you're watching. Even if it's on Netflix. So, there are all kinds of weird things that you can imagine in a well in dystopia. If Samsung can actually see what you watch on Netflix or YouTube then they compute a profile about you and then sell that to advertisers, so that's one thing I wouldn't want.

5. What do you think is currently the most likely attack vector in a smart home?

So, the most likely attack would be some form of injection from a webpage. So, sending some malicious codes. I think in this case, the smart TVs would be the most likely entrance. So, on these TVs and go to YouTube and see a webpage, not a C++ application that has query, database and so on. It's the same HTML content that you're watching on the TV or even on your phone. Most of your apps on your phone, they are just webpages with CSS and JavaScript and stuff like that. So, I think the most likely attack vector would be something like that because it is so easy to do. If you give the users the ability to browse the internet from their TV, they'll just going to go Reddit or 4Chan or some weird website. Then, the website will determine that they are using an IoT device like a TV and penetrate. So, I think that would be the most likely attack vector.

6. Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam

The answer is a big yes. The reason this is the case is, the cyber security researcher that I've worked with on devices that are off the shelve like the LIFX or some other devices like an online webcam security camera with a shutter. We have found that on day 0 exploit on these devices. From these devices that you can get on Amazon and so on, we have found security issues on these things that allow you to escalate privileges like the lock example that you showed me. So, these examples that are reported are not toy examples. They are real problems. Especially for cheap devices like a lightbulb. So, we had a project and took a bunch of IoT devices; a scale, a webcam, some sensors and actuators, and an Alexa. We did two things with them. So, these devices are off the shelves, and we hacked them pretty easily. We install them into people's houses and see if the users are actually notice when these devices don't work very well. So, the issue that we found were in real development and not a scientific case study.

7. What are the most frequently reported security incidents that you know of or you've experienced?

My feeling is that we will never know because they are never really reported to anyone. But I think the kind of things that are you're talking about, the baby monitor and so on, happens a lot. So, hacking a webcam happens a lot. There are these websites that probably still exist that will scan IPs to find webcams. So, webcam is a big one, I think. Now, you have way more webcams than it used to be.

8. What vulnerability do you think is the most dangerous in a smart home systems?

Depends on what you mean by dangerous. So, going back to your question 4, so I think in the next 5 years, there would be more examples of issues related to cyber physical attacks which are a hack that has physical consequences. For example, there are these smart valves for the radiators, or smart boilers, or some sort of humidity sensors. So, these devices can have physical consequences and destroy your house. They can spark a fire and kill people. I think in the next 5 years, there will be more of these things. I think the most dangerous are these devices that are meant to actuate things in our world. For example, I just move into a new house, and we have to change the oven for a split second we considered to get a smart oven. So, the oven would be controlled either from the phone or use my location to start the pizza for example. So, this is dangerous because you can burn the house. So, there are many issues like that that can happen. I work a lot with social housing companies. So, 10% of the houses in the EU are owned by company, not by private owner but private company that themselves manage thousands of homes. So, these housing companies have to find a way to manage these houses that they possess. Instead of sending a technician to fix the lightbulb, they would rather wait till the lightbulb say "hey, I need to be fix". So, there are IoT manufacturers who develop, for example, smart boilers or smart radiators that the housing companies can manipulate from a distance. I think these cyber physical things will happen even more because the housing companies will need devices to manipulate their boiler or these sorts of smart devices. So, it's actually a dangerous thing if it happens.

9. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box

I think it will come into 2 points. The first one is I do not believe that a security company that their solution will be just technological. I think that the only way that there will be good securities is by training the users in understanding their network, understanding what they do and what that means. That would also go with the government imposing on manufacturers explain on how to use data. The other aspect related to the technological systems that you talk about. I do think that some technology would be able to detect if the network have been compromise but not in an easy sense. In a sense that would be related to just the users. The technology will be able to detect if the systems is being use as a weapon of mass attack for example, as a DDoS attack. The way that you would do that is by looking at the amount of traffic. If all of a sudden, your smart TV which is not being use, starts to emit thousands of package and use all the bandwidth to send package to a DNS server in the US, then it means that your TV is being use as a weapon. So, I don't think that the single user like you and me will necessarily be the target of the attacks, but I think that the devices themselves will be use to attack infrastructure like national infrastructure like the Internet. In 2016, this is exactly what happened with thousands of smart TVs that got used as weapon of mass destruction and put down

the Internet of the east coast of the US for a couple of days. So, these devices, Norton core, Kaspersky, and so on, will be able to notify the users when smart TV is acting out and being use as a weapon, but it did not going to be able to tell the users 'hey, your data is being use and harvested in ways you don't like'. So, these devices because they don't know the details of all the devices on the network, the only thing that they can see is the traffic on the network. Also, this traffic is often encrypted. So, the device itself will not be able to inspect deeply easily in the traffic especially if its encrypted. But it can see if there is more traffic than expected. So, for example, one of the weird behavior that we observed from a webcam that we gave to people, is that their webcam periodically ping back to the manufacturers in the US and transmitting a lot of data. We had no idea what this data was about, what it was doing. Who knows, so maybe that's a regular thing that they had to do, completely legal and so on but it's definitely something that is a bit of a gray area. So, Norton core for example, wouldn't necessarily have picked up that this was bad because it was a regular behavior.

10. Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry

In my opinion, the manufacturers are the most responsible. They are the one who should be held accountable if there is something going wrong. They are the one who need to make sure that the users and consumers know what's going on. They need to train the users. Government second, security industry third, and consumers. So, the manufacturers are the one who build devices. They want to put these devices into the consumers' homes. They have a duty of care towards the consumers. So, they have to make sure the devices are bullet prove. They usually don't really care because they want to be the one to put the device first out in the market. So, they don't necessarily spend the time to make sure the devices are fine. Then, the government because in my opinion the role of the government is make sure that we all are okay. They have the power to impose constraints onto the manufacturers. I have a rouse view that the manufacturers have conscience so that's why I put them first. Then, the government could constraint the manufacturers themselves by creating a legal framework where the manufacturers would be forced to do the right thing. But I'm still hoping the manufacturers would do the right thing on their own. Then, the security industry. I know they already trying hard to figure out what is going on. So, they themselves would want to do more if they were listened to more. So, it's difficult to hold them accountable for stuff that are going wrong. Finally, the consumers. Even though the consumers can make mistakes, doesn't really know how to handle the devices, I think they are the first one who are in the front line of the issues. Therefore, they are the most at risks. So, I think that all the other actors; the manufacturers, government, security industry should make sure that the consumers are better prepared. It's difficult to say that every consumer should have a degree in computer science. We cannot really say that. So, we cannot really be upset for them when they don't understand how the Internet works.

11. Would you like to add something?

No, I don't think so.

Interview 4

3. What is your opinion on the current state of smart home technology?

- **a. How did smart home technology change over the last five years?**
- **b. What changes have you observed in the field with respect to smart home security?**

So, I would say that there was an initial phase where everything becoming internet connected and it was a little bit like wild west at the time. So, whoever wanted to innovate in that sector with whatever appliances they were making, they would just connected to the internet and that would be the innovation of the year. So, it goes a little bit like disorganize, there were no decent standards, everyone was doing their own thing, 5 years ago. At the moment, it looks like things have been standardize with very good extend. Even if we're not talking about specific protocols or specific technologies, even just as approaches, interfaces, user experience, generable logic, business model, the main player still using pretty much the same approaches in everything. So now, there is the same network technologies and the user experience is similar. It looks like the smart home technology market is kind of getting to agreed 'norms' let's say, to what it should be doing. In terms of security, some products start appearing lately specifically for smart home security. So, at commercial level they have started selling for example, intrusion detection systems, and products that are specifically you buy just to increase the cyber security of your smart home devices. In addition to the dedicated cyber security technologies even physical devices, there is also an increase interest, among the manufacturers, in improving by design their own cyber security inside their own devices. So, I would say that all the reputable manufacturers that I'm aware of, that I've worked with, they are now consider cyber security as a significant part of their concern, let's say. At design level, they know now much more than they were 5 years ago without a doubt. Generally, in terms of processes, they most know how to channel how to disclose vulnerabilities ethically. They have back bound the programs. So, I would say for the big companies, like Philips and others around the world, they tend to consider cyber security at appropriate levels. Now, there are still smaller manufacturers or manufacturers that develop only one device, where investing in cyber security is not reasonable as it is for large companies because in large companies they will invest in know-how that will apply across 20 devices, while in small manufacturers usually only has one and not have this luxury to do that. But generally, there is clearly a positive trajectory. Clearly, cyber security is considered way more now than 5 years ago without any doubt. I'm not sure why and I don't think it has anything to do with regulations as much because regulations not playing any significant role here. I don't think that the customers are asking for cyber security so much. So, the vast majority of people, I don't think they know that much about cyber security or even privacy when it comes to IoT devices with very few notable exceptions which are the one that read about it in news articles. If, they see something about, for example, a baby camera getting hacked, that goes everywhere and everyone finds out about it and that's become a factor. But for other things, I think the majority of people have no idea what's happening in cyber security and worry too much about it. So, I don't know what the driver is but the trajectory is quite positive.

4. **What developments do you foresee in the smart home security area in the next 5 years?**
    a. **Which of these developments would you consider most relevant to your own role, and why?**

There would be more cyber security products specifically for cyber security in IoT. I've seen already a few years, 3-4 years now, the first few physical devices that have to do with monitoring the network. That exist already and I expect more coming. I expect all the big players to have their own smart home IoT security kind of device that they will sell to the consumers. There will likely more regulations and standardize coding for example of the cyber security ingredients inside the device. By ingredients, I mean like in the same sense you buy food and says 20% sugar. I expect something like that will exist in the near future where people have to disclose what data they're collecting. Perhaps,

also what security mechanism they put in place but certainly what data they disclose or they collect. I don't think that within 5 years from now we will still be completely in the dark just like what they collect like Google Home. I don't think that would be the case. I'm pretty sure they would have a regulation to disclose. The one that I think is most relevant I think is intrusion detection. So, naturally intrusion detection systems in smart home will make the most sense for me. So, intrusion detection is a technology that is detecting cyber-attacks.

5. What do you think is currently the most likely attack vector in a smart home?

At the moment, I would say devices used as bots is the most likely purely statically. All of the devices that has bad cyber security by design are easier to compromised. I'm not sure it would be firmware level, it could be application layer, it could be just the passwords that still at default in many devices. So, I think this is statically the most common at the moment. So, I think botnet like Mirai botnet is the more likely attack for very simple reason. Hacking a single device is kind of impractical in most cases. Why would someone hack my own camera today and invest all this effort to hack my camera while hacking thousands of already existing vulnerable devices makes more sense. It's a matter of how much effort the attackers put in and how much they get. I think Mirai style kind of botnet still statically more likely.

6. Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam

Can they? Of course, they can. That's why they were disclose. Will they? Likely not. Why? As much as cyber-attacks are extremely popular in the news, for example, if you see the latest news on a website and magazines about technology cyber security especially IoT cyber-attack are all on the front page because, if you are a journalist, it's so cool to talk about an attack on a car for example, it's much cooler than something boring like Sony PlayStation like from 20 years ago. What do I mean by that? So, if you don't hear about an attack in the news, it's unlikely it has happened for something like that. There are so many reasons for people to leak such information that we would have found out about it. So, August smart lock, LIFX, and so on, if researcher disclose them, we see papers about them and see black hat conference presentation that are lovely. Then it happened in the real world and doesn't know about it, that is unlikely. A few years ago, we did ethical discloser of some vulnerabilities to the company. They acknowledge it and they said "yes but we're not going to solve it because it's more expensive than not solving it in the long run". So, the users are more inconvenience by the solutions that are needed and so it's better to just let the users have the vulnerabilities rather than causing inconvenience. Others that were disclose, they were fixed the next day. So, it depends on the company, and it depends on the internal decisions. So, I would not call these real cases because researchers can give you 3000 cases in one day. For something to be a real attack, it means there is something like a business case for cyber attacker to do it, make money out of it, and spend the time to actually develop the attack and complete the whole hack. That's not very common. For one of your examples, the baby camera, I think this is the one that routinely happen all the time. I don't know if it's because of internal decisions of the camera manufacturers, but the attack might be happened because they are just so attractive to attack. But, you could still expect at least one per year baby camera attacks but I don't know if they exploit the same vulnerabilities because I haven't check. I remember 7 or 8 cases that are real criminal cases in the real world, not in the labs.

7. **What are the most frequently reported security incidents that you know of or you've experienced?**

Most reported is the baby camera. Depends on whether it's incident or not. If it's for incident, I would say it's the baby camera, the only one that keep coming up all the time. Generally, smart home incidents are not that common. So, I don't know there is any statistical data that will show this is more common.

8. **What vulnerability do you think is the most dangerous in a smart home systems?**

I think it would be implementation errors in the network protocols. I think this kind of mistakes still being made too often. Thus, creates vulnerabilities that are the one that are usually disclose. So, how you fix it? by removing the mistakes. The standards are fine but it's just the implementation of the protocols are very often wrong in the devices for a number of reasons. The impact would be obvious, theft or burglary.

9. **How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box**

So, first of all, I think it can only protect at the network level. So, it cannot cover the full range of IoT security. Also, the attacks need to have some kind of obvious network footprint, which is true for some attacks like DoS attack but I don't know if it's true for Zigbee for example, manipulation. The Bitdefender box connected to the router. So, it can only do something that the router can see. If it's an attack that is for example, which ever Samsung smart things devices, or Philips light, these are Zigbee devices. So, they have a hub which connected to the router but after the hub, they have nothing related to the router, from then on, it's the Zigbee network. That part cannot be seen at all by any of these security devices that you showed. So, naturally, the protection is up to the level of the router and not at the level of the devices themselves. What does that mean? It means that what they could do better is actually protect the networks of the devices themselves which can be a Wi-Fi but usually it's not. The Philips light is not and it's the most popular in the light market for example. So, that's what I think they could do. Other things they could do is they could help with educating the users. So, these security devices can protect for the network part that can be seen by the router, these security devices can detect it but any attacks that are local like in the local Zigbee network, there's no way they can see it. I think it would be useful to have some contributor education of the users but again I don't think they have the business model that contribute and let users have better understanding at cyber security.

