A

Project Report Entitled

(PENTESTING SMART HOUSE AND FINDING VULNERABILITY)

by

MR. ANJEESHNU BANERJEE

LIST OF CONTENTS

LIST OF FIGURE

ABSTRACT

A Smart Home (SH) essentially is a home with communication network that connects smart devices, sensors and actuators, enabling the owner to locally and remotely access, monitor and control them.The goal of smart homes is to have smart household devices delivering services needed for efficient home functioning with minimum human intervention. Based on the fact that many electronic devices are digitalized in our world in order to facilitate our lives, there is a large potential for development in the home. The objectives for this thesis is to bring up common communication technologies,hardware, security and vulnerabilities in the context of a Smart Home and what could be done to protect them in future. In order to investigate the objectives, an experiment has been conducted . The experiment exploits weakness in a common Smart Home technology used in the network enable devices in the form of threats and vulnerabilities in order to mitigate and minimize threats and vulnerabilities in smart homes . To conduct this experiment I will use GODSEYE .tool along with several pentesting tool to find bugs . GODSEYE is a wlan auditor developed by Anjeeshnu. Its basically modular, program written in python3 to simplify the process of performing manipulation on a wireless network. The goal of the tool is not to compete with existing tools or scripts, but to provide as much functionality and simplicity to the end user as possible.. this is all about finding bugs and vulnerability in smart homes with help of GODSEYE (used just as a tool along with several other tools) and exploiting the found bugs to gain access of the smart home and user data .

The contribution to forensic science is that the work is supposed to enlighten the cyber community regarding communication technologies and security used in smart homes . the bugs and vulnerability found during the experiment of this thesis can be used to build a secure smart homes as well as IOT devices used in smart home in future .

CHAPTER 1

INTRODUCTION

This chapter presents the theoretical knowledge that needs to be explained to understand the context of this work. In order to understand the security and vulnerabilities the definition of a Smart Home must be presented, followed by the security, threats and vulnerabilities in the context of a Smart Home.

DEFINITION OF SMART HOME

The definition of what classifies as a Smart Home is a home or household that is built up with automated systems where the devices constantly communicate with one and another. These automated systems provide the resident with monitoring and control of all the units in the household . Further the general Smart Home is divided into three subcategories: Smart Home, Connected Home and The Smart Connected Home.

A Smart Home

A Smart Home is based on a system that allows a resident to use the home appliance local within the residence. This system relies on a wired-based standard which is not connected to the internet and it focuses on automation for example lights and windows.

A Connected Home

A Connected Home is different and allows remote control and this typical over internet. This type of home usually provides services as security or health management. The system for this is usually controlled from a gateway that can be operated from a smartphone.

A Smart Connected Home

A Smart Connected Home is based on a system that is combined from the two types of smart home mentioned above and further it has the capability to learn. The system for this type of house can learn different things e.g. forecast and lifestyle of a resident within a home environment. When implementing this type of Smart Home cloud services are often used and the programs that are used for analyzing collected data is cloud-based. These services can take actions if needed for the system and that can happen autonomously. One example is that if there is a water leak, and a smart leak detection system is implemented, the system will notify the resident that there is a leak somewhere and probably where the leak has occurred. Today a Smart Home is considered the same though it is more developed but is still used for many different purposes. the Smart Home is used for comfort,

safety and security but also to be more cost efficient and make it possible for the resident to manage the energy consumption, which is from both economic and comfort perspective.

Figure 1 showing a smart house

4.2 SECURITY OF A SMART HOME

Cybersecurity or information technology security can be defined as how a computer system can be protected from theft or damage. The importance and awareness of security are increasing with the development of devices and requests. Network enable devices in the context of a smart home require reliability, stability and resilience . The most security systems provide features as monitoring, detecting and the ability in order to control security threats. Motives to implement security in the systems are to prevent data loss and therefore ensure privacy and integrity, protect equipment and have a system running that is reliable and constantly available. Security for Smart Homes and safety systems normally involves remote control system that can recognize physical threats such as fire or someone breaking in and entering the house. When a threat occurs, the system must be able to automatically make decisions. An example of decisions might be when a fire breaks out and the water sprinkler system is automatically turned on due to the level of smoke sensed by a smoke detection. Another example is when Smart Home are installed with an alarm and a breaking in occurs, the movement or the impact triggers the device to automatically turn on the alarm . Security are the main reason that consumers are buying Smart Home systems and the main part of all those consumers live in cities where crime rate is higher. ENISA (European Union Agency for Network and Information Security) specifies that the

need for security in a smart home area is increasing and has been for past years, but there is still a difference between the security regarding the Smart Home and the traditional security. The downside of the increasing need of security is, as mentioned by ENISA the devices used in a Smart Home are not designed or built to handle strong protection, most devices and sensors for smart home systems are too weak to handle heavy implemented protection. Regarding the hardware and connectivity, the security standards are not identified for the equipment or hardware that are used in the implementation of the Smart Home, i.e. the devices have weak CPUs, limited memory, bandwidth and small or weak batteries. ENISA offer "good practice" to improve the security in the context of Smart Home Security and Resilience for Smart home environments.

4.3.4 Intentional Threats or Abuse

Intentional threats or abuse such as Eavesdropping, Interception or Hijacking, might be performed by an attacker. The purpose of this type of threats might be to gain access or find or implement weaknesses. After a performed attack the user or resident might have lost control over the network enabled device or privacy data and therefore the confidentiality and integrity are tampered with. Identity fraud could be an issue since Smart Home stores and processes user information for different types of services. An attacker can forge this information and appear being a legitimate user. An attacker with this type of forged identity might get unauthorized access to administrator privileges and tamper with the Smart Home set up. (Distributed)Denial of Service, DDoS or DoS, can easy compromise the communication and traffic between connected devices. The DoS attack can be data specific, like spoofing or flooding, where the attacker specifies what data should be sent from one host. If the attack is distributed the data will be sent from several hosts. The result of this type of threat or attack is to prevent the use and service of the device. Manipulation of information found in sensors and network enabled devices can result in consequences. The sensors or the device can be fed false and inaccurate information. This might result in bypassing of security features and disclosure of credentials. It can also result in blackmail, fraud and rising of privilege. Hijacking/traffic interception might be the cause of action to gain unauthorized information. Many of the sensors and devices produce large amount of data which are related to the users of the Smart Home, such as absence, presence and activities.

4.4 COMMUNICATION TECHNOLOGIES

This section presents the communication technologies used in the context of a Smart Home. Each communication technology is presented with characteristics, security and

vulnerabilities. At the end of this section a summary of all the communication technologies and their characteristics are presented in a table (Table 3). OSI model have an important role in the network enabled devices. The OSI-model is presented for each communication technology and is further explained in a table (Table 2). The table presents different type of attacks . Table 2. This table show the OSI-model layer by layer with examples of what attacks might occur towards each layer of the OSI-model.

OSI-model	Attacks
Layer 7. Application	SQL-injections, Malware, Virus
Layer 6. Presentation	SSL- & HTTP attacks
Layer 5. Session	Session Hijacking, Telnet DDoS
Layer 4. Transport	Denial of Serice (SYN Flood)
Layer 3. Network	Man In The Middle
Layer 2. Data Link	MAC- filtering/spoofing
Layer 1. Physical	Jamming, physical damage

Table 2. This table show the OSI-model layer by layer with examples of what attacks might occur towards each layer of the OSI-model.

4.1.1 ZigBee

ZigBee is a low power wireless technology, built as mesh topology based on IEEE 802.15.4 standard for Personal Area Network (PAN) with a focus on applications for monitoring, controlling and sensing. It mainly operates in 2.4 GHz ISM band and has a nominal range of 100m. The ZigBee Alliance is working to be the standard for Smart Home devices, from temperature and lighting systems to security monitors and smoke detectors the highest data range is up to 20kbps on 913 MHz and 868 MHz bands and 250 kbps for the 2.4 GHz band. ZigBee uses the IEEE 802.15.4 standard as a physical and data link layer while the protocol is based on the OSI-model (Table 2.) and working on the upper layers, from network to application layer The ZigBee technology was released in year 2001 and updated to ZigBee Pro Specification in 2007, the last one is fully backward compatible and the main difference that the feature provides better security . The pro version is often used when the ZigBee network is very large and better security features are important for the network . ZigBee have established itself as one of the leading communication protocols for wireless sensor networks (WSN: s) and the technology advantages are low-cost and low complexity. Known limitations are restrictions of nodes, limited amount of memory, constrained energy consumption and communication capabilities as the data-rate .

Security and vulnerabilities

In the ZigBee technology there are four concepts that are considered important for the security. Following bullets explain each one of them.

• ZigBee is supporting two different security levels, one called “Commercial Security” which has high security and on with standard security called Residential Security. The differences between those are mainly distribution and management of keys.

• In a ZigBee- enabled network one of the units the “TC” is responsible for the security. TC or the Trust Center provides a security mechanism with three different types of security keys, the network key, the master key and the link key. The Trust Center is also responsible for selection of the security level and key management. The ZigBee unit then share corporate network key and the link key can be divided between two ZigBee devices the link key is from the master key and is important for long-term security between two ZigBee-units.

• Authentication and Data Encryption Data is encrypted with 128-bit Advanced Encryption Standard (AES) with CCM mode which is allowing authentication and data encryption called AES-CCM . CCM only useful for 128-bit cryptographic block ciphers. ZigBee uses a modified version of CCM called CCM*, CCM* enables the use either authentication or encryption. In the regular version of CCM the both are required.

• To make sure that integrity and freshness of data is properly a Message Integrity Code (MIC) can be used. MIC verify that data not has been changed during the transporting and generated through the CCM* protocol. In order to enhance security within the ZigBee technology some counter measurements are highlighted. One enhancement is named “WZ-lcp”, which is a protocol/scheme to enhance the security and protect against both active and passive attacks in smart home environment. “WZ-lcp” uses a new method of authentication, the encryption used are the XOR and the calculation is performed twice. The limitations within the technology mentioned earlier, restrictions of nodes, limited amount of memory, constrained energy consumption and communication capabilities, makes it harder to implement a security mechanism as public key cryptography to improve the security. Later versions of ZigBee offer improvement of for example power consumption, still the technology have many weaknesses which can lead to security failures . Highlighted attacks could be physical attacks (e.g. vandalism and sabotage), key attacks (i.e. an attempt to recover the cryptographic key of an encryption scheme) and replay and injection attacks (i.e. a network attack in which a data is fraudulently repeated or delayed) as possible threats and vulnerabilities to the security in the ZigBee technology Another study on

ZigBee mentions that sensors and actuators often run on batteries and has a very low duty cycle. Low duty cycle means the relationship between an active radio time and the silent period, which the network has predefined to wake-up intervals for saving battery. However, this can open doors to a Denial of Service attack, where an attacker can repeatedly attack the media. In this way, an infinite loop of the DoS-attack can cause the battery to run out or greatly reduced. ZigBee security is focus on interfering, sabotaging or manipulating the data . A physical attack can also be done against the ZigBee technology and this must be included when forming the network. Since ZigBee is often used to controlling monitoring and sensing, which can contain of control critical systems for example an industrial plant or a home security system, it is very important to have in mind that the design of the ZigBee network is done in such way that the devices are protected from a physical attack. This can be done by placing the units in places that they are hard to reach but also protect with surveillance. If an attacker is stealing a ZigBee unit it is possible to extract the data from it, also the stored security keys. However, this attack is only working on ZigBee chips from some vendors, for this reason automatic system is important to detect and report missing units. If a unit is missing the security keys must be update directly to stop a possible unauthorized use of the whole ZigBee network.

Example of devices which uses ZigBee are - Philips hue to connect bulb ,Honeywell thermostats , Bosch security systems etc .

Wi-Fi

According to the Wi-Fi Alliance the worldwide network of company, Wi-Fi is the most common wireless communication technology. It is the primary technology for internet traffic and with 13 billion devices in use. This makes it also one of the most popular technologies for smart homes . The Wi-Fi signal can be used for various things in a Smart Home, but sensing operations, i.e. motion recognition and fall detection due to its sensitivity to environmental dynamics are preferred. A Smart Home that is based on Wi-Fi is considered cost-effective and offers comfortable deployment . The Wi-Fi standard IEEE 802.11ah is the most relevant developed standard according to this study. IEEE 802.11ah provides an improvement of the limited range and can with the latest development provide larger range and therefore make it easier to connect with applications and devices . The Wi-Fi standard IEEE 802.11ah operates on frequency 2.4GHz and 5GHz and is reducing the complexity of implementation. The earlier established Wi-Fi standards in the 802.11 family are more effective at the nearest access point and couldn’t provide service to the users with large homes. 802.11ah standard is operating on Layer 1 and Layer 2 according to the OSI model (Table .2) IEEE 802.11ax is an upcoming standard , which is marketed as

Wi-Fi 6 is likely to be the one that is prominent in the market. The standard is adding for instance efficiency, flexibility, and scalability this means that new and existing networks can increase both in speed and capacity. The expansion of systems within Smart Home and IoT has forced the development to improve and the new standard is a result of that. The IEEE 802.11ax is expected to be in full distribution later in 2021.