10. **Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry**

So, first I would say the manufacturers because they sell the devices. The devices need to have, by design, at least a minimum level of protection. Second is consumer because they are responsible for their own security and safety. Third is government because regulations can help push companies to produce cyber security where there's not necessary financially beneficial for them. So, only regulations can have such an impact. What I means by development I meant manufacturers so they are the one that should do the security of their own devices. And the security industry would be good if they could collaborate with manufacturers by being a bit less expensive. The security industry is ridiculously expensive to others and manufacturers would not do collaboration with any of big

security companies because it would just blow their budget completely. Then, this cannot be pass onto the consumers. You cannot buy a Philips light that is already expensive and then double the price just to have a security provision in collaboration with one of the major partners. So, I would say the security industry is fourth, manufacturers number one, consumers number two, government number three.

11. Would you like to add something?

No, I don't think so.

Interview 5

3. What is your opinion on the current state of smart home technology?
   a. How did smart home technology change over the last five years?
   b. What changes have you observed in the field with respect to smart home security?

So, I can see the smart home has more and more devices came out during the last 5 years and more smart home protocols or more generally about IoT protocols that came out. That same people have all different opinions and different technology. They just tried to put those things into the smart home. So, that's what I've observed over the last 5 years. In security perspective, I can see that some certain of improvement but not that much. The reason is because there are more and more security breach in the smart home that we've heard on the news. Especially, you can tell there is a lot of malicious attackers that they actually target smart home devices. I think there is improvement but it's not to the level where you can say "okay, it's safe now".

4. What developments do you foresee in the smart home security area in the next 5 years?
   a. Which of these developments would you consider most relevant to your own role, and why?

I would say more automation will come into smart home security area. The reason for that is for the home user, they have no idea how to protect their smart home security and they don't have the ability to do it manually. So, I think we should have a way of automated smart home security process which the user don't have to think about anything too much. They know and find this system and know it's going to be safe. Then the product will automatically communicate with each other and then be able to be protected as a whole.

What do you mean by automation? Is it the Artificial Intelligence or Machine Learning? Or is it about the communication because there are a lot of devices in smart home

That's a really good question. I think the AI and machine learning you mentioned will play an important part on it. Another most important aspect is the auto-configuration of smart home devices. For example, your garage door is a smart garage and has smart devices control. So, if we don't have a way to automate the configuration between the garage door and you have a smart car, so each time your car approaching and close to your home, it will automatically open the gate. So, your smart garage and your smart car have to pair themselves then they have to set up a certain condition such as what time you got back home, and the garage open automatically. But, if I just drive pass by my house and I don't want to get into my house, should the garage door open or not? We don't know. So, we should have a way to utilize the AI and machine learning to learn the pattern.

Another important thing is how the information exchange between your car and the garage door. So, that has something to do with auto-configuration. So, what devices that has the ability to control the garage door? I give you another example which is the smart smoke alarm. If something happen and home catch a fire, so the smart smoke alarm will automatically open the garage door or not? To let people to escape. So, this is one of the examples. So, the automation combined with auto configuration and the AI and machine learning.

5. What do you think is currently the most likely attack vector in a smart home?

It can be many different one. It can be physically or remotely. So, let's say someone want to break into your home. if they can approach your home and use anything that can interfere with the garage door of your home to allow them to get in, or they can turn off all of your security cameras and the alarm system. So, the physical so maybe they injected something in the smart home and get in. This is one of the examples. Another is people can remotely hack from anywhere in the world to control the devices of your smart home. For example, they can check into your security camera, they can listen to what you're saying and know what you're doing. Another thing is, apart from monitoring, they might also put malware into your smart home devices. So, when they try to launch a DDoS attack, they can use your smart home devices as a bot to form a botnet to attack others. So, we're seeing this a lot these days because smart devices usually are a hellish devices. Even when you got hacked, you have no idea what's going on. So, the most dangerous I think is the remote attack vector through the internet.

6. Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam

Yes, very likely. I also noticed the fact that those things not just happen in the lab but also actively exploited by people out there. There are a lot of people that do this hacking which is by the example that you showed me. It's very likely that this thing could happen so that's why we need to improve the security of the smart home.

7. What are the most frequently reported security incidents that you know of or you've experienced?

Yeah, so it's the one that happen in 2016, the Mirai botnet. So, what it does is using the weak credential of smart devices and get inside it, then put themselves into the devices. So, they actually launch the attack to DNS server and a lot of big companies, and services can't work like Facebook and Twitter. I don't remember the DNS provider but it's a big DNS provider in the US, so the malware attacked these things.

8. What vulnerability do you think is the most dangerous in a smart home systems?

No doubt, it's the remote code execution. The worse part is there is a lot of smart home devices that expose to the internet directly. So, that's why you can use Shodan, the IoT search engine, and find all these devices on the internet. Remote code execution or RCE. So, what I can do is so I just send you some package and then I can have full control of your devices. Then I can run any code remotely on your devices. So, on your local machine you can run code, but I can control it remotely. So, technically I have full control of your devices. So, that's why it's the most dangerous one. Not the DDoS because it's nothing because if you DDoS one device, then only on that one device. But if you

Remote Code Execution, you can control your device and then use your device to do other stuff. So, it's more about the network. I think hacking hardware, I don't consider it quite dangerous because that means you need to get into your home first, such as to touch the hardware and have physical access with smart home devices.

9. **How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box**

So, I think they can help to a certain degree to solve the problem. When you look at those examples that you gave me, they look like a man in the middle. You have a device, you connect it between your devices and your gateway. By the look at how the Bitdefender Box, it looks like they have some kind of scanning on the ISP because all your data is through ISP. So, for the last 5 years that I can see is that there is a lot of devices that now has implement encryption in their protocol. So, it means that if they just be a man in the middle, they don't have the ability to decrypt the traffic, I doubt about how much they can do. They might be just block IP address or look at the package and see if there is some kind of abnormality in the data package, they might block it, but they can't see what's inside the package. So, attacker can easily send command or hack the smart home devices by using the encrypted traffic and these middle devices have no idea what's going on.

10. **Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry**

So, I would say is the security industry is the first because when you look at the manufacturers, consumers and government, they are just a part of it but the security industry as a whole, it can actually interact with the manufacturers, consumers and government to come up with a solution. Manufacturers, they can certain part but cannot do as a whole. Not to mention, consumers, their hands are tied. Government, what they can do is quite limited. So, the security industry is the one that connect all of them together they can have some kind of protocol or communication that responsible for the smart home security. So, the first is security industry, second is manufacturers, third is government, and last is consumers. The rank is more about the impractical and what impact they can do. So, you can see the security industry has the most impact. So, the ranking by me is based on the impact that it can do for smart home security. So, the manufacturers is number 2 is because a smart home, there's a lot of different manufacturers. For example, Samsung doing very well for their product but what about others like Google and Amazon, or any other companies. If they're not doing good enough and only Samsung is good, technically it's still can be vulnerable. The whole security of a smart home is the most less security devices. So, imagine if you have a bucket, the bucket have water in it and then you build a good quality bucket but if there is a hole in the bucket even no matter how good the bucket is, water will leaking out from the bucket. So, if all manufacturers can be good as a whole, that would great but unfortunately in reality it's not. Only 1 or 2 maybe that can be good and always some that doing bad. So, that's why I manufacturers at second. The third is government. Government aren't more concern and high priority tense smart home. So, I don't think they will spend too much money and resources in this area. So, consumers last because they have no idea about security. So, you can't count on them to have responsibility for the smart home security.

11. **Would you like to add something?**

I think smart home security is a scam. The only thing we can do is make it harder for attackers to get into it, but you can't eliminate the attack for the smart home security. That's why it keeps people in their job because you have people that searching for the attack, people searching for defense and then you have people that buy these devices on the market because it's more secure. So, it keeps people employed. It's a good ecosystem.

Interview 6

3. **What is your opinion on the current state of smart home technology?**
    a. **How did smart home technology change over the last five years?**
    b. **What changes have you observed in the field with respect to smart home security?**

Smart home has changed a lot in the last 5 years. In terms of, you don't care about having a switch that turn on lights or a motion detector that tells you that somebody has enter into your house. It has become more sophisticated than that. What I see is that now you have an ecosystem of devices that are gathering information all the time, thousands of bits of information, that can help you improve your home experience inside your house such as how you can feel and how you do things daily. Based on that information, you can make your home be part of you. Let's say when you are stressed, you enter your house, and the lights will automatically diminish so you can be calm, or you can hear a soft music so you can be calm as well. So, this big ecosystem that you have on your hands, you have on your phone. It also helps you reduced costs in terms of energy, water, and gas because you can monitor how much you consume it every day. So, it's not only your home but also your tool to help you have a better budget in your life as well. It also gives us comfort because we don't have to stand up to turn on the lights or when we are outside of our home, it can provide some sense security inside our house because we can just take our phone to turn on the lights, turn on the music and make that home like if somebody is in there. That has changed a lot in the last 5 years. Not only turning on the lights but have this sense that someone living in your house that in charge of your lights, consumptions, electronic devices and make you feel better. About the smart home security, I think that's the weakest point because it's like everything that you have in every technology. Every day you have new things that are top trending, but the weak point is that they don't care too much about security because they focus only to provide you the thing that you need and they don't care about security. For example, let's talk about house lock, you can open a house lock by just using your phone but the protocol inside the house lock is not clear how it works. Sometimes it's very weak, they use very weak keys in order to protect or cypher the information and that's the weakest point. So, you care only about functionality, but you don't care about the non-functionality requirement which is security which are the base of having a secure place with all the facilities that you need. Sometimes it's funny you have security lock but it's insecure. Also, in terms of an authentication, it is not clear how you can authenticate or de-authenticate in terms of the technical specification of the protocols. For instance, if the manufacturer not working anymore, who gives you that support? So, you just producing new things, but you don't care about the future in terms of security for those things.

4. **What developments do you foresee in the smart home security area in the next 5 years?**
    a. **Which of these developments would you consider most relevant to your own role, and why?**

I think in the next few years we will definitely have AI in our homes. We already have AI in terms of you can play music but we still looking to have that AI into other things. For example, my house will know when I'm going on vacation and it will just turn on some lights, turn off all the pump that is on so water consumption will be reduce to zero, as well as electricity and gas costs. The costs will be reduced without us being inside the house without having to tell the house that we are leaving. So, I think that's the feel that will be explore in the next 5 years as other things that we are seeing right now like self-driving cars. I think AI will power our house in the future. In terms of security, I think we will be going to some password-less which already in place. You don't have to remember your password or your credentials, your token or something that you don't have to care about remembering such as big passwords and things like that. There are places already that use biometrics to enter a place, or a camera will recognize your face. Also, in terms of security, I think the initiative of zero trust will be apply as well. There is something that is not already in IoT, but it has been implemented in other areas but for IoT, for sure, it will be implemented. I think that there is very few research in this area but probably in the next 5 years, probably will be top trending in security in IoT. Zero trust is based on what privilege you should give to the devices like you just trust in very few things and all the other things are not trusted by you. I haven't read in depth in this topic but it's something that related to that "you just trust a bit but not the other things". It's like in a scenario when you don't know anyone, but you can trust in a little bit portion. Something like that.

5. What do you think is currently the most likely attack vector in a smart home?

I think the most common one would be social engineering is definitely a common attack and it's in every area. I think it also possible for smart home because people use to trust in unknown people. However, there are also attack vectors that are more technical such as weak authentication protocols. I think it's a common one because you can break the security of some devices by just using some devices such as a device that let you capture the frequencies of anything that works under 5Ghz. So, you can copy that codes and recreate that, and use that to open others. That's pretty common because you don't trust devices that sending the signal but you just follow series of steps in order to open others but you don't care who is sending that signal. That's one of the most common attack vector in smart home. Social engineering is trust too much in people that you don't know. Weak authentication protocols in all types of technology such as Zigbee, Z-Wave, BLE, or any other protocols that you can use in your home.

6. Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam

If, the devices are expose and there might be a way that you can access them and send some malicious code in order to make them do whatever you want. In the case that you have to be near the device, you have to modify and access the firmware, it's a little bit complicated but I'm not saying that it's not feasible. It's feasible but you have to have other things in place so that the attack can happen. But if your device is connected to the internet, there's absolutely a way that you will be vulnerable. All these devices in the future will be connected to the internet with their own public IP address because of the user IPv6. Every device will have its own IP and will be accessible from the internet, that is the main purpose of IPv6. So, in that case, those devices are definitely expose and vulnerable to attacks. If you buy a device right now, the device might be secure, but you don't what's going to happen in the next 2 or 3 years. So, it all depends on the continuity that the manufacturer

gives to your device. Some devices are just fancy this year but next month when a new version release, and you buy them for maybe 100$, so the old version is not worth in terms of security anymore. So, that's the main problem that I see. The attacks are possible, but you have to understand what are the scenario to put in place in order for that attack to happen and exploit the vulnerabilities. So yeah, they are definitely possible.

7. What are the most frequently reported security incidents that you know of or you've experienced?

Well, the one that I've seen are related to two topics. First is denial-of-service (DoS) attacks where this gang of cyber criminals had taken over cameras, thermostats, smart Wi-Fi switches and they had performed DoS attack to other infrastructure. The other one is the lack of authentication or the lack of awareness in terms of configuring a well scenario for authentication. All devices come with easy 'username and password' for the normal end-user to configure them. But most of the users, they don't care about that setting. They only care about settings like changing the light or optimizing something, but they don't care about the security. So, they just left those credentials by default and that is a weak point for any attackers that has access to the devices that knows the brand the devices that is vulnerable. They can just search it on Google and then they will have access to cameras, and they just need to surf a little bit and use default password like 'admin admin' and they will have access to those devices. So, those are the most common attacks that I have seen and still pretty common today.