Security and vulnerabilities

The known issues with the Wi-Fi technology are WEP (Wireless Equivalent Privacy) and WPA (Wi-Fi Protected Area), since both can the cracked. The Wi-Fi Protected Access 2 (WPA2) is an enhancement and if it is properly configured it takes longer for an attacker to crack . In January 2018 the Wi-Fi-alliance announced that it should be new improvements to the WPA2 specification. The improvement called WPA3 has authentication, encryption and configuration requirements included. In fact, an enhanced protection for the networks that use password-based authentication, with improved privacy in open networks, palliative against Denial of Service and stronger cryptographic algorithm. WPA3 will establish a mechanism for Internet of Things (IoT) devices without or a with a limited user interface for trusted networks. Known vulnerabilities regarding Wi-Fi can be that an attacker duplicates an access point and get unauthorized access to the system of the Smart Home. When an attacker proceeds with the access point-duplication it is possible to implement the system with malware. Furthermore, there are reports that the WPA2 has been trespassed, where an attacker has been using wireless networking tools to detect networks and information about networks, with the intention to get unauthorized access or to exploit the system . Another threat which Wi-Fi is vulnerable to is a Denial of Service attack (DoS), a DoS attack is meant to shut down or compromise the availability of a network. This can be done through consume resources with a Flooding DoS-attack or protocol abuse attack called “DeAuthentication DoS” which targets communication between a user and a Wi-Fi wireless access point. In Layer 2 of the OSI model, the management frames of 802.11 are sent in plain text and broadcast, this makes it possible for units within reach to discover networks and demand connection. This is the reason many security issues emerges if an attacker catches a plaintext management frame, they can fake the packets. The two potential frame types that can be used for a DoS state in the 802.11 protocol are DeAuth (DeAuthentication) and DisAssoc (DisAssociation) frames. Reception of either the DeAuth or DisAssoc frames will move the victim off authenticated state in the Access Point and into not allow for exchange of data Packets [29]. With the information above it is easy for an insider or an attacker from the outside to use a tool like Wireshark in order to

perform eavesdropping of the network traffic and get valuable information about the network which in the later stage can be used for an attack

Z-wave

Z-wave was developed in 2001. The newest update of the communication technology is ZWave Plus and was released in 2013 with improvements as better battery lifetime and larger wireless range . Z-Wave is a low-power wireless communication protocol for home automation specifically for remote control application in residential and light commercial environments. Z-Wave is implemented in a huge number of products all over the world e.g. home theater, automate window treatments, pool and spa control and automated meter readings . Z-Wave is implemented on the four lower layers of the OSI model (Table 2.), the physical, data link, network and transport layer . ZigBee is also built on a mesh network topology, which means that the devices works as signal repeaters and the network will be stronger when you install more devices. The signal easily travels through most walls, floors and ceilings which result in a large range of 100 meters or 328 feet in open air due to building materials reducing the range indoors even though it travels well. The recommendation is to implement one Z-Wave device roughly every 30 feet or closer for best effect . Z-wave is not compatible with IP and cannot connect directly to internet or to a user device without a controller to manage the devices. The controller acts like a gateway which manages the interaction between Z-wave devices and a smartphone through internet or from a local network. Good knowledge is that Z-Wave is a proprietary protocol which is owned by Sigma Designs and promoted by Z-wave Alliance which has sold nearly 100 million devices

Security and vulnerabilities

Sigma Design tried to improve the security on Z-wave and they have recently announced a new security framework for the technology. The new firmware implementation within the latest framework will affect the gateways and the devices that have received the firmware update, the devices that doesn't have the update may have potential security issues . Known vulnerabilities and threats to Z-Wave is e.g. "Impersonation attack", which is an attack when an opponent assumes the identity of one of the legitimate parties or communication technologies. Normally this type of attack is made by sending an email to the target where the sender masks itself as a trusted source, to gain access to sensitive information. Another attack is e.g. "A black hole attack" which is an attack similar to "Denial of Service attacks." The router is supposed to relay packets, but instead discard them when this attack occurs .

KNX RF

KNX is a both wired and wireless communication technology, KNX and KNX RF (Radio Frequency). KNX is a short for “connexio”, which is Latin for connection. KNX was developed in 1991 and were back then the most common used technology within the area of Ventilation, Heating and Air-Condition, summoned as HVAC. Many devices were KNX compatible and in 2006 KNX became a standard by the ISO/IEC. KNX RF is based on the OSI-model (Table 2.) and is working on the data link, transport and network layer. Other mediums used in the discipline of KNX are twisted pair, powerline and Ethernet. The KNX RF is used with same bands as industrial, scientific and medical. The frequency is between 868 MHz and 2.4GHz

Security and vulnerabilities

KNX defines no security measurements within the technology apart from plain text transmitted passwords. This is a considered vulnerability, because if an attacker is eavesdropping on the transmission of the messages, the attacker could retrieve the passwords and therefore get unauthorized access to a system. The KNX has been developed further with KNX Data Security which provide the technology with encryption, integrity check and authentication using AES 128-bit .

4.1.5 Bluetooth

Low Energy (LE) Bluetooth LE is a wireless communication technology. The communication technology is a widely used communication technology and almost everyone has experience from Bluetooth. This method is a cheap way to transfer data and requires that the devices used are supported by the communication technology Bluetooth LE. Bluetooth LE is working on the IEEE standard 802.15.1 and the frequency between 2.4GHz and 2.485GHz, and the nominal range is 10 m, which is considered small range . The power consumption of the devices used in this technology is reduced and the lifetime is long due to the use of cell batteries. The use of Bluetooth LE offers a direct connection between the devices used, and there is no different between using a mobile phone, tablet or smart home devices. The network topology is built as a Star-Bus topology and works as one-to-many nodes .

Security and vulnerabilities

Bluetooth LE offers security features to protect information when it is exchanged between devices that are connected . The security features are divided into two modes, mode 1 and mode 2. Each mode has different levels. Mode 1 has multiple levels that provide encryption. Level 1 provides no security features, which means there is no encryption or authentication. Level 2 provide no authentication but pairing with encryption. Level 3 provide the full security with both authentication and encryption for pairing. The encryption is not as strong as desired. Level 4 provides stronger encryption and authentication. The encryption is using the AES-CCM (Advanced Encryption Standard - Chiper-based Message Authentication Code) algorithm in addition with P-256 elliptic curve . AES-CCM is a keyed hash function that is based on the symmetric cipher as AES. The encryption takes the encryption key, the encryption nonce and the payload as input . Mode 2 has multiple levels that provide data signing. Data signing provides integrity but not confidentiality for the data. Level 1 requires no authentication with data signing when pairing devices. Level 2 requires authentication with data signing when pairing devices . 28 There is no protection against passive eavesdropping even though the encryption and authentication are implemented in the technology.

This makes it possible for an attacker or the passive eavesdropper to determine either of LTK (Long-Term Key), CSRK (Connection Signature Resolving Key) or IRK (Identify Resolving Key) . The feature “Just works”, which is a pairing method, do not provide MITM protection when devices are paired, which means when Just Works-feature are used the technology is weak for MITM-attacks (Man-In-The-Middle-attacks). If this occurs the attacker can manipulate the data that are transmitted between devices. Bluetooth LE devices should never be implemented with the feature “Just works”, to mitigate MITM and eavesdropping attacks. ECDH pair of keys, if weak, they might minimize eavesdropping protection for SSP. This weakness might make it possible for an attacker to determine the secret link keys. All devices should therefore have strong key pairs. When pairing devices, the passkey provides the device with protection when using SSP. Weakness is found when these passkeys are static, and that might make a MITM-attack happen. Therefore, the passkeys should be unique, and unique for each pairing. If a device are set to a specific security mode and that the device can fall back to a another security mode when connecting with a device that do not support the same mode or level, it could happen that the device falls back to security mode 1, which do not provide any security at all. When attempts for authentication are repeated, there must be an implementation in the device with the Bluetooth LE technology, for the device to be able to handle the threat without faults. This implementation should be that there are unlimited authentication requests, but if the requests are set to a waiting response an attacker could sneak in between the attempts and

retrieve information about the secret link key via the response challenges. A considered vulnerability within Bluetooth LE could be that if the keys that are used to manage and maintain connectivity are stored improperly, they could be retrieved by an attacker. The data between end-to-end devices are only encrypted and authenticated on specific points. At the intermediate point the data is decrypted, which makes it important to have additional security to mitigate this issue. The security features overall are not a part of the standard. I corporation with the developer the security can be improved .

The Bluetooth LE technology is in risk-zone for planned attacks and threats such as following. Bluesnarfing - which goal is to gain access to a Bluetooth enabled device via exploitation of the firmware. Bluejacking - this attack can be conducted on any mobile device with Bluetooth enabled. The attacker sends messages to the user of the device, and changes can be made on the device. There can come to harm for the user or the device if that's intended. Bluebugging - this attack exploits the security flaws in the firmware to gain access to the device. The attack performs actions without informing the user and the purpose of the attack except from gain access can be to place or eavesdrop on phone calls, send messages or exploit other services. Car Whisperer - exploit the standard passkey (if the users have not chosen a random passkey) and aims for Bluetooth devices installed in cars. Denial of Service - like most wireless technologies, Bluetooth LE are sensitive for this kind of attack. The goal with this attack can vary but the main goal is to disturb the traffic. Fuzzing attacks - This attack sends malicious data to a device and wait for the reaction. If there is a reaction the attacker can assume that there is a weakness in the protocol stack that the he or she can take advantage off. Pairing eavesdropping - the attacker collects the frames that are sent when a paring between devices occur and further determine the secret keys and from that retrieve decrypted data. Secure Simple Pairing Attacks - there is many tools to force a device use a feature like "Just Works", and after that exploit the device with a MITM-attack due to the lack of protection .

4.1.6 Thread

Thread came into the market 2016 by Tread Group and is at the moment of writing growing as a communication technology and is backed by few of the biggest companies in the field; Apple, Siemens and Samsung. Thread is developed and categorized for home automation. This communication technology is addressed to be unique in terms of interoperability, security, power and architecture of smart home devices. Thread address to be a low-power mesh networking protocol, able to connect both device-to-device and device-tocloud, have zero point of failure and is based on the IEEE standard 802.15 . Thread is designed to be used in both small and big networks with low-power devices and

the nominal range is 30 m, which is considered medium range . Thread is working on the radio standard IEEE 802.15.4. The IEEE 802.15.4 standard is designed to run on low-power consumption and low latency. Further Thread is using the protocol IPv6 for communication, which is a wireless mesh networking protocol, where 6LoWPAN is the foundation , which is an acronym for “IPv6 over Low-Power Wireless Personal Area Networks” . The OSI-model is a central part in how the communication works within the technology. Thread protocol implementation takes part in layer 3 and 4, while the IEEE 802.15.4 standard takes part in layer 1 and 2 (Table 2) The Internet Protocol is the key to reach the Internet and since Thread is based on IPv6, the technology is provided with the possibility for devices to talk in a seamless way with home devices, cloud and mobiles. IPv6 make it possible for Thread technology to be connected with both users and devices .

Security and vulnerabilities

Thread has zero point of failure because it, as a technology, can heal itself. The network with Thread implemented is therefore resilient and can reconfigure itself when a new device is added or removed from the network. The resilience is important from a security perspective, but further there is security added to the self-reconfigure feature e.g. only authenticated devices can join a network . The communication is secured with encryption . The encryption is the fundamental security of the Thread communication technology. The encryption method is an AES-CCM (Advanced Encryption Standard-CCM) encryption and the key-exchange takes place via a method based on P-256 elliptic curve Diffie-Hellman, which is a NIST-standardized elliptic curve . The key exchange-method via elliptic curves is named “Juggling Password-Authenticated Key Exchange, J-PAKE” and operates as a key agreement and further the Schnorr NIZK (Non-Interactive Zero-Knowledge) signature operates with the authentication between peers. Here a shared secret established based on the passphrase . A network-wide key is used as network protection for the Thread communication technology. The network-wide key purpose is to prevent eavesdropping and disruption towards the communication technology. The key operates on the MAC-layer (Media Access Control) to protect the data frames of 802.15.4. Since the key is a network-wide key it is not optimal to use only this key-exchange as the only security in the communication technology, due to the risk of becoming compromised or revealed . Further this network-wide key is known by all devices in the network and the Thread technology requires additional protection e.g. Transport Layer Security (TLS) and Datagram Transport Layer SecurityRFC6347. These combinations provide extended security service. The counter measurement with the full security combination is that it might have an impact on performance and the use of small embedded devices might not have the capacity to handle

the combination. Therefore, if the TLS or DTLS are not used consequently, might result in a severe security issue for the communication technology . At the moment of writing the author is not able to find any vulnerability for this communication technology. The Thread technology is according to Thread Groups white papers secure and there is to the writers any known vulnerabilities that can be exploited.

Technology/Characteristics	ZigBee	WiFi	Z-Wave	Thread	Bluetooth LE	KNX RF
IEEE standard	802.15.4	802.11	N/A	802.15.4	802.15.1	N/A
Frequency band	2.4GHz	2.4GHz, 5GHz	900MHz	2.4GHz	2.4GHz	868MHz
Nominal range	100m	150m	30m	30m	10m	150m
Data rate	250 Kbps	1Gbps	100Kbps	250Kbps	1Mbps	16.385Kbps
Network Topology	Star, Cluster, Mesh	Star, Mesh	Mesh	Mesh	Star-Bus	Line, Tree, Star
Number of nodes per network	65000	250 per Access Point	232	300	One-to-many	65000

Table 3. This table includes information and characteristics of Smart Home Communication Technologies. Each technology is presented with same categories with data.

CHAPTER II

LITERATURE REVIEW

A literature study review was the main method for this work. The literature study was performed as a review of previous published journals and scientific articles. This method was used to address the objectives; What are the common used communication technologies in the context of a Smart Home? What are the security threats found in the communication technologies in the context of smart homes and what are their consequences? How can the security be improved in the future regarding communication technologies for the smart home device? The literature study was performed by searching for published articles and scientific articles in well-known databases; IEEE Explore and Google Scholar. Keyword used when searching for relevant journals and articles for this work was; Smart Home, Security, Vulnerability, Threats, ZigBee, Z-Wave, Wi-Fi, KNX RF, Bluetooth Low Energy, Thread.

Jose and Malekian explain the different SH structures from a security viewpoint. They examine the current security flaws and challenges in home automation systems from the standpoint of both the homeowner and the security engineer. They have carried out a literature review about the challenges faced by home automation, but have not set up an smart home testbed to carry out experiments to find vulnerabilities and apply suggested security measures .

According to me smart homes should be build considering the security point of view such as the main network should be hosted on thread instead of wifi , a proper security policy should be developed in context with smart homes.