8. What vulnerability do you think is the most dangerous in a smart home systems?

I think that the lack of credentials or poor credentials because if we are talking about a device that can control the gas in your house, it could make your house explode or it could kill you because it will open the gas and you breath the gas and then you die. I think that those are the most dangerous. Lack of credentials depending on the devices that you are targeting.

9. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box

I've seen another device which is very similar to Bitdefender box and I think it all depends on the complexity and the access of the end-users have. The Kaspersky example that you showed me, if you have to ask ISP to enable Kaspersky smart home security so that you can have it, then I feel like you don't have enough control of it. As an end-user, you need to have full control of your home. In terms of security, at least you need to have all the knowledge and all the control of the devices that you put in your home to stay safe. So, if you have to trust your ISP, I think that's not feasible for me. It would be easy if you have something like Bitdefender box where you just plug it and that's it. But you have to perform another step, I mean those devices like Bitdefender box should come with a very clear user manual that have say like "please change your password or it would be damage" or something like that so that the end-users could understand that at least they have to change the default password or put strong credentials. So for other devices, the Bitdefender box should be able to help with people that don't have enough technical knowledge like people that don't know what's an IP, what's communication protocols. The box should offer something like a profile for the advance user that have knowledge and very low profile that the box does everything, and the user doesn't care. So, that would be a great solution. But as I mentioned before, you have to have 100% control of the devices. You cannot dedicated that to another device because you don't know how this device is

behaving. I mean, you cannot trust any company, no matter what even if it says Kaspersky, Google, you don't know whether the people that work there and how conscious they are in terms of security because we have seen that these big companies are vulnerable and have been attacked. So, you can't trust and put your devices into another device because you need to have full control of your home. It's very nice that these security companies are interested in the security in IoT but they have to focus on who is going to use the security devices. Whether it's going to be a kid, an elderly more than 65 years old, which have limited capabilities to use something like mobile phone. You cannot ask these people to configure an IP, configure a DNS because they don't have enough knowledge. These companies need to understand their costumer before producing these solutions. So that they can protect smart home devices and also selling their product.

10. Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry

I think the first one is manufacturers. Second is a tie between government and security industry. Third is consumers. Why manufacturers in the first place? If you have enough knowledge on how to build smart home devices and you mainly focus on covering functional requirements, then you have to put security as part of your functional requirements as well. You not just care about how users turn the lights on and off, you also have to care about how the users will authenticate over their network to have access to that device that let them to turn lights on-off. So, you have to consider all the best practices, perform a vulnerability assessment, and be able to responds every time someone discovers a vulnerability and publish it, you have to act quickly in order to protect the consumers. As manufacturer, you have to care about that because you are the one who is putting your brand there and you don't want your brand to be in the news tomorrow saying "your company got attacked because of weak credentials or authentication protocols". You have to be concern about that. The second is tied between government and security industry because the government has to direct the manufacturers to be obligated to comply with some kind of standards. In Europe, you have standards depending what country you are or area, there's standards that care about your public records different than developing countries like Ecuador. In Ecuador for instance, they just released data protection law last year, but it's just about data and it has nothing to do with best practices or minimal requirement that products should comply before it's being sell on the market. Then, the problem with security industry is sometimes there are relations with government. The government have relation with security industry that has some interest to have a law or to bypass a law in order to produce something. That's like a chain where you have the government which interested in security and the security industry is interested in trying to build something new product with a manufacturer. So, this chain is really hard to break but they have to be conscious that they are not only making money, but they have to conscious that if they are trying to provide some products to the people, they have to do it with care as like you do with medicine because you will have IoT devices in the future or maybe they already exist, that control the hearth, breathing of a person in a hospital. So, you have to care about that because a life would be in danger if you don't care about the small things recommended by the security industry because the security industry is the one that recommend something like "okay let's use this protocol because it has stronger keys and don't use another protocol". So, the government try to fine these manufacturers that do not comply with these policies. Not only for that particular country or continent, but it also has to extend to all over the world as you do that with some medicines that are approved by a higher entity. You have to do that with security because security is a very important thing that are part of our life. The point is that you

have to care about security because you are controlling technical infrastructure and critical things with technology, and if you don't have a good background in technology, if you don't have a government who is controlling that security industry, publishing new things, innovating in protocols, finding new ways of authenticating people a strong pattern, then manufacturers will still building smart home devices with weak security. Then the consumers are last because not a lot of people know about technology. Few people that know about technology, they probably know a bit about how to use a social media, how to send an email, but they don't know a more complex things that they need to know in order to manage their IoT devices. So, manufacturers have to make things easier to consumers and easy to understand. Not just explaining about how to configure the devices but also explaining what are the possible risks that they will be facing if they don't follow the guidance on how to establish a good security in the devices. Consumers usually buy a device because of a particular brand because they trust the brand even though the brand has been attacked.

11. Would you like to add something?

You might have the most intelligence home, but if it's not secure, you have a dummy home. You don't have a smart home.

Interview 7

3. What is your opinion on the current state of smart home technology?
   a. How did smart home technology change over the last five years?
   b. What changes have you observed in the field with respect to smart home security?

I think it's clear that more and more devices are being manufactured particularly in the smart home that promise smart home functionality that could be considered IoT devices. So, there's clear consumer demand and clear marketing push from product vendors. In terms of how it's changed over the last 5 years particularly with respect to security, I'm still very concern about the security of smart home devices particularly consumers smart home devices. Personally, I run a guest network on my home network, and I put any smart home devices on the guest network, and I don't allow them on my private network because I've got the technical skills to do that. I quite frankly don't trust consumer IoT devices on my network. That's not based on any particular evidence, but I know because I've worked in embedded systems industry and I understand the pressures that the company and developers are under, and I don't believe that security is yet the priority that it needs to be in that industry. I think they far more focus on features and new product releases, and far less focus on security audits and/or retrospective firmware and bug fixes for security vulnerabilities. So, specific changes, there have been some moves to improve security such as things like devices forcing a change of default passwords on first power up. I don't think that's universal yet. So, I think there has been a bit of recognition that security is an issue but I'm not sure how much is really changed.

4. What developments do you foresee in the smart home security area in the next 5 years?
   a. Which of these developments would you consider most relevant to your own role, and why?

I think 5G is going to be quite interesting in the smart home space. I think we're going to increasingly see smart home devices with build-in 5G networking that don't rely on the consumer Wi-Fi network for internet connectivity. That would be a radical shift. In some sense, it's a positive shift for security

because it means that I'm not letting untrusted devices onto my private network. So, it's a net benefit from a network security point of view. However, from a privacy and personal point of view, it's worse because currently I can monitor the network traffic, or an individual can monitor the network traffic coming from IoT devices as it's traverses their private network. So, you can know if an Amazon echo is streaming data back to servers even if it's switched off, you can observe the network behavior of your devices even if it's encrypted. But, with 5G, with devices going directly into the mobile phone network and bypassing the consumer Wi-Fi network for network connectivity, you have no observability into how the devices are behaving because its internet connection is direct to the manufacturers rather than through your private network. So, I think 5G is going to be huge once it becomes more common and cheaper, and embedded in IoT devices. I would like to believe that we will see an increases focus on security, perhaps some industry standards. There's been a discussion in Australia about, you know the same way that we have those kind of consumer tech (CE) that indicates consumer safety of electronic devices, I think it's called CE. There's been talk of introducing something like that from a cyber security point of view. So, that means require manufacturers to submit their product to security audits and requires them to make minimum standards about default passwords, secure connectivity. So, this hasn't become legislation or standard practice in Australia yet, but I believe there's some discussion about it. So, this is an industry wide move to recognize that the security of IoT devices is critical because we put them in our homes, in our businesses, in our children's bedroom, and we deserve that all these devices to be secure. So, I hope that the landscape changes, but I can't say that it will.

5. What do you think is currently the most likely attack vector in a smart home?

I think the most likely attack vector is probably vulnerable unpatched older versions of open source, utilities that get used in IoT devices and unpatched vulnerabilities in things like networking platforms and operating systems that are used for IoT devices. It's about unpatched vulnerabilities because generally, the industry is focus on new product releases and features. Older devices, once they're more than like 6-12 months old, there are no subsequent security updates being release for older devices. The devices are not being maintain, there are no patches, and those devices might remain in people's home for 5 – 10 years. So, it's those kinds of unpatched vulnerabilities I think that are the biggest threat vector.

6. Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam

Yes, absolutely. I think it's probably happening very commonly. Not all of the vulnerabilities are found by white hat hackers and get reported, some are just being exploited. When you added services like Shodan that make it very easy to find devices of particular types, when there are devices with known vulnerabilities that never been patched and it's inevitable that some of these attacks and vulnerabilities are being exploited in real development.

7. What are the most frequently reported security incidents that you know of or you've experienced?

I don't track that very closely, so I have an opinion and sense of the kinds of issues. The sort of things that you were shown by the 3 examples that you just gave, those classes of problems: default

credentials, no credentials, unpatched vulnerabilities in legacy firmware. I think those are the most common type of vulnerabilities, but I don't have data to back that up.

8. What vulnerability do you think is the most dangerous in a smart home systems?

I think it would be anything that allows Remote Code Execution (RCE) type attack. So, I'm thinking about for example Mirai botnet which compromised insecure device firmware and then allow the attackers to run arbitrary code on those devices. The reason that's so dangerous is that it can be used in a way that it was used in Mirai botnet which was for generating massive bandwidth for DDoS attacks. But it can also be used against the individual because these devices are installed on people private networks. They potentially provide an access point to other devices in the network. This is why I run IoT devices on a guest network. Even if my smart TV gets compromised, or my media player gets compromised, the attack is not on the same network as my private computing devices, my mobile phone, my computer that I use for work, internet banking, etc. So, I think it's a kind of Remote Code Execution vulnerability compromised that is the most dangerous in smart home IoT because it's installed in private trusted network.

9. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box

I'm not aware of these products but I'm glad and not surprise that they exist or they starting to be marketed. I like idea of working with the ISPs, I think that's important. I think there are opportunities for third-party security companies to help. For example, network and router or modem vendors, all of the networking equipment that we have, they could default to having guest networks and having guidance that recommends that IoT devices get connected to guest network. So, recommending the setup of what I have for example. So, raising awareness. I mean in the more abstract sense, these ideas that having standards and guidance instead of guidelines that devices have to meet and they can be given a tick like 5 stars like some kind of security rating or some kind of independent audit and assessment of the security of smart home IoT devices might also be appropriate. So, that's not a product but more of an environment that could be created within the industry. So, I don't know if these devices that you show are any good but I support what they are trying to do.

10. Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry

I would say manufacturers first, security industry second, government third and consumers fourth. So, manufacturers need to be first because they are the ones who are develop the product, so they need to be responsible for the way of that product is secured and the way that it's used. I mentioned it before my concern that security updates don't get priority from manufacturers, and I think they should be forced to. I think that it's not okay that there are 5-year-old internet connected devices on the market that have known vulnerabilities that are not getting patched. That's not okay and that's the manufacturers responsibility. So, they have to be the frontline and they have to have responsibility of doing security audit for their product, having secure settings by default, documenting ways that the products can setup securely, etc. Secondly, the security industry. I think that really comes to my comments about let's establish minimum standards that require audits of products, let set baseline expectations of security in smart home IoT. That I really see as a sectoral respond. The sector needs to accept responsibility for that in the security industry more broadly. Thirdly, I rank government because they define the regulatory environment in which these things are

sold. We have safety standards for children's toys, car seats, swimming pools, everything. We exist in an environment where the government imposes minimum standards for the safety of the consumer. I don't think that cyber security and home security IoT is any different. So, I think government has responsibility to create and influence a regulatory environment that supports that. Finally, the consumers because it's not reasonable to expect consumers who are buying electronics at their local electronic retailer, it's not reasonable to expect consumers to be doing the kinds of things that I'm doing as an expert like guest networks, demilitarized zone on networks, and all sort of that stuff. That's not reasonable behavior to expect from most consumers. Most consumers were lucky if they use unique passwords and it's not realistic to expect more than that, so I don't think they carry a lot of responsibility.

11. Would you like to add something?

No, I don't think so.

Interview 8

3. What is your opinion on the current state of smart home technology?

a. How did smart home technology change over the last five years?

b. What changes have you observed in the field with respect to smart home security?

Before, it was like a lab concept specially dedicated homes use as labs with people as data. Now, the technology is no longer in the hands of researchers but in the hands of private homes own by people. We've seen devices such as Amazon Echo, Google Homes which we didn't have before. As a change, I think we are seeing a lot of devices using voice as an input channel. So, what makes it a smart home is that you can monitor, manage, and control your house potentially anywhere using your mobile phone. However, over the last 5 years, I think there is a lot of technologies that enable you to have a better experience in controlling the home for example using the voice and also using biometric features such as gestures or hand movements. This has not yet been released into the market as far as I know but there is research about bringing computer interfaces. So, it trying to read what the user are thinking and interact just using by thinking it. I think that will be coming up in the future. About smart home security, what I've seen a lot is there are new regulations that are coming up especially regulations concerning security for example in the UK, when you purchase a smart home device, there are initiative telling you that the device should have a good password protection and not be shipped with default password. There is also GDPR made in 2018 which also help in terms of security and privacy that need to have a certain baseline of security and new standards come up. When it comes to product, I think there is a lot of AI being use in some of the recent smart home technologies. There are dedicated devices that you can connect to your network. Then, these devices can be used to get some baseline behavior of the house holders and then sort of like connect or disconnect people depending on the activity. If there's any malicious activity, then these devices will take care of that. Recently, I see a lot of research going on into using AI with cyber security in the IoT in general.

4. What developments do you foresee in the smart home security area in the next 5 years?

a. Which of these developments would you consider most relevant to your own role, and why?