CHAPTER III

AIM AND OBJECTIVE

AIM

The aim of the research is to find bugs and vulnerability in smart homes and IOT devices used in smart homes to minimize and mitigate the vulnerability for future .

OBJECTIVE:

A gap was found during the literature study where others work missed out on the security and the vulnerabilities presented together with the communication technologies. Knowledge regarding the Smart Home from a security perspective must increase. To fill the gap that was thought was missing during the study for this work I proposed following objectives .

1. What are the common used communication technologies in the context of a Smart Home?
2. What are the security threats found in the communication technologies in the context of Smart Homes and what are their consequences?
3. What bugs are present in most used IOT devices ?
4. How can the security be improved in the future regarding communication technologies for the Smart Home device?

CHAPTER IV

EXPERIMENT

PURPOSE

The purpose of this work was to identify common communication technologies used in the context of a Smart Home. The focus was on security and vulnerabilities found in the communication technology used for connecting the smart home as well as on connected IOT devices. The work is supposed to inspire and enlighten the reader about the security and vulnerabilities in the context of a Smart Home and the common communication technologies used for the purpose.

Ethical aspects

Ethical aspects are always important to keep in mind when working within the field of IT and security, the field is broad and there are many options to gain information and access. Further 13 there is a lot of information that must be protected, and ethical aspects must always be mentioned and brought up. In addition to the literature, ethical and moral has been studied, to reflect the work our work to the related literature. Regarding the experiment there has been ethical aspects that are mentioned in this section.

- The experiment has been done on a controlled and stimulated virtual environment .
- The proper permission is taken from the owner of the home before pentesting.
- The experiment is done for educational purpose ,the project does not support any illegal activity such as hacking .
- Everything done in the project is completely ethical.

To perform the experiment the following guide was used:

• Gather information about the unit. as much information as possible will be collected about the technology and the smart home device that it is implemented on.

• Modeling threats. Here the method or threat for the technology and the smart home device must be shaped. Decisions about what attack that will be made to the technology and the smart home device.

• Identify known vulnerabilities, e.g. the result from the literature study.

• Immerse ourselves in the vulnerability - how much can the vulnerability damage the Smart Home System?

• Report findings from the experiment and present in the result.

PREREQUISITES OF THE EXPERIMENT

- **OPERATING SYSTEM** kali linux in our case
- **FEW PENTESTING TOOLS** such as godseye , routersploit , nmap ,metasploit
- **A TARGET** A smart home
- **WIFI ADAPTERS** which support monitor mode and packet injection
- **AN ATTACKING MACHINE** capable of running kali linux

KNOWN VARIABLE

In our case known variable is the target is a smart home network

And using wifi communication technology to create a network to connect all smart IOT devices and communicate between them and ultimately to the internet .

METHODS USED TO PENETRATE THE MAIN NETWORK

The device was running on the Wi-Fi technology and this is what is going to be exploited in this experiment. The choice of experimental attack is Denial of Service-attack & Man In The Middle Attack (MITM) The expectations from the attack were to see if it was possible to tamper with the connection and the data transmission. Further the expectations were to see if the network is vulnerable and to gain access into the network .

METHODS USED TO PENETRATE THE CONNECTED DEVICES IN THE NETWORK.

There are several devices connected to the network which is using wifi communication technology which we are going to exploit and try to gain access and once we gain access we will try to attack the devices . The choice of experimental attack will be Blind Injection , post exploitation , backdoor trojan attack , Denial of service attack .The expectations from the attack were to see if it was possible to tamper with the connection and the data transmission and to gain a reverse tcp connection via backdoor installation . Further the expectations were to see if the device shut down or not, or how it behaved when stressed.

EXPERIMENTAL ATTACK

Attacking the main network ;

Step-1 First we will check our network card in which mode it is currently working weather its in managed mode or monitor mode or any other mode and to do so we will open the root terminal in kali linux and use the command (iwconfig) this will show information regarding our network card / wifi adapter .

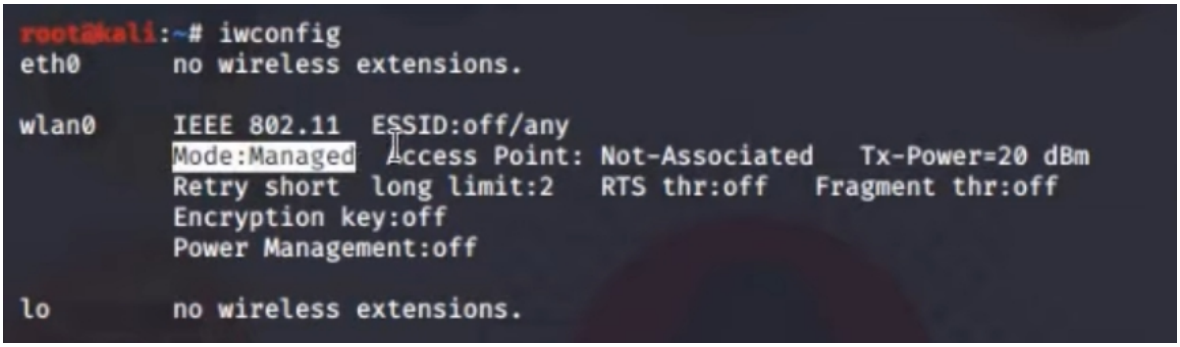

Figure 4 showing wifi adapter mode

Step-2 Our card is in managed mode in this mode it can not capture data or sniff data so we need to change it to monitor mode so that it can sniff packets from air and to do so we will use godseye tool.(I like to use this tool . you can use any other similar tool to do so)

Figure 5 showing menu of godseye tool

Step-3 From the menu / attacks we will select option 6 which is to manipulate the systems wifi card with manual control .

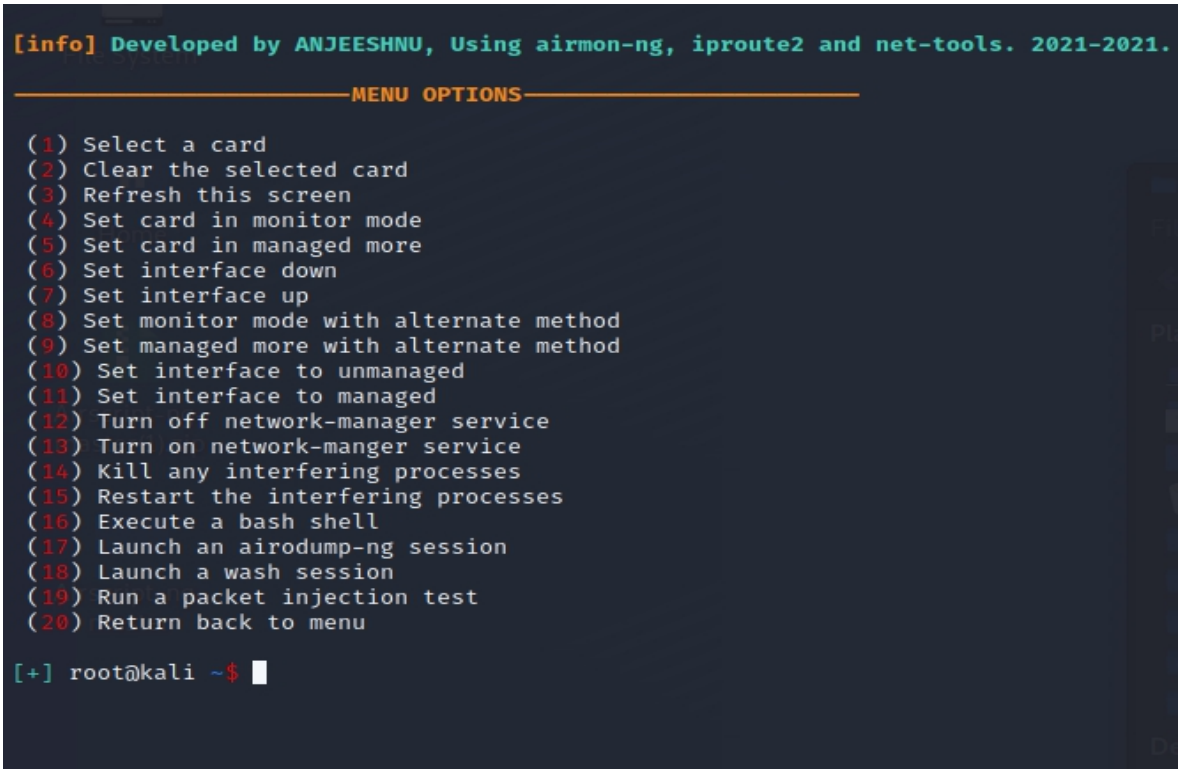

Figure 6 showing options to manipulate wifi card

After this we will select the desired wifi card and and set it to monitor mode so that now we can sniff packets from the air .

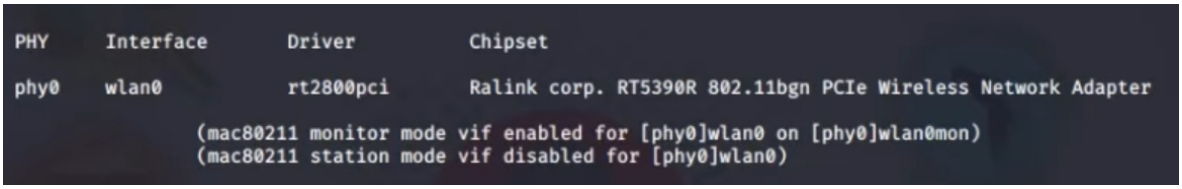

Figure 7 showing conversion of wifi card to monitor mode.

Step 4 After this we will again run the command (iwconfig) to ensure that our desired card is set to monitor mode .

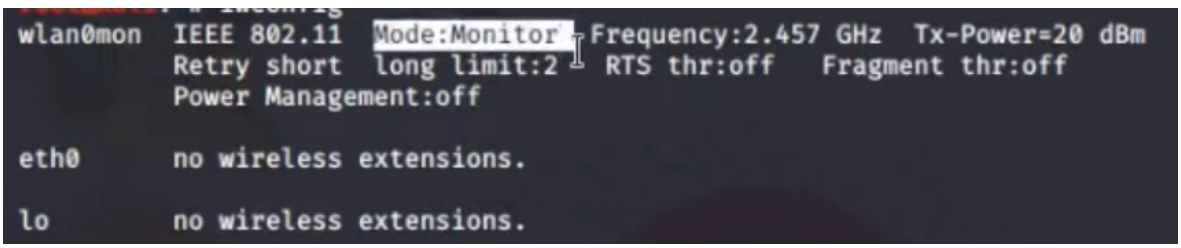

Figure 8 showing card in monitor mode .

Step 5 - Once the card is set to monitor mode we will scan for the available access points around the air .

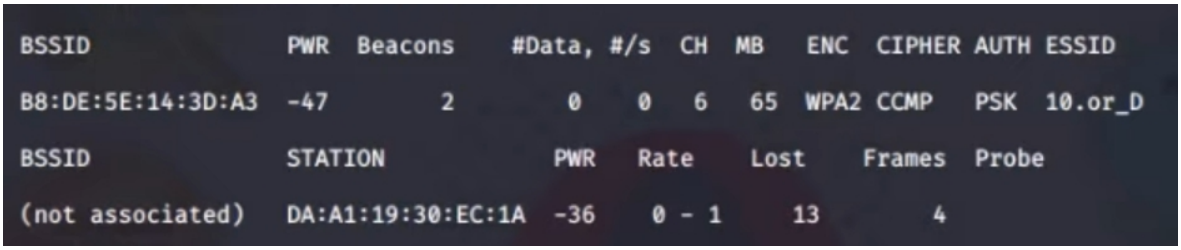

Figure 9-showing available access point for different networks

Step 6 From the available list we will filter the target access point (target accesspoint is the access point to targeted network) . in our case (smart home network) it is the one with ESSID (10.or_D) so we will select that to launch the further attacks

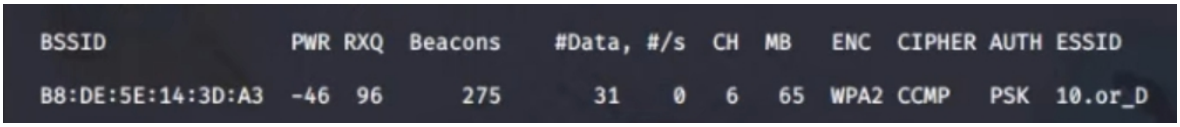

Figure 10 showing filtered access point

the first attack we are going to do on the network is Denial of service attack by sending too many authentication request on the access point which will eventually lead to disconnection of connected devices in the network . as soon as access point will be bombarded with too many request it will make the service too slow and eventually leading to resetting/ restarting of the network which will then automatically disconnect all connected devices .

Step 7 we will specify the BSSID of the the access point in order to launch a dos attack

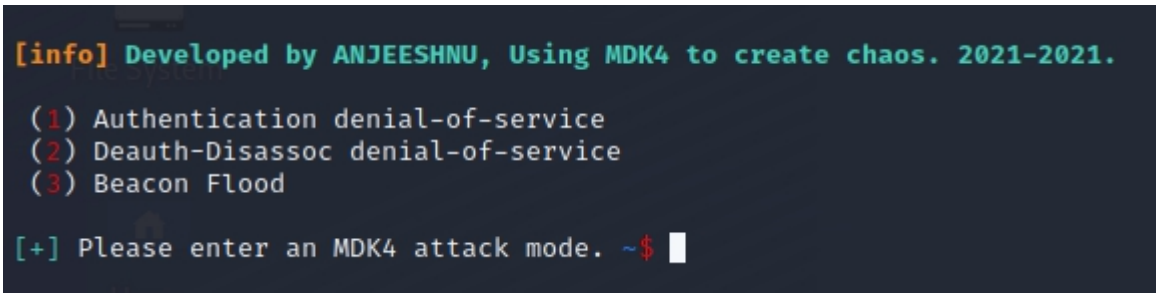

Figure 11 showing dos attack option

Once the BSSID of the taget is set and locked we will perform a Deauth-disassoc denial of service attack by flooding the access point with unlimited deauth packets .