I think AI is a very important tool because smart home is interconnected. Now, there are more protocols that are open and different devices are communicating with each other. In a way, security should evolve in such a way to cater for these differences in the device. For example, a device which is not powerful such as a sensor that just detect the presents of people. Because IoT is a huge spectrum of devices such as sensors which could be at the lowest level of functionality and sophistication, then you have a more powerful devices such as smart home gateways, robotic vacuum cleaner, and drones. So, the spectrum of smart home devices is very varied. The question is how can we design a security in order to cater different types of devices from the weakest to the strongest device and can we use AI for that? I think AI should be the technology for that as we move forward. You tend to have a variety of users so you may have a user that's not technical at all like your grandparents, then there are users that are quite technical such as maybe you and me, then the question is as these devices are integrated into your home, how can we raise awareness to these people and how can we provide security to different people with different expertise of security and technical awareness? That's really a challenging thing to do. So, AI can help in that aspect about how to tailor security to be effective to different people. That's is one of the challenges of security. In the technical challenges, if you have all these different devices then how you create a solution that cater for a low device such as a sensor to more powerful device such as drones. That's a challenge plus with different protocols.

Could you explain more how AI will play a role in security?

When you have a really long password, you could say that you are secure but you might forget your password because it's long. When it comes to an effective security, it has to be usable. So, by having a lot of security, then the smart home devices may not be usable to different user groups. So, I think AI in the next 5 years can help in making security more usable for different user groups that are present inside the home. There needs to be a more open protocols when it comes to security. Smart home uses a lot of cloud technology for a device like Amazon Echo, then the device doesn't have all the voice recognition software it in so it needs to communicate with the cloud in order to translate your voice. The smart home, as far as I understood it, you need some kind of cloud technology for these devices. Cloud security is a very important aspect for the next 5 years in smart home so having a security deploy in the cloud is really important. So, you can protect your smart home from the cloud. The more devices and more integration there is, the cloud plays an important role. In the next 5 years, cloud security should be a priority. Also, another thing to consider is that you don't have to solely focus on the cloud because, as a researcher, we know that there is an important of edge computing. Meaning edge computing is that you are no longer relying on the cloud to off-loading the devices with the cloud because there are more powerful devices. Because these devices are becoming more powerful, you can do some computation in that particular smart home devices rather having to go to the cloud. So, perhaps in the next 5 years, in addition just focusing on the cloud security, you also have to focus on edge-to-edge security, meaning to have security build inside the device. The thing that would connects all these things together can be AI or machine learning

5. What do you think is currently the most likely attack vector in a smart home?

They tend to be from the simplest things like hacker trying exploit the weakest link inside the smart home. I think the most common one is the human factor in this case would be the password. Users tend to choose a simple password to connect to a device. Then you have a tool such as Shodan search engine, a search engine for IoT devices, and you can use Shodan to find how people are

securing their IoT devices. The point is the human factor in a sense is weak password, it can be one of the factors. When it comes to what can be the target can range a lot. One of the examples that I read a lot is smart home router. That can be a good target because once a hacker gets into the router, then there is a chance if the devices share the same network especially if they have weak passwords, the hacker can jump from one device to another. Typically, the attack vector can be as simple as like default or weak password, or insecure configuration. So, insecure configuration is the key here especially if different devices connected to the same network.

6. Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam

When it comes to security in general, we have to distinguished between academic attacks and practical attacks. Some of the research that researchers do in the lab, some of them never materialized in practice. Of course, researchers have to do research and find the vulnerabilities before they become a reality. Some researchers that I've worked with, we did research on cameras, locks, and we found vulnerabilities in them. If the vulnerabilities materialized or not, we don't know that but as a researcher, we have to responsibly disclose what they found to the companies and tell the company to address the vulnerabilities. For example, researchers found vulnerabilities with minimal resources and time, then there is a possibility that the vulnerabilities will materialize in the real world if it's not already been exploited. So, this depends on how committed and what budget the hackers have. Some of the academics discover, like protocol related stuff, probably they have already been exploited without a lot of people knowing them. So, yes, this attack can happen. Then again, we need to distinguish between theoretical attacks and attack that which are practical. For example, theoretical attack such as when we talk about encryption, we talk about AES which is the modern workplace for symmetric encryption, or we talk about hashing function like SHA-512. There are attacks that at theoretical level on those functions but to materialized in the real world, they will take years to occur. So, it really depends on what researchers are doing in the lab but from experience, some of the attacks, they can manifest in the real world if not already there.

7. What are the most frequently reported security incidents that you know of or you've experienced?

I think DoS is one of the incidents that happen to IoT in general and also in smart home. So, DoS attack is when attacker try to access a device, for instance a smart lock, then suddenly you don't find this device available. In smart home, this can happen. For example, when there is a cloud service, then suddenly the cloud service or the company is down. Then you try to access a device such as a lock or camera that connected to that cloud service, then suddenly your devices won't work because the devices are not available. DoS attack can also happen in IoT security like what we've seen with Mirai botnet. So, Mirai botnet is basically, it formed into a huge botnet consisting of many devices and most of these devices are smart home devices ranging from refrigerators, coffee machines, etc. These devices form into part of the Mirai botnet, then they were used to take out a website. So, DoS attack is one of the heavy hitters when it comes to IoT in general and smart home.

8. What vulnerability do you think is the most dangerous in a smart home systems?

This is depending on what you mean dangerous. If it dangerous in terms human life, you would consider safety risks. There are safety risks depending on the use case that the smart home is

satisfied. For example, there are different smart home services like entertainment, energy, safety and security, healthcare, etc. We see a lot of services now like health care inside the smart home. If you think about what kind of devices that this use case uses, such as blood pressure monitor, or insulin pump. Consider insulin pump you use in the smart home, what if this device gets attacked, you might get the wrong insulin and it can possibly kill you. So, it really depends. Also, there are more cases like this for example, smoke alarm. Imagine if it's attacked and it cannot detect if there is a gas leak inside your home. That is dangerous because it can kill people. When you have a device which becomes unavailable, so availability and integrity, they can be the most dangerous attacks.

9. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box

The company can offer you product and/or services that they can help consumers to improve security. These devices that you showed me seems like a dedicated computer or device that you can use like some kind of firewall/intrusion detection system that protect all connected devices. So, yes, they can help the users. If you have a device such as a sensor, you would not be able to upload an anti-virus on the device because it's not that powerful because maybe it doesn't support operating system. So, in that case, these devices are protecting smart home devices so it's good. However, at what cost, in a sense that how is the data such as "what is this product doing with all my data, what is the company gathering about me". So, you maybe say okay to security but then what about privacy. There is more than one way to protect smart home devices such as through the product that you gave as example, it can be also through the cloud services. I think what we should focus more is education or guidance. It's nice to have third-party security companies to offer some help with their product but it's also nicer to educate the consumers who are purchasing the smart home devices on how to use them securely. If the consumers want to use the third-party security companies' product, which may be good and maybe not so good, then how can you be benefiting even more from using smart home devices without having to sacrifice other aspect of your life such as the privacy. So, it's a matter of trust.

10. Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry

I think the answer is clear as everyone should be responsible to the smart home security. Everybody should play apart from the consumers, up to the government. Of course, the government should be the driving force as they can regulate the manufacturers and the industry. The consumers also need to responsible in a way like they need to be careful what they purchase and learn on how to use the devices. The manufacturers also should help the consumers in guiding the consumers. I think you forget a very important component, the service providers because maybe they are taking care of the security. So, there no rank and everyone should be responsible. If you put the government as number one, then where are you going to put the consumers? They need to be at the same level as the consumers need to shop properly and to use the product securely. So, all should be on the same rank.

11. Would you like to add something?

What I would like to add is that you are focusing on security, which is fine, but you cannot ignore privacy because one of the if not the most pertinent threat when it comes to smart home is the threat of privacy. When it comes to privacy, there are a lot of issues such as profiling, building your

information and trying to anticipate your needs and then use that to recommend your product or maybe change your behavior. So, you need to be secure in order to be private so it's good to have security but it's not all about security. There is privacy which is very important threat in the smart home. Such as there are voice powered devices inside your home and may say these devices are secure because it's made by Amazon or Google. However, what about privacy? Are they using my data without my consent? So, you can have a good security but what about privacy. So, you need them both in order for the smart home to advance to the next level. Also, the AI is becoming even more powerful. AI and machine learning becoming more in used in the smart home devices, more so than it was in the past. Because AI can be used for a lot of benefits such as it can anticipate what are your needs and help you more effectively but at the same time, AI can be the subject to more threats. We haven't seen the threat in the wild yet but it's still be in research because it's a new thing. We haven't seen them in the smart home yet, but I think it's because it's not reported to the public. But researchers are thinking and trying to find these AI threats.

Interview 9

3. **What is your opinion on the current state of smart home technology?**
    a. **How did smart home technology change over the last five years?**
    b. **What changes have you observed in the field with respect to smart home security?**

In the last 5 years, I think smart home change a lot because you have a lot of devices that control your electricity, alarm, etc. You don't need a lot of knowledge to install a smart home device. You can buy any devices that you like Amazon, Google and you can have your own smart home. In respect to smart home security, I think there are a lot of improvements but I think there is still a gap because the design in the smart home is not taking account of the security. You don't have security by design. I think there is a big gap in this aspect.

4. **What developments do you foresee in the smart home security area in the next 5 years?**
    a. **Which of these developments would you consider most relevant to your own role, and why?**

I think in this aspect is machine learning. All kinds of algorithm you can think of in machine learning and data analytics, focus with the application of smart home. So, both sides will be affected, for protection and for development of the application. For example, the devices learn your behavior in your home and trying to turn on and off the lights automatically. So, maybe in the future we will have an algorithm machine learning embedded in IoT devices. So, that's now the challenges on how to put machine learning in IoT devices such as lightbulbs. So, I think this is the course for the next 5 years, machine learning embedded on IoT devices.

5. **What do you think is currently the most likely attack vector in a smart home?**

It's complicated because I think in smart home, it's difficult to define the most common attack vector because in IoT, there are so many layers so you have attack in physical layers, network layers and application layers. There are so many technologies as well such as Bluetooth, Wi-Fi, Zigbee. Each technologies have different attack vector. Maybe in physical, with sniffing attacks. Maybe in network or communication, you have DoS attacks. Maybe in application, you have malicious code injection. I think you have to define the most attack vector in each IoT layers. Maybe the most common attacks

are replay attack, DoS, eavesdropping, malicious codes. So, there are many options. All depends on what the attacker trying to get from the devices. I think replay attack and eavesdropping are more relevant today for smart home.

6. **Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam**

I think the researchers try to find vulnerabilities in the lab, it's a good approximation about what could happen in real environment. I think these kinds of attacks are not so easy to happen in real environment. For example, you have a smart lock installed on your door, so the attacker needs to be in physical range of your lock. So, it's not so simple. When you try to analyze data set for attacks on IoT in the labs. You don't have all the information because you only have a small data set. So, when you try to analyze in the lab, you focus on specific attacks or sequential message. In real environment, it's more complicated. For example, you can put your smart lights behind your router and behind your firewall. So, if the attacker wants to hacked into your light, need to pass your router thus need to pass your firewall. That is not easy things to do. Easy to do in the lab because you have the smart light and just hacked it but it's not easy to do in real environment. Some researchers tried to do the same attacks that they made in the lab and real environment. In the lab, it took around 20 minutes and in real environment, it took 1 hour to get the same results. So, it's not easy to replicate.

7. **What are the most frequently reported security incidents that you know of or you've experienced?**

I think it's when user know about your organization or your home and try to connect to your device. It's unauthorized user. For example, I leave my home and then there are people from China, Russia, US trying to connect. A lot of unauthorized people trying to get into your home.

8. **What vulnerability do you think is the most dangerous in a smart home systems?**

I think it's the not updated firmware. For example, you buy a smart light 10 years ago and there are no updates in the smart lights. So, you will have vulnerabilities either in physical level, or software level. The same case with smart TVs. For example, you buy your TV 5 years ago, you update the software of your smart TV. Then the updates stop, and you will have vulnerabilities in your smart TV. Another example is that you buy your smart lights 2 years ago, you buy Alexa 1 year ago, and you just buy a smart refrigerator. How do you keep periodic updates? How do you expect the consumers made an update? They are mostly not technological people.

9. **How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box**

I think the support provided by the third-party security company is good because they provide good solutions for the smart home. I think the problem that I see is privacy. You don't have any idea what these companies are doing with your data. It's a good solution but the consumers need to think that do they want to sacrifice their privacy for security. These companies provide good solutions for security in a smart home because you want a peaceful live when you own smart home devices. You don't want your cameras at your home to be hacked and have someone whisper bad words to your kids. So, these companies help me to have peaceful life in a smart home.

10. **Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry**

I think the first is manufacturers, second is security industry, third is consumers, then finally is government. I think the manufacturers is the one that design the device so they responsible to put security in the design. I think, they consider the security for the consumers. I think they are the most responsible because today, we don't have a complete regulation for smart home. They are the one responsible for a good security solution. Next, security industry because they are responsible for security development. Then, the consumers because they are the one that use the smart home. I think they are responsible maybe to complain to manufacturers or security industry based on maybe something is wrong. People will change their mind if they think about security, such as a better security from different devices. Finally, the government. I think the government need to make a regulation about smart home. I think it's complicated because the government don't know anything about the smart home because smart home is smaller priority for them. Maybe, smart city is more important because there are countries with smart city maybe Netherlands or Australia.

11. **Would you like to add something?**

I think machine learning will be use in the future. How are the machine learning will be use over blockchain for example for smart home security. I'm not an expert in blockchain. The problem with smart home is authentication of your devices, how do you control your smart light, or refrigerator, maybe use some framework of authentication. Maybe blockchain can be use for that or maybe another alternative. So, I think framework on authentication and machine learning solution for IoT.

Interview 10

3. **What is your opinion on the current state of smart home technology?**
    a. **How did smart home technology change over the last five years?**
    b. **What changes have you observed in the field with respect to smart home security?**

If you compare the car industry, the car industry is more advance, every car is smart. Home automation is not built into homes, so you have to added the fact that a lot of different solutions are not very mature yet. What change over the last 5 years is that major players like Apple with HomeKit, Amazon, Samsung, and Google investing in it. So, we get more and more products and more standard solutions. It's not quite standard yet but it's getting better and easier. Of course, there are new standards like Thread and Matter that might be a way forward. However, now, we still have to deal with all kinds of protocols, different devices, apps and so on. So, it's all kind of stuff. Maybe your washing machine is intelligence so it's using Wi-Fi with very strange particle that you can only use with the app that goes with your washing machine. Apple have something else, Philips's use Zigbee. So, it's difficult for end users to just start. They have to buy all kinds of stuff and have to change their home. For example, maybe you want to move your curtains automatically, you have to buy stuff and open stuff so it's pretty difficult sale for a lot of people. The IoT security in many cases is not mature. A lot of devices don't have any security, or they just publish everything to the cloud, and then you have to have an app to get it back which is dangerous because everyone will be hack. Eventually, there are also a lot of devices that lack security and privacy. For example, if you want to install a camera for your home, all the images and all the video streams are actually push to China or some

other data center that's own by Chinese companies. Then, you have to have a subscription to see your own streams. So, the video streams leave your house first, then it gets back. In order to have access to your own stream, then you have to supply your exact location, your birthday, your first name last name, and so on. So, I think it's really bad for most of the standards, there's only a very few companies that actually takes care of your privacy and security. Most of the devices are just open up a connection to the data center to where your stream go to. So, its really terrible.

4. **What developments do you foresee in the smart home security area in the next 5 years?**
    a. **Which of these developments would you consider most relevant to your own role, and why?**

I think more people will be aware that they actually opening up their home. They think they are making it smart, but all the data is just leaving their home. I think it's unacceptable. People don't know. Houses will be hacked. People will break into your house by means of smart home. Using Amazon or Samsung to open the door and get in. Of course, you have a problem and also they know when you are not home. People can hack into your camera and it's very easy. So, I think there will be a maturity thing going for coming years. Especially consumers, they will demand security on smart home devices and question vendors about their privacy policies. I think consumers will force vendors to be able to choose where to store the data. So, it can stay in your home just like it stays in your car. For example, BMW is not listening-in to what your doing while you're driving. So, it's only when you go to garage, they can do further updates maybe check some information. So, development I think there will be a central hub in your home that can store the data of your cameras, your energy usage, your alarms, when your doors open, etc. I think it's essentials because of the privacy and security of your home.

5. **What do you think is currently the most likely attack vector in a smart home?**

So, I think it's more of the devices that open-up connection to cloud and services. For example, there are many devices that send all the data to the cloud and they either open a port or ask people to open a port or install open port to homes. So, it's actually the controllers and the hubs that are making the protocols vulnerable because there's so much logic added to it and it's stored in the cloud. I think that's a problem.

6. **Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam**

Yes, these things can happen. Some devices don't have any security. When you buy something cheap and think that it's protected but it's not. People start buying stuff from bigger companies that have the security for their devices. So, there might be patches that fix issues. For example, you bought a nice speaker, so it's not just one device but the entire network is exposed. In [my company] website, there's a report when somebody scan a port and use for KNX. Many systems integrated have remote access to the configuration of the KNX system and then open a port and leave a port open. Even though KNX, the protocol, and all the stuff is wired, it's secure because it's physical so you have to be in the house to get there, because there's a controller because people buy a control to add to such a system, then open it up to the internet and it's become unsecure. Many cameras are open, and many people don't know about it. I think they're using an app to watch the stream from their home but also works when they're not home. So, you wonder so, how it can be stream from data center then

back to you is a vulnerability. If you want to have remote access, then that's another thing you make sure to buy professional remote access, you have a VPN, you understand the security, and somebody maintains the keys. But, in most cases, it's not done.

7. What are the most frequently reported security incidents that you know of or you've experienced?

Well, I haven't experienced any attack in [my company] because it's not connected to the internet unless you choose to. We use very advance VPN technology. Like I said before, the report on KNX, I think there are 17000 households with KNX and KNX is super high-end. If you have KNX you probably a multimillionaire. It's really high privacy. But since it's integrated in IP gateway, there are hundreds of thousands of KNX systems, so people can access it remotely. These things, IP gateway, that sold by many companies, they don't have proper security. They allow just open up a port, don't have any password policy, or don't use high encryption. Because of that, people use default admin password. People buy expensive devices such as cameras and alarm systems, but they don't know about the little thing that open, so attacker can get to the controller or the heard of the system. The report, so they do a worldwide scan and found many of these installations that are not secure.

8. What vulnerability do you think is the most dangerous in a smart home systems?

I think it's network access so to be able to remotely monitor what's happening, then learn the behavior of the people in the home and know when they are not home, could lead to physical break-in. Physical access can be a problem if you don't secure it, but you need to be near the home for example with a Bluetooth lock, it's probably about ten meters. If you know what you're doing, you should take care of the keys and make sure the security of the devices is good. I don't think the threat is big when people are ten meters from your home and they want to use hack to get in, I think they would just break the door. When it gets bigger, it will happen just like what happen with cars where people picking-up the signal as you are opening the door. However, it's not big right now. I think in 5 years, that will happen where people will sniff about what is going on around the home, copy keys and try to get in. Now, it's more of a remote network related.

9. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box

I think it's very important. I think it's going to be demanded by law. At certain point, I think all this home automation systems will have to prove that they're actually up to standards. Now, when people buy stuff from Apple, they are probably aware that Apple is a very privacy and security aware company. If you buy a vacuum robot, well these people can make robot, but maybe the remote access is not up to date. So, I think whether it's Kaspersky, or TNL, I think there will be standards for smart home security. So, there will be certifications. I don't want to hire these companies to make sure that their homes are good because it's too expensive. Maybe in the KNX, it will happen, or it does happen. I think it's going to be a thing that vendors need to arrange, and I think by the EU law, this things will have to be approved that they are up to standards and maintain the standards.

10. Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry

I think the first is the consumers responsible because it's their home. Second is the manufacturers because they should be trustworthy and be able to prove that they respect the consumers. Third is

the government because I think they need to make sure that whatever consumers are expecting is actually can be proven by the manufacturers. I don't think the government will be active there so that's why I place them on the third. Finally, the security company is last because it's their profession but it's not their responsibility. I think they should be monitoring what's happening, monitoring new standards, do surveys, reviews of stuff and make sure that they create awareness for consumers and warn manufacturers when this thing not happen. Maybe they can also assist the government on setting up standards.

11. Would you like to add something?

If you buy anything, make sure that you have the right and the possibility to check what's happening with your data. For example, you buy a smart washing machine or smart light, make sure that the vendor assesses something about the security vulnerability and some of the privacy because security policies are very hard to read, and says something at the end about they can do anything with your data. [my company] is one of the exception, I think. When you buy something from [my company], we send it to you, but we don't register which product is send to what customer. So, we don't know what product you have, we don't know where you live, we don't know how many traffic there is, we just store everything on the product. You have a database on the product, so all the history stays on the machine and it's a very powerful machine. When you want to do software updates or maybe support online backups, if you want that, then you can and will be warn, we will say "okay, this information is going on the cloud. We explicitly explain how the security is done, whose owner of the keys, etc."

Interview 11

3. What is your opinion on the current state of smart home technology?

- **a. How did smart home technology change over the last five years?**
- **b. What changes have you observed in the field with respect to smart home security?**

The technology changes a lot in the last 5 years like Alexa and Google Home. I started dealing with home automation in 2010 when the systems still using a lot of buttons and no voice activation yet like Alexa. With the increase of internet usage over the years, there's a tremendous increase in appliances available that you could buy from lighting and alarm. So, the applicability also increases as you can just use your voice to activate it with Alexa such as opening the curtains and turning on the lights. I believe the younger people starts getting these smart devices for their house. Most of the devices are plug and play. So, the consumers leave everything to the big companies like Amazon or Google and trust them. What I understand from my personal research is that Google has everything about you or your habit from all of these smart home devices in your home. What I noticed from my research with Google smart assistant is that, of course the unencrypted data, Google has it such as our voice, habits, everything. Even if the data in encrypted, when attackers try to get in and intercept the command, the attackers can understand it because of the package size, the habits of people living in the house. So, in terms of privacy, it's dangerous. This is one of the major issues in smart home. You lose privacy with these devices. In terms of hacking, if an attacker enters with any route in the house, you will not find the attacker because there are not a lot of network in cyber security. So, big challenges coming in the next years.

4. What developments do you foresee in the smart home security area in the next 5 years?

a. **Which of these developments would you consider most relevant to your own role, and why?**

The most important is privacy which is, to be honest, I don't see a lot. You see news about Facebook that they will close in Europe because of GDPR. In Europe, I think GDPR is a good thing. Now, how would you apply GDPR to other companies like Google and others that produces smart home devices, this will be a great challenge. I think, the most important development is to have homomorphic encryption in these devices where the user that has the device is the one that control the data. So, Google will not know about our habits, our voice, etc. but they will be able to execute what we ask for. So, this is a big challenge that I see develop in the next years which is something more on the privacy of the users but not much on the security part. In terms of the security part, there are many new products coming that comes with firewalls running on the device that do a better detection, better isolation of the device, finding malicious act on the devices.

5. **What do you think is currently the most likely attack vector in a smart home?**

It depends on the smart home. If the smart home have a firewall, I would say phishing. After sending an email, when people click on it, it will download the malicious code or malware and the attacker can enter the smart home. I say that the attack in smart home nowadays is through the users because of the lack of education or guidance to the users. Most of the users don't know anything about cyber security and they don't know how to work with cyber security. So, the weakling is the people.

6. **Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam**

Yes, it can happen. Generally, if the devices could access the internet, it could be hacked with one way or another such as remote exploit, etc. especially Wi-Fi where hackers don't have to enter the home network because it's already available, you can hack it easily. Even if it's just radio signals such as Wi-Fi, Bluetooth, etc.

7. **What are the most frequently reported security incidents that you know of or you've experienced?**

Ransomwares. So, basically hacker hacked your device and encrypt everything so you cannot use it. Then, they ask for money to unlock your device back. The more data they save, the more money they ask.

8. **What vulnerability do you think is the most dangerous in a smart home systems?**

There are many of them depending on the criticality in the smart home system that you use. Remote exploitation is the worst and most dangerous because you can exploit software inside the smart home devices and install whatever you want. For example, you have a smart meters and attacker is hacking into your smart meters. Instead of stealing your energy, the attacker decide to put his energy bills to your house especially if you live close with your neighbors. Maybe you can take advantage of your neighbor and send your bills to your neighbor. You can send different readings from your device and your neighbors.

9. **How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box**

In the Bitdefender box description, it says that they include VPN for extra privacy. It means that Bitdefender use VPN to steal your data. So, that's one that I see from Bitdefender. If the VPN activated and use in other devices, it will take more bandwidth. I don't know how much work they do with encrypted traffic, but I believe they do nothing. So, if I use encryption, they will see nothing. Generally, that's the main problem of all the smart home devices. That's the reason we need new technologies in terms of protecting infrastructures. That's the reason, this kind of third-party security devices solutions are good but not robust because there will be encryptions. The trickiest part is to be handle the encryption. For example, if Bitdefender box is handling the encryption communications, then after the box and the smart home devices exchange keys that the box has, then the box bypasses the encryption issue, and then the box will see inside the packages, and then, the box can really see and identify the threats in the package. That means the box is injecting certificate in your network in order to monitor your traffic. Then, we come to the privacy issue because it says in the Bitdefender box description "includes VPN for extra privacy" which is questionable. For whom is the extra privacy? for Bitdefender which has all the private encryption keys? So, that's the main issue here, privacy and also encryption. How are they solve this issue so that users has privacy and also devices to be protected. There is a plus and minus between these two things and hard to choose 100% on privacy and 100% security. You need to compromise privacy sometimes in order to have a better security or sometimes the opposite. It's a good try by these third-party security company but I don't know exactly what they do and what they are monitoring and what they get, but at least it's a good try because it's needed to have a extra protection on the network level. Furthermore, I'm not sure how the security devices are scanning for malicious activities but it's good for virus, but how it works, it needs to be tested. I'd say that it's good that these third-party security companies considering the consumers that they need something more advance to protect their devices.

10. **Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry**

Government is first, security industry is second, manufacturers third and then consumers is the last one. Government should have policies, for example all products that enter UK or Netherlands should have a random password of twelve characters and not "admin admin", so should be random username. That's the policy that the government should implement. So, government will not accept any devices that are produced without following these policies. Then, the security industry is the one that proposed security solutions to the devices that are good, but they also need to be active in suggesting better alternatives. The security industry also needs to produce security devices to further support the smart home devices or accompany the products that are released from the manufacturers. Then, manufacturers need to listen to what the law and policies from the government and also what the security industry is proposing. If manufacturers cannot apply their own security in their devices, they need to collaborate with the security industry. For example, one device is supported with Norton so in order to use it in the consumers house, they need to have Norton. Finally, the consumers have the product, install them and everything is okay.

11. **Would you like to add something?**

No, I don't think so.

Interview 12

3. **What is your opinion on the current state of smart home technology?**
    a. **How did smart home technology change over the last five years?**
    b. **What changes have you observed in the field with respect to smart home security?**

I think in the last 5 years, there has been more of integrating with some of these smart home hubs such as Alexa and Google Home. The other change in the last 5 years is as more devices become more available and more connected to the internet, there's been a lot more work in identifying security faults or security vulnerabilities in this area. I think what hasn't happened, that some people hope would happen, is there's been some clear standards for smart home systems that would provide security. I still think that hasn't happened at all that there aren't really good systems. The only default systems are what you get from some of these smart home control systems. So, you get things that are compatible with something like Google Home but that doesn't mean they have a very good security. The changes with respect to smart home security are that people are now more aware of some of the vulnerabilities of these systems but we haven't seen a lot of work in good systems for removing those vulnerabilities.