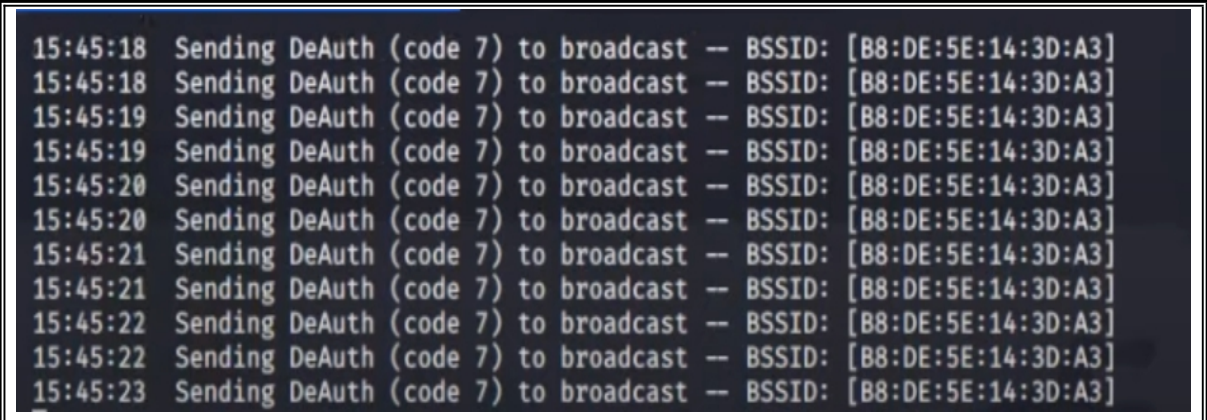

Figure 12 showing dos attack

as soon as access point will be bombarded with too many request it will make the service too slow and eventually leading to resetting/ restarting of the network which will then automatically disconnect all connected devices . once the devices are disconnected from the network devices will try to connect back and in order to connect back itwill have to make a 3 way handshake (A three-way handshake is a method used in a TCP/IP network to create a connection between a local host/client and server) and this 3way handshake contains password in encrypted form . so at this point we will do man in the middle attack and capture the handshake .

Step 8 once dos attack is launched successfully we will launch a man in the middle attack to capture the handshake .

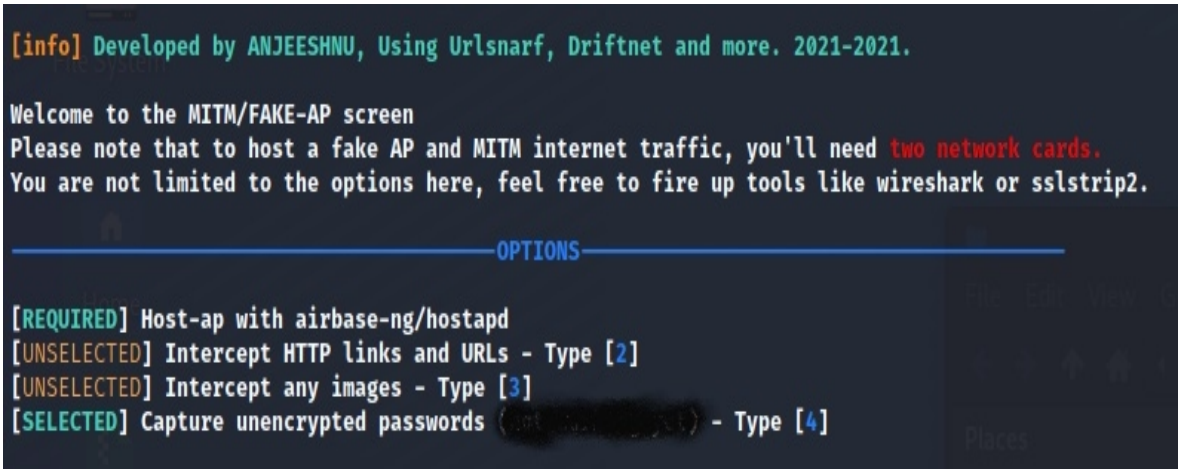

Figure 13 showing options for man in the middle attack

Step 9 after lunching man in the middle attack we will wait for the devices to connect to the network and when it tries to connect to the network we will stop the dos attack and capture the handshake file .

Note - repeat step 9 several times till handshake file is captured .

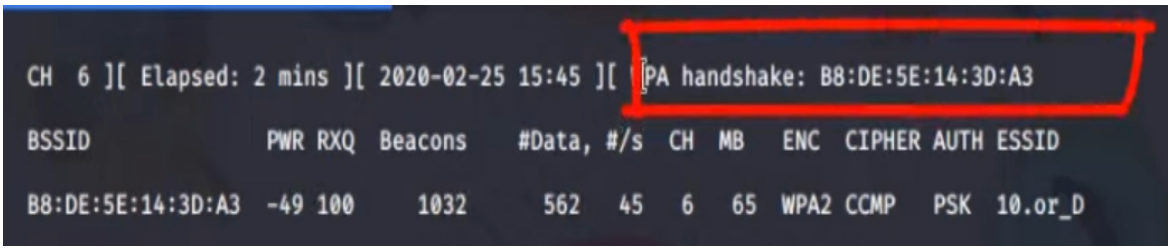

Figure 14 showing captured handshake file

Step 10 step 10 or the final step is to crack the encrypted captured file

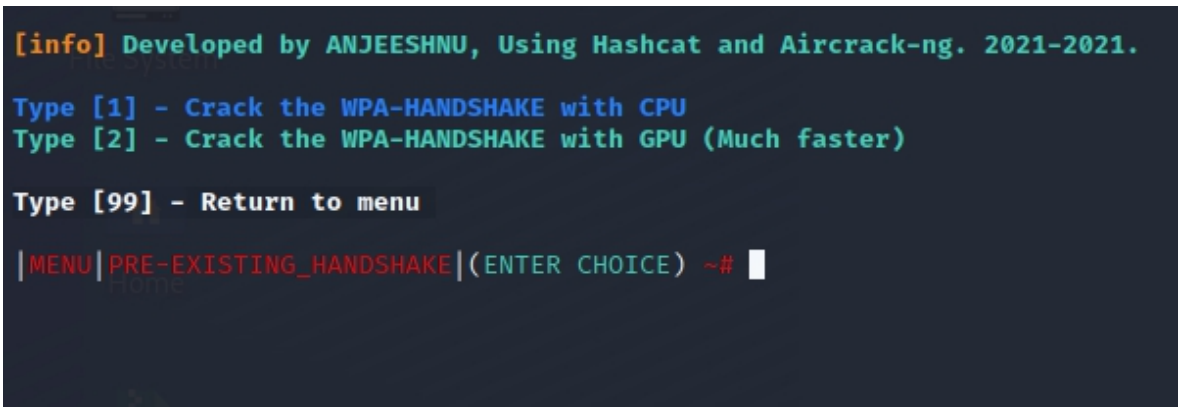

Figure 15 showing option to crack the encrypted handshake

Here we will specify the path were we have stored the handshake along with the path of word list in my case I always save it to desktop . after cracking is done we will get our password in plain text .