4. **What developments do you foresee in the smart home security area in the next 5 years?**
    a. **Which of these developments would you consider most relevant to your own role, and why?**

So, I think it would be developing some real standards and also some clear ecosystems where all the devices meet some standards that would allow them to operate securely. So, that's what I think should happen in the next 5 years. I think one of the issues that could also happen in the next 5 years is that the smart home security area will move from just being fringe area to a more significant area. Even with some of the devices such as Google, I think that the penetration of smart home technologies still at hobbyist level. It's something that interesting to have but it's not really critical to anyone. One of the potential areas where smart home systems could be more useful is in things like energy management. So, it will make the difference in the sustainability of the houses. In the security area, I think people would become more aware of the security vulnerabilities of the systems. Thus, hopefully will force manufacturers to produce more robust and more secure devices for the smart home.

5. **What do you think is currently the most likely attack vector in a smart home?**

Currently, it seems to be a combination of wireless communication and poor security. That's one of the most likely attack vectors is for Bluetooth enabled devices or Wi-Fi enabled devices. Then, if people can get close to the smart home and get access to the home through improperly secure wireless connection, so that's one vulnerability. The other vulnerability is the lack of good password protection. So, you must be familiar with some of these smart home attacks like Mirai botnet. So, for the Mirai botnet attack is because people hadn't changed their default passwords or hadn't changed it into strong passwords. So, that's also a likely attack vector. That one, I think, is the most likely one at the moment which is the lack of using the security features that are actually available such as changing the default passwords and appropriate setup. The reason why those attacks vectors happen which is something that researchers have been looking in their research, is because if you are

building an IoT systems at the university, then you would have computing professionals setting up the security systems. On the other hand, when you at home, you don't have it. Most people have no idea how to setup the systems properly so that it's secure. So, that's why those attack vector works in that scenario.

6. **Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam**

The one that you mentioned are the ones that are hypothetical ones. So, researchers have shown that it's possible to do this. So, the baby monitor one is a possibility because it's something that really happened but the light and the lock one is just examples where researchers have shown that it's possible but it's not clear if attackers have done that. Other examples probably something like hotel locks with key cards where people managed to crack those. Some people get physical access to the hotel key, manage to hacked it and extract some information out, and make your own cards that give you access to. In this situation, it was quickly patched by the manufacturers. So, these things are possible especially the security cameras because it almost requires no work at all. So, yes there are a lot of these attacks that are possible in real deployment. Another vulnerability is the patch for these smart devices. For smart home devices, you need to patch it manually and not many people know if there is a patch or not. For example, the smart lock example that you shown me, not many people that there is a patch the next day after the exploitation unless people active reprogram their door locks. So, this is one of the vulnerabilities on how to automatically do the same level of patching to your PC to these IoT devices.

7. **What are the most frequently reported security incidents that you know of or you've experienced?**

When you look at security, you can look at different aspects of security. One is confidentiality where only those people who want to see data can see it. Another aspect is authorization which means only those people are allowed to control AC to be able to control your AC. So, normally in computer systems you have passwords, and you have to log on. So, how do you stop that access? If you have a smart home system, then you want to make sure that you always have access to that because if you have a smart door lock and suddenly there's a security intrusion and everything stops working, that's not a good way to go because people want to have access to their system. So, what do you do when everything stops working? So, everything in your house controlled by smart home controller so what happens if the smart home controller gets hacked or can't recognize your command. So, it's basically DoS attacks and there are variations for DoS attacks for smart homes. For example, DoS attack that target devices with battery and make that device ran out of battery faster thus it doesn't work anymore, or it can jammed a Wi-Fi systems. So, the most reported ones I think is the confidentiality because it's pretty easy to see what people are doing in their smart home especially the cameras. The reason either because the cameras haven't been secured or some vulnerabilities that have been exploited. I haven't seen any example such as the smart lock to gain access to a house to steal something. So, I think the most reported ones are the unauthorize access for cameras that leads to lack of confidentiality.

8. **What vulnerability do you think is the most dangerous in a smart home systems?**

I think it's probably the same one which is the lack of confidentiality because smart home are probably not yet critical control systems. In other words, it's not the only way you can do many things such as if your smart lock doesn't work, you probably have a key as well. However, once a system like that becomes critical, then I think the most dangerous ones is DoS attacks because when that happens, your home won't work at all. If you do a DoS attack and the only lock you have is a smart lock, then the system has two choices. One is that everything stays locked, no one can get in or out, or they become unlocked, everyone can get in or out. So, DoS is the most dangerous one where it's hard to know what you would do if your house depended on a smart home control system that no longer works. If the vulnerability is about confidentiality like something from cameras, then what cause them is probably because people haven't properly secured them. Usually from the users that haven't properly set them up or sometimes it's vulnerabilities in the devices themselves but for the most of them I think it's cause by the users that haven't set them up with adequate security.

9. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box

I think they have a big advantage that you have one place for all security sits. This is a little bit similar to the work that we were working at, where our approach to smart home security was to put in a gateway device which is what these devices are, a gateway device. However, it does stuff that making the devices a little bit insulated from the wider internet. I think, the biggest danger from smart home devices is the fact that the devices are connected to the internet. The security devices act like a firewall type device that prevent access. However, it's only half the battle because you also need to make sure that the security devices themselves are secure. A big danger for these devices is the conflict in making things easy and making things secure. Often what happens is these systems will automatically identify all the devices that are on your home network, so one way to get into the home network is having a fake device that also connects into the system. So, how do you make sure that you can identify fake devices? Another thing is for the device how do you make sure that it's really talking to a hub and not a fake hub that someone else has? For example, you switch off the power of all the devices, so everything stops. Then switch it back on again and everything will reconfigure, but when that happen, your phone is now the hub, and not the real hub. So, there's a whole of protocols in things you need to put around there to make all of these things secure. So, I think a gateway type device is the best approach for providing home security, but it will be best if it's integrated with some of the controllers like Google Home controller. If they specify protocols to make sure all these devices could connect securely, that all these devices could have firmware updates, and also takes care of the password problem such as updates the passwords in the smart home devices into strong passwords. So, this approach puts in a gateway but doesn't improve the security of the smart home devices. So, I think these gateways are design to allow anything to connect to them. Where as Google Home systems, you have to have devices that are compatible to the Google home systems. So, we're going to have some standards and you have to be compatible with those standards in order to be part of the smart home. So, who's going to set the standards? I think it would be big companies such as Google or Apple and not the security companies. If they can identify standards that require a gateway, then they will also have control of the gateway. So, to answer the question, these sort of devices are the best that we have now but additional standards to make the individual devices and their communication secure would be even better.

10. **Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry**

So, I think the government can do very little, so I think they are at the bottom. The government is not going to mandate standards for home security. They could give suggested standards, but I think that's not government responsibility. At the top, I think, is manufacturers. Manufacturers need to provide devices and protocols so that the devices need to be made secure. Second, I think is security industry which really is all the manufacturers together rather than individually because they need to come up with standards. Strong security solutions require individual devices to make particular standards to allow them to operate together securely. It's unlikely that different devices from different many manufacturers can be made really secure. Consumers third because eventually consumers need to take some responsibility and most consumers don't have any technical skills.

11. **Would you like to add something?**

There is no easy solutions. You can't have something that is easy to use and also secure.

Interview 13

3. **What is your opinion on the current state of smart home technology?**
    a. **How did smart home technology change over the last five years?**
    b. **What changes have you observed in the field with respect to smart home security?**

There's been a lot innovation and a lot of big companies get into smart home. Big companies in the west such as Google, Amazon, Facebook are producing quality products that have good overall security but those don't really make up the bulk of the IoT its face. The majority of IoT devices appear to have poor security. We've seen they get exposed more. So, IoT devices always had bad security. Furthermore, the acceleration of the threats such as botnet that are targeting IoT shows that how poor the security is. In terms of change, people are aware of security for smart home IoT devices and consumers are more concern about privacy than security because there haven't been any threats to demonstrate the impact on their personal life or something that's tangible to them. Companies are trying to do better with security but it's a hard problem because it's not as simple as securing a device. I think at least, the big companies have hundreds of engineers that are dedicated to work on the product, build quality product with quality assurance, testing, and with security in mind but start-ups don't have those resources. So, we're going to have these gaps that will probably have negative impact on the security in many of the IoT devices. I think, there has to be a little bit of waking up call, maybe something like a big cyber security breach that abuses smart home devices and causes major outage or major impact for a sign of real change in this field.

4. **What developments do you foresee in the smart home security area in the next 5 years?**
    a. **Which of these developments would you consider most relevant to your own role, and why?**

I see smart home devices being more adapted and more available everywhere. They all going to be integrated in many new physical applications around us in the next 5 years. In terms of security, I don't know if the security will improve. I think, for some devices it will improve but the bulk devices will remain the same because of how economics work. For start-up company getting a product out in the market, having it visible in front of the customer is a more priority than actually securing it because it delays the product and they get beat to the market. So, it doesn't make sense for them to

priorities security. So, I think, we're still going to see security issues, probably growing security issues. I think, the security will start manifesting itself into different areas in the society, from hospitals, clinics, to industrial setting, even government offices. These smart home devices, they have the name "home" in them, implying to be at home but you can think of a smart home coffee maker. So, in a company, there might be multiple of these coffee maker and these are compromised, then it's a way into the network. So, I think these are the development that we're going to see, a lot of these smart home devices are going to be deployed in different industries such as for conveniences and their security flaws are going to impact these businesses in some way or somehow.

5. What do you think is currently the most likely attack vector in a smart home?

So, a lot of the botnets weaponize, security cameras, network video recorders, and devices that are usually expose in the internet, routers, are a big target. From my research, what I've seen is that there is a path where an attacker or botnet can actually compromise a router, then pivot into the local network and infect a home device. That's possible because a lot of the botnets that are out there, incorporate multiple exploits for different devices. So, they have the capabilities to pivot from one device to the other. Currently, I think the biggest target are routers, at least for residential. Then, I think the evolution is inevitable but what would happen is that once it gets on the router, they'll start scanning for other devices within the network to actually move there and be less detected from the outside. So, I think botnet probably one of the biggest threats. The other threat is probably insecure network. So, if someone close to your home or you have a smart lock and someone can actually get on your network, they might actually be able to unlock, have physical change and open the door, or disable a sensor. That's less likely than the bot situation.

6. Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam

Yes, absolutely. I've this in my research. I've seen botnets incorporate vulnerabilities that directly go after, for example Belkin. Belkin has a couple flaws in their smart switch that you can put in the wall and control an outlet to turn on and off. I've seen the exploits from vulnerabilities embedded in bots. So, they're looking for these devices. So, it's very real that if they are given the opportunity, they'll be able to actually take on one of these devices. I think the far-fetched ones require either hardware, modification, or a little more advance exploit, are less likely but they're still possible. For smart home, I've definitely seen a direct exploit for a smart home embedded in the IoT botnet.

7. What are the most frequently reported security incidents that you know of or you've experienced?

The most frequent is services. Any service that runs on the device or expose on the device, those are probably the most popular vulnerability security reported. There's a lot of these web applications and these web applications, they don't sanitize the input correctly and what would happen is that you can pretty easily exploit them and have your exploit download a malware onto the device. From my research, this is what I've seen as a most common security flaw. It's basically exploiting the web applications that are expose on the device. So, it's on the device itself and not the cloud. So, if the devices running UPnP, or running UPnP service that lets you configure the device or control the device, there might be a vulnerability in that UPnP protocol that will allow you to execute code on

the device. A router is famous for this. If you expose the management interface on a router to the internet, most likely there's a vulnerability and then that device that would get compromised.

8. What vulnerability do you think is the most dangerous in a smart home systems?

Vulnerability that would basically allow you to take control of a device. Most of the exploits that we see that target routers, they'll give you full control or give you root access to the device. I don't know because it depends on the device that you compromise, is it critical device, maybe if it's a lock, I can unlock your home and break-in and that's a dangerous thing. It could also be your oven because if it's a smart oven, I can turn on the heat and burn down the house, that might be a physical damage. It's hard to say because I wouldn't be able to give you an exact answer to that. It's relative to the device and it's functionality and the damage what it can causes.

9. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box

From my experience, there's two issues with these devices. One is that they are smart device themselves, so they are vulnerable to being exploited and actually being a point of weakness in the network because they see everything. Two, it's really hard for you to tell, let's say vulnerability is being disclose for August smart lock, how do these devices quantify that vulnerability and figure out like "we should alert home owner to update this". I don't know third party solutions can actually have a way to help with that because there are so many devices. There's a challenge of actually figuring out what's on the home network. That's not an easy task. Second task is actually how to determine what's on the network that's vulnerable, that's another hard task. The third hard task is how to determine if the vulnerability is critical, is it something that has to be done now because it's being exploited or being abused. All these things are very hard to answer because they are high level, and they seem simple. When you plug a device like that, all it is really is a firewall. It has signatures and looking for certain signatures, looking for mass scans or looking for traffic with DDoS, etc. that's what it's looking for. Many of these do-it-yourself routers actually have these firewall stuff. So, I don't know how much added value these security devices would have. I personally don't think that anti-virus companies have good detection systems. They do an "okay" job, just being able to detect what's known out there but when it comes to a new attack, I don't think it'll help much. I think, vendors are the one who can probably make a change, but they're not incentivize economically to make a change. So, the only way to do this is to convince the customers to buy security devices. Then, to buy security devices, you have to educate the customers about what is a secure device. So, it's a little complex and I think, that's where government needs to play a role. So, I think these third-party companies are just capitalizing on the fact that they know that this is an issue, and they say "hey, we can sell an added value here". But I don't think it will actually put a dent into the smart home IoT security field.

10. Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry

I think, manufacturers should be responsible because manufacturers right now, they're putting the responsibility on the consumer, to make that decision. I don't think it's the right way to go because this is also done different areas. For example, recycling, in the US, food manufacturers, when they sell food, they sell it in plastics that can't be recycled or can be recycled in a way and they say "hey, that's the consumers problem. They should be able to recycle and take care of it" instead of the food

manufacturers solving the issue at the root and say “okay, we’re not going to use plastics, we’re going to up the cost a little bit and use something that’s biodegradable, good for the environment and it’s not the consumers issue anymore”. When you put it in the consumers hand, it’s not going to go anywhere. Consumers are driven by different economic incentives and it’s not going to solve a problem this big. I think definitely the government plays a role, so I would rank manufacturers, government, I think the security industry can be a valuable partner for manufacturers. So basically, integrate some of their pre-existing solutions and give insights on how to protect this. So, some type of partnership between security industry and manufacturers. If I have to rank it in this list, I have to go manufacturers, government, security industry, and consumers. I think the consumers need to be educated. Security is not easy, even to experts, it’s hard. It’s not something you can quantify easily. You can’t say “this device is more secure than this device because it has xyz”. It’s a much harder problem, it’s like a risk tolerance and with consumers, I don’t think they can perceive risk correctly. When government passes a mandate and say “any smart device that’s sold to consumers has to meet these qualifications such as the password has to be change, it has to automatically updated”. Manufacturers have no choice but to comply because they can’t sell their products. Even if the cost goes up, it doesn’t matter. Now, I think manufacturers thought that they don’t need to update the device because the consumers buy it to solve a certain problem. A lot of people will not revisit the device, they will revisit it when it stops working. So, it’s less in the consumers hand because there’s that knowledge gap and they don’t have much of a choice. For example, I’m knowledgeable about technology and I have a poor security device, I can’t do much about it because the device is locked. I can only interact with the interface, so what if there’s a vulnerable service on it, if I turn the device off, the device won’t function. So, the consumers don’t really have control, but they’re force to put it in their home because they’re looking for a certain feature. So, that’s why I ranked the consumers last.

11. Would you like to add something?

Smart home devices seem simple, but I think, we’re not fully understand the possibility of abuse that could happen. With my research I look at both the security flaws and the attack such as malware and botnet attack that abuse those flaws. So, you get to see both perspectives and the urgency of things. You could imagine a vulnerable thermostat in everyone’s home and if I could compromise a subset of them such as 30-40%, I might be able to manipulate power consumptions. I could turn on and off other people AC and cost surges in certain areas, disconnect electricity and attack the grid. The grid is protected very well at the power production area where power gets produce and generated, but the end point where it’s being consumed have no protection so that’s like a reverse DDoS that could happen on the grid network. There’s couple of papers that have demonstrated you can cause surges, you can manipulate prices for energy and benefit from them. So, I think these attacks, they seemed far-fetched, but I think within the next few years, we will see them.

Interview 14

3. What is your opinion on the current state of smart home technology?

- **a. How did smart home technology change over the last five years?**
- **b. What changes have you observed in the field with respect to smart home security?**

In general, the smart home technology has changed a lot in the last 5 years, like exponential changes. 5 years ago, there was not much a lot of technology such as Alexa or Google Home. Even if there

were technologies like that, at least they were not in every home like you can see in the post-pandemic era. Other example like smart bulb, this is one of the first thing that came into smart home because there is no motion needed and the bulb will automatically turned off to save energy and electricity bills, another example is smart cameras. Those examples were the first that came into picture as a smart home technology. You can control and see who is coming to your home from outside or a baby monitor. So, these kind of devices that actually came to the market and people started using it in the early days of the so called smart home technology. But those devices are very faulty and there are many reasons for it. Most of the IoT devices at that time, they came with a buggy code and the main reason is that, at least from what I know, the companies compete with each other a lot, even now it's a very competitive market. So, two things that are very important for those companies, first is you have to be the first and second you have to be the cheapest, in order to capture the market. These two things together make you have to sacrifice things in the process such as you don't do the coding properly or don't do the testing properly. I think from the monetary perspective, testing holding the product to be in the market, so manufacturers don't like that phase a lot. In my opinion, the manufacturers don't do testing properly or do a deep test considering the costs. So, those software and codes are open and easy to hack into. You can see a lot of papers that discuss about security issues such as baby monitors or security cameras and one of the famous attacks was Mirai botnet where it captures millions of security cameras and made them into cyber zombie. In the early days, when you buy something smart, those products come with default user ID and password that's written on the product and most users never change their default ID and password. It's very unlikely that users would log in into the management system and change the user ID and password. So, for hacker, it's very easy to know the user ID and password of a particular product. I think, the problem with smart home is that people want everything into their hand such as all the apps in the mobile phone. This work two ways. Hackers somehow get into one of the smart home devices, because the devices are interconnected and communicate with other devices, then, the hacker can manipulate all the other smart appliances. For example, smart refrigerator tell the users what groceries they need or pay in advance, so this is another way for hacker to get into the users' bank details. There was a famous incident in UK where hackers get into the smart camera of a smart TV and they had recorded people's personal or intimate activities and uploaded into a website, I think it was in 2016 or 2017. So, it's very easy to get into the camera even if the camera is turned off. So, in the last 5 years, one thing for sure has changed is that people are more concern about the security and privacy.

4. **What developments do you foresee in the smart home security area in the next 5 years?**
    a. **Which of these developments would you consider most relevant to your own role, and why?**

I think the security will take the front set because people are more concern about security. During the pandemic era, we had seen so many banking fraud or messaging app fraud where people lost money and a rise in cyber-crime. It also has economic impact because people losing their jobs in such a way and the cyber-attack is a lucrative business, so people are drawn into this area like scammers and there are many videos online where scammers tried to manipulate people to get their account and money. So, it's a business itself, it's a shady industry but it keeps growing in the background of the normal economy. So, the pandemic has aggravated the problem. In my opinion, people started talking about cyber-attacks and people are more concern about their data and how to secure their data. The manufacturers also change their protocols towards a more secure way of performing

business with their clients. So, I think security will be one of the main driving forces in the industry because people are more aware of it now.

5. What do you think is currently the most likely attack vector in a smart home?

I think it's the network. You can think of a smart home as a separate network and hacker tries to hack the network from outside. So, I think the network attack is always the first step towards more exploitation. Then, there is a buggy software, it comes into the second step, in the larger picture of attack scenario. For example, a smart home device that tries to communicate with other things such as smart refrigerator communicate with your grocery, placing all the products your need in your mobile phone. So, this is a message communication between two entities separately and hackers can snoop into those message network package, then they can steal information like ID, password, what things they are ordering, and make a profile about the user. There is another thing as well such as monitoring. Hacker can monitor the user's activity without having to get into their home physically by using something like how many lights are on, which lights are off. The hacker can find a pattern like if there are people in the house, the lights is on, microwave is on, and if there are no one in the house, the lights off, microwave is on, communications between devices is going down, etc. With this, the hacker can find the user's pattern of activity such as when the user's going to go for groceries, when the fridge is empty, who comes to the user's home and who goes out. Pretty much the entire idea of the user's daily routine. For that, the hacker doesn't even have to break into the home, and he can do it by just gathering the data. I guess, network monitoring is the first. I cannot give opinion about which one is greater like buggy software is greater, attack on network communication is greater because I think both work hand in hand for the attack to be multiplied.

6. Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam

I'm pretty sure there are multiple attacks that already happen in real development. The smart TV attack is a real attack and people not even know that they are being watched and monitored, the same thing happen with smart cameras and Mirai botnet because these are attacks that already happened in the real world. Most of the cases, people get to know about this cyber-attack exist is because it's happened. Sometimes, the research communities is a step ahead or the other way around, it's like a cat and mouse game. Someone suspected something so they trying to see if it can be exploit. However, most of the cases, the hackers or attackers are always one step ahead. For example, the smart TV hack, people get to know this exist because there were cases where people found out about their private information were uploaded to shady website. Then, police came into action and research communities started taking action. Sometimes, research communities found about vulnerabilities and found solutions to improve the security but unfortunately, most of the manufacturers do not implement on what researchers found in the lab. Money is the driving force of the economy. If the manufacturers think that it's necessary, they will do it, and if it's not necessary, they will not implement it in their system because the system will be heavy. Cost will increase, data size increase and the performance will be impacted. The lightbulb from your example, that's a physical attack and you need to get access to the lightbulb to do the attack. So, you don't necessary need that if you can get access to the network and break into the system. So, if you can hack into one lightbulb, you can basically get the entire lightbulb in the network. So, you don't necessarily need to get into the house to do the attack.

7. **What are the most frequently reported security incidents that you know of or you've experienced?**

Most frequently reported security incident is the banking fraud. So, it's always about people that are not use to the mobile banking because most of the bank are moving to paperless activity with apps, emails, etc. Old people or people that are not tech-savvy, they are being targeted for this kind of attack such as a hacker send a message say "your device is broken, please click this link", then they click the link and put their private information such as credit card data. So, I think is the most frequent attack and people keep on losing their money. The bank already doing their best to raise awareness such as saying they never ask for their credit card data, or debit card.

8. **What vulnerability do you think is the most dangerous in a smart home systems?**

I think it depends on the applications scenario we are thinking of. For example, Stuxnet attack which was a remote attack in 2010. So, it was kind of a remote attack in a nuclear plant so physically very secure. The nuclear plant is cut off of the grid, had its own network, so attackers have to breach an air gap in a sense that there are no connectivity between two networks. So, it was a mix of physical and network attack. Undoubtedly, if the attacker has physical access to the system, you cannot do anything. Even in our research, we always assume that if the attacker can get physical access or your device get hijacked, you can't do anything no matter what because the hacker can tear open the system, get the code, extract the key, and everything. So, the nuclear people put the server behind a concrete wall, it's a physical sense of security because if the attacker get into the server, everything is done. So, in my opinion, it depends on the application. If it's a smart home security, I'd say that remote attack is more dangerous because if its physical attack, you can know that the person is coming into your home or getting into your home such as you call someone and that person tears open your devices, so it would be notice easily. So, for smart home, I think remote network attack is make more sense and more prioritize.

9. **How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box**

It's a good start for normal users but they have limitations too. They can get hacked too. Furthermore, you are trusting a third-party for your security and you don't know what's happening to your data. For example, you trust a VPN company because they are secure but your activities are being locked into their system, their server. What is the guarantee that they are not sharing your information to other parties? So, basically you are trusting everything to one particular entity and it's even more dangerous in privacy because that guy can have everything. For example, you install the security device in your Wi-Fi router, that means all the communication through the router is gathered by this security device. From security perspective, it's good for smart home but from privacy perspective, it's not good. For me personally, I would not buy them because of privacy concern.

10. **Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry**

I think everyone is responsible equally. So, government has put laws and rules in place and force manufacturers to follow it such as GDPR where the European Union make it clear on what kind of data they can collect, and data they can't collect. So, the government should have a very clear, to the

point data policy so the normal people can understand. I can give you an example, before installing any software, so the company that give you service will ask for permission and if you don't accept their agreement, you don't have to install it. So, when you accept it, they can change the terms and agreement in the middle of your contract. So, there are some shady clauses and I'm pretty sure none of us read the terms and agreement. So, government should have proper policies in place. That's number one and number two is the manufacturers should be more careful and do more testing. Slowly but surely, they are trying to focus on the cyber security because if their devices got hacked, it will be a bad reputation for them. So, the manufacturers should be more careful about the proper security practices, testing, and development. They also need to keep on providing patch frequently because not everything can be fix from the get-go. Consumers should follow the instructions and security guidance such as change ID and password. People need to be more careful on what they are sharing online. Then, security industry has to be more focus on detecting the attacks that are possible, finding new ways to secure the systems. So, I think pretty much everybody equally has a role to play and this thing will not be working if one of them doesn't play their role properly. If one of them fail, no matter how good of a system it is, it's bound to fail. For example, when you open a website, you will get notification to accept or reject cookies. The government already put some restraint and it is the consumers job to play the role of not just accepting everything. So, everyone has to play their role because this is a team game.

11. Would you like to add something?

In general, more careful on what you share online. Be careful on what software you're installing. Be vigilant on what kind of website you are clicking because it could be a scam. Try to understand about cyber security better.

Interview 15

3. What is your opinion on the current state of smart home technology?

- **a. How did smart home technology change over the last five years?**
- **b. What changes have you observed in the field with respect to smart home security?**

In the field of smart home and the kind of technology, you have to know this technology exist already for more than 20 years. In the past, they used to be like some kind of close systems for variety of systems. Later on, there was some addition for communication for the rest of the world. Initially, it was just in the building and such but then the communication beyond the building happen in two ways, to the people themselves by mobile phone or remote control, and to the outside world. So, initially it was not so complex technology like SMS, dial-in modem, and so on, but now usually over the internet because most places have internet connection. Then, the problems came there. Initially, if you'd like to control something in your house, SMS was one of the popular techniques, you could easily send a message to somebody and vice versa, you could send an SMS to your house, then it's some kind of command which is always protected with some kind of password. That's how you could control things. You could also have dial-in modem and that became more popular but now it's mostly over the internet. The problem right now is that many people are buying cheap solutions and just put it in their home without thinking of the consequences. Most of those systems are not good on the protection level. In the past, a lot of care was taken for protection but these days, it's not. The users are actually a big issue because they just put the devices on the same network as their home

automation which make their home vulnerable. Of course, good solutions always are to protect the network and have different networks such as having intrusion detection in your network. However, the biggest challenge nowadays is that most people just download good looking apps on their mobile phones and connect it directly to their smart home, even buy equipment which not always trustable for example cameras that connected directly to the same network as their home automation system and very easy to exploit those devices. For the last 5 years, these smart devices and you think they are smart from the home automation point of view but up to some level they are like some kind of gadgets. They have some limited functionality, it looks good, and you can talk to it but it's not integrated in the whole building. There are other systems which are controlling the whole building, shutters, windows, and so on, and they have a different level of certification and things that are needed electrically. The devices that you have now such as Google Home and Alexa, are just ad-hoc devices that you can add to your home and maybe you can control one window, or one light, a few shutters but not a full automation of the home and also not a level of quality about reliability from electrical point of view. So, what has change? We now have a new wave of ICT type of technology in devices that people use in their home. The issue is that if you can take control the whole automation, then you can take control the whole building which has more impact. So, what has changed is that you have this kind of new devices that are very poorly integrated, and security not taken into account too much.

4. What developments do you foresee in the smart home security area in the next 5 years?

a. Which of these developments would you consider most relevant to your own role, and why?

I think we should think carefully about how to integrate this new technologies, how they relate to the building infrastructure and that deals with standards and security. I think, we will have a lot of serious security appliances including gateways and so on, so that you can make sure which type of signals can go outside and inside that you will have a much better control on it. Networking, monitoring, device management will be needed and the importance of standardization and certification of the equipment to make it more than just gadgets. We also have to educate the users to make sure that they not buy devices recklessly such as buy it in a budget store and connect it to something for example Alexa to mobile control system of their car and not in their house. So, education is important in this kind of security appliances, standardization and certification also play an important role. Probably, right now, most countries have some kind of certification of your electrical installation of your house so it's certified and checked. So, if we try to integrate this kind of new technology at the higher level, then some checks need to be done as well.

5. What do you think is currently the most likely attack vector in a smart home?

The cheap uncertified devices that people put in their home that connected to the internet without being aware of the security risks. The certified devices already an issue for experts because some factories were hacked in the past which has the same risk for smart home. The big risk is that people installing devices without any certifications, or any protections and they are connected to their home network. So, these uncertified devices are devices that have no procedure that make sure that these devices are reliable and have security standards. People also put these devices on the same network as the one that they use their smart phones, computers, etc.

6. **Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam**

Yes, it can happen. It's astonishing that these things don't happen much more frequent because there are so many vulnerabilities at the moment. So, this is a really big danger and something that should be taking into account. For example, places such as hotels where you can go into a room and if you know how to do it, you can make the room electrical systems going off including the elevators, lighting systems of the building, and the door. If it's only turning on and off the light is fine but if it's the attack is penetrating your network, then it's a bigger issue and if it's taking over control then it becomes a serious issue. Therefore, there is a need of good infrastructure inside your smart home to make sure that in case a problem occurs, it can only have limited impact and at last not be able to take over the whole systems. Furthermore, so many services are relying on the internet which is also makes it they are unreliable. So many services connected to the internet from different manufacturers that makes the maintenance and the overview of the security quite difficult. For example, the smart light that rely on the software that running on the internet that you need to have a user account which makes it quite vulnerable.

7. **What are the most frequently reported security incidents that you know of or you've experienced?**

Network intrusion, data sharing, and data privacy lost that some people have access to your private data where they should not have access to, they can see some things about your behavior, and that's a big issue. So, the data that's available outside of your home can be seen by third party. For example, Google knows about you, they have rough idea about you and they can profile you based on your data. That's quite a big issue because what if you have a data leak and you share a lot of your habits online, it can be use by attackers to do nasty things to your house or to you. So, the things that you want to keep private becoming not so private anymore because somebody else has access to that kind of data. Another example is network intrusion, where another party, a hacker, or some kind of organization that has access to your house because you have a network that makes the house reachable from the outside world in a way that you don't want. The consequences of network intrusion are that once you are intruded and attacker has access to your data, he can also control the infrastructure. Once attackers on the network, they can also control some of the devices.

8. **What vulnerability do you think is the most dangerous in a smart home systems?**

I think the connection to the internet, but this is also the nicest things about it. Data connection to the outside world typically the internet is a big issue because when it gets hacked, you can do anything you can imagine. So, we need a nice protection.

9. **How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box**

I think they are doing quite a lot of work, it's good and these devices are certainly needed. However, they should also have the possibility to look into the payload of different protocols. It's a good step and I think people already buy these kinds of devices. However, these devices need to be aware of the different payloads in different devices. For example, a good website that has good security systems not only checking which websites you visited but also checking about what you are

downloading from the website. Similarly, these devices will also need some firewall, do some checking about which sites can be connected, know about the communication of the systems in the infrastructure, and the protocols, how they do and how they are configured. Typically, these devices don't have that yet. So, these devices need to monitor the payload on different protocols such as monitoring payload in Zigbee and Z-wave. So, these devices need to look into the payload of these protocols and see what they are doing, and see if it's allowed or not. You also probably need device management such as the telecom company can look at statistics and have a look at abnormal behavior that has abnormal traffic such as traffic that should not be there or traffic size that is too big. So, smarter gateways that have some kind of intelligence that can detect abnormal behavior. I think that's needed.

10. Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry

I think they all responsible for security and you also missing a few players. It's not just manufacturers, consumers, security industry and government but there is also installer of systems, so there is electrician that come in and install your home electrically. These guys need to be aware of the new technology as well because there will be smarter devices such as smart shutter, the lightbulb, the gates, home entrance systems. There are so many things and these things should be installed so this people quite responsible as well. Also, education is quite important which is not on your list. If you would like people to have a better smart home security, then at least you need to educate them. There is also a must to check the certification as well so there should be somebody that does the certification process. There is also a need of something that make sure it's still running okay, so monitoring is needed there which is the job for telecom companies. I mentioned certification, and also standardization bodies is needed to make sure that the installation meet the standards that are needed. Device management is needed as well to remotely check what's going on and upgrade particular part of the systems in case new requirements are there or vulnerabilities are protected. So, much more than the list that you showed me. It's not one particular entity that more responsible than others. If there's a weakling, then that's where it breaks. Manufacturers, consumers, government and security industry are yes. Government should be there for legislations and put policies such as which standards should be applied. Security industry also play a role but for them it's usually business. Also all the others that I mentioned education, certification, etc. also play a role. So, all players have a role and they play different roles in the game.

11. Would you like to add something?

No, I don't think so.

Interview 16

3. What is your opinion on the current state of smart home technology?
   a. How did smart home technology change over the last five years?
   b. What changes have you observed in the field with respect to smart home security?

I'm a big fan of HomeKit devices. The reason I chose Apple like 5 years ago was because Apple was controlling the protocol and ways of how user communicate with HomeKit devices and servers. The alternative at that time was either Google Home or Alexa. Alexa for example, 5 years ago, Amazon

didn't have secure connection to clients as long as you implement some interface, for example for Amazon devices using Amazon Cloud function. In the beginning HTTPS was not even enforce and even if it did, the language or the protocol they use to communicate to Amazon devices itself was completely vendor defiant as far as I know in the beginning. For that reason, I chose HomeKit. HomeKit was not very advance 5 years ago. However, I don't think protocol change for Apple devices. For Amazon and Google, things improved a lot in 5 years. Still, what is not address by any of the big vendors is something like firmware updates. Firmware updates is something that vendor will decide how to do it. It doesn't matter how secure the protocol is if firmware verification procedure on the device itself has security flaws. Then, me for example as an attacker, I will be able to push some malicious firmware that will do things what I want. I think there's still flaws in all major smart home providers. There is thing called Matter protocol where big companies Apple, Google, and Amazon are working on unified protocols for devices in the future. It's still in work and there is no devices use that protocol yet, but at least they are working on a new standard and smart home providers can be interchangeable easily. Right now, if you buy a HomeKit device, maybe it will have Alexa support or maybe not. Definitely, if you buy Alexa that doesn't have HomeKit, it's not going to have HomeKit support later in the next firmware updates. So, this Matter protocol will help these devices from different vendors can speak the language that all the providers can understand and consumers can choose who to pair it with such as HomeKit, Google Home, Alexa, etc. For security in smart home, we can take an example from IP cameras. Long time ago maybe around 8 years ago, me and my friends did a research on IP cameras and one of our major find besides the actually vulnerability on the device was me as an attacker, I could push any firmware to this IP camera, which is a very slow and outdate Linux system running on the device, I could run any program on the device. The problem at that time was the IP camera provider, Foscam, even if they know about the vulnerability, they didn't have a mechanism to notify all users other than sending out emails. They didn't have a mechanism to force push firmware updates. There was no good way of validating the firmware that it actually came from the manufacturer and not from a random guy like me. I think that part was improved a lot over the last 5 years. Right now, vendors have mechanism to force push firmware updates. Furthermore, no body talking over plain text HTTP anymore because it's possible to read the traffic from the device or through the device with HTTP. Thus, force push firmware updates becoming an industry standards and HTTPS becomes secure default protocol.

4. **What developments do you foresee in the smart home security area in the next 5 years?**
    a. **Which of these developments would you consider most relevant to your own role, and why?**

I think, the Matter protocol will be the biggest thing that will improve the adoption of smart home devices in the next 5 years. If most manufacturers adopt this new Matter protocol, any smart devices will interchangeable. You will be able to switch your smart home providers easily and not tied to a particular ecosystem such as Apple, Google, or Amazon and people will have more choice. For example, I want to buy smart blinds and I think there are 2 manufacturers that support HomeKit that create smart blinds, it's Ikea and some other vendor. However, Alexa or Google, there are a lot of manufacturers that are creating smart blinds. So, I can move my ecosystem from HomeKit to something cheaper such as Alexa.

5. **What do you think is currently the most likely attack vector in a smart home?**

What I'm worried most is secure communication. All these vendors pay attention to secure communication between their devices and the costumer such as their phones. They also pay attention on how they communicate from their devices to their servers. There is an assumption that your device is running in safe environment because it runs in your local network and assume that it's isolated from the rest of the world. However, an attacker can find the weakest link for example, I have a printer that connected to the internet and attacker can hacked into the printer, then he's in my network and attack other devices in my local network. I don't think vendors pay much attention to that. Another example is that if it's a Bluetooth device, nobody pay much attention to Bluetooth security 2-3 years ago. After several major proof of concept on, for example August lock, they started improving that. So, basically, they don't pay much attention to close proximity attackers. For example, somebody walk close to my door but outside of my house, they can hack into my Wi-Fi network or they can hack into smart devices through Bluetooth if the device use Bluetooth. Another concern is hardcoded device. Many manufacturers have hardcoded some secrets in the firmware such as debugging keys that they hope nobody will find out but they can do diagnostic on my device. There's something like universal keys that can give access to any device in the world and compromised them. Furthermore, there's no way to updating the key remotely in a very short period of time by the vendor. Thus, causing a lot of customers under a threat of being hacked.

6. **Do you think some attacks reported by security researchers in the lab that you can think emerge in real development? Why or why not? For example, August smart lock, LIFX, and Foscam**

Well, Foscam attacks were real. That's an example where people use our or other researchers exploit to their advantage. Foscam couldn't fix all the cameras because they didn't have a mechanism to fix them. When I say fix, they released new firmware but they didn't have mechanism to push that firmware to the devices. Thus, a lot of Foscam cameras were with vulnerable firmware. Since we published our research already, people knew about the vulnerability and use the vulnerable cameras for their own interest. I would say most of the attacks reported by security researchers are going to be replicated in the real environment. Well, things improve over the years because now manufacturers have found a way to force push security fixes to the devices. So, there's less vulnerable devices in the wild, but on the other hand, there are still manufacturers that do not implement force push security fixes and those devices are completely open and vulnerable. Additionally, the vulnerability is a public knowledge so people that are bored, read the research about the vulnerability, try to exploit it. Since, there is no government regulation, people can sell anything. For example, manufacturers that want to sell a camera in the EU, they need to have a firmware push mechanism. If there's no regulations, those cameras will still be vulnerable. I honestly think it has to be government regulated. You cannot sell the camera unless it passes a certain security criteria

7. **What are the most frequently reported security incidents that you know of or you've experienced?**

I think it's hardcoded credentials or hardcoded username and password that comes from the factory. Usually, it's even printed on the label of the device itself. Most of the cases, the username is "admin admin" for any devices or randomize but predictable and attacker can predict it easily. I think, that's the easiest problem that still exist.

8. What vulnerability do you think is the most dangerous in a smart home systems?

I think, it's Remote Code Execution. If somebody can remotely execute something like arbitrary program on the smart device itself, that means they can achieve anything they want. So, yeah Remote Code Execution or RCE.

9. How do you think a third-party security company could help consumers improve security? For example, Norton core, Kaspersky smart home security, Bitdefender Box

There is a similar device from Apple, and it enhances security for HomeKit. If you have HomeKit devices plus a router from Apple, the router will try to block malicious connection. They basically protect users from malicious vendors. It's similar to the example that you gave me. I think it is useful because it protects users from malicious vendors or hacker. Vendor can be malicious because you can buy a camera from AliExpress for example and think that it's secure and only works when it's turned on, but it works 24/7 and send some data to China. You do not know anything about the camera traffic unless you have a device that monitors and check the traffic and letting you know if there is an unwanted traffic in your camera. Maybe the manufacturer is not malicious but the camera have some vulnerability that's exploited by an attacker and somehow the camera talk to a house in California for example. You as a consumer have no idea about it unless you have a device that monitors the traffic from the smart devices and notifies you about the unwanted traffic. This means that you need to completely trust the security device on your home network either from Bitdefender, Kaspersky, Apple, etc. which is another challenge. What if this security device is hacked? There is so many cases of Apple router is hacked but what about Bitdefender? Maybe with the same success, but who knows. It moves the trust from the smart home devices to the security device from security company but when it's hacked, it becomes the weakest link. There is a trade-off.

10. Who is more responsible for smart home security? Manufacturers, Consumers, Government, Security industry

I think manufacturers is the most responsible, then government because they need to regulate the manufacturers. The most important thing is manufacturers to have security in mind when they manufacture devices but the government has to be the second one to enforce the security in the devices. Then, security industry can probably influence government. Government probably can come up with stupid ideas and this stupid ideas can be steered to the proper direction by the security industry. Then, consumer is the last because you cannot expect the consumers to be knowledgeable about security. For example, you cannot expect a single mom to take care of the smart home devices and the security of the devices. So, you cannot blame consumers.

11. Would you like to add something?

No, I don't think so.