Figure 16 showing password

Now when I got password of the network we can connect to the network anytime we want using the password of the network which is(breezeless) .

Result of this experiment

After doing DOS(denial of service attack)& MITM (man in the middle attack) we were able to successfully obtain password of the smart home network , which is eventually used to gain access to the network .

Vulnerability founds

{The network is vulnerable to DOS(denial of service attack)& MITM (man in the middle attack)}.

Now when I'm inside inside the network we will try to attack the devices (IOT devices) to find vulnerability in them .

PRINCIPLE USED TO PENETRATE THE ROUTER

As I'm already inside the network I will first try to find out the router inside the network and after finding the router I'm going to check the router against the known IOT devices vulnerability database to find exploits if any . further this exploits can be used to gain shell access of the router by creating backdoor using the found exploits . TO successfully do this attack I will use routersploit tool (it's my personal choice to use this tool . one can use any tool they like to perform the attack) .

ATTACKING THE ROUTER

STEP 1 first open root terminal and enter the command(ipconfig | grep inet) ipconfig is used to get information regarding ip address whereas grep command is used to filter something in our case inet " | " (pipeline is used to connect two different command in linux) this command will show us our current ip address inside the network

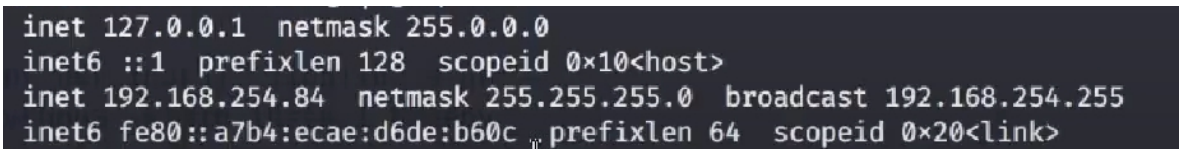

Figure 17 showing my ipaddress inside the network

STEP 2 After getting the inet or ip address , netmask and broadcast I will calculate the iprange of the network manually . ip range of this network is 192.168.254.0/24 . if you don't know how to calculate ip range of network you can check it by entering the command "ipcalc" followed by the ip address .

```
Address:   192.168.254.84       11000000.10101000.11111110. 01010100
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
⇒
Network:   192.168.254.0/24     11000000.10101000.11111110. 00000000
HostMin:   192.168.254.1        11000000.10101000.11111110. 00000001
HostMax:   192.168.254.254      11000000.10101000.11111110. 11111110
Broadcast: 192.168.254.255      11000000.10101000.11111110. 11111111
Hosts/Net: 254                   Class C, Private Internet
```

Figure 18 showing network range

STEP 3 Now when we have the iprange min&max host value we will find out the ip of the router . generally the ip of the router is host max value which is 192.168.254.254 but cross checking is always better . we will cross check it by using the concept that router communicate via web interface which means it uses http services that means it uses port 80. so we will scan the network for the device which is using port 80 via a nmap command (nmap -p 80 192.168.254.0/24 --open) .

```
PORT   STATE SERVICE
80/tcp open  http
MAC Address: B0:35:9F:CF:7D:E9 (Intel Corporate)

Nmap scan report for gateway.frontierlocal.net (192.168.254.254)
Host is up (0.0017s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: C0:89:AB:48:E9:A0 (Arris Group)

Nmap done: 256 IP addresses (8 hosts up) scanned in 9.78 seconds
```

Figure 19 showing ip address of the router

After checking the nmap result we came to conclusion that our assumptions were right and ip address for the router is 192.168.254.254 .

STEP 4 launching the routersploit (The RouterSploit Framework is an open-source exploitation framework dedicated to embedded devices. It consists of various modules that aids penetration testing operations)

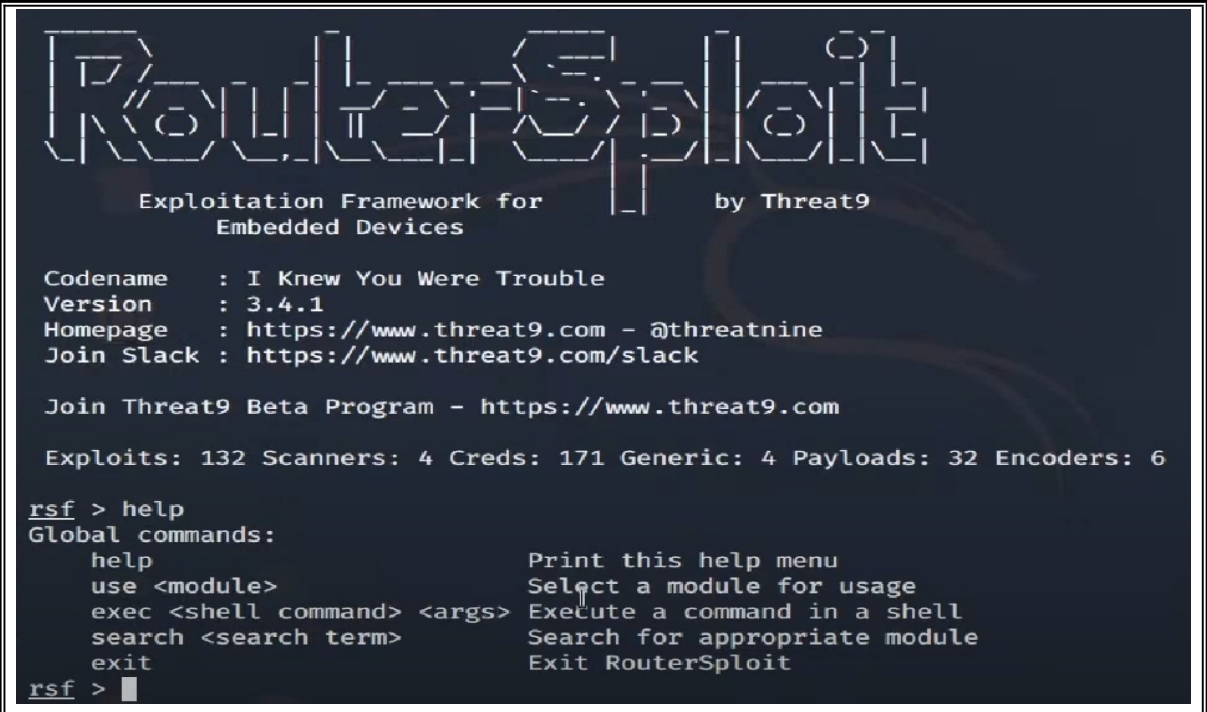

Figure 20 showing routersploit framework

Router sploit has salot of modules but what we are going to use scanner

STEP 5 In this step we will use the scanner module to search exploit for the router so will use the command use " scanner/autopwn"

STEP 6 once we are inside the module we have to specify the target by using the command

Set target followed by the ip address in my case (set target 192.168.254.254)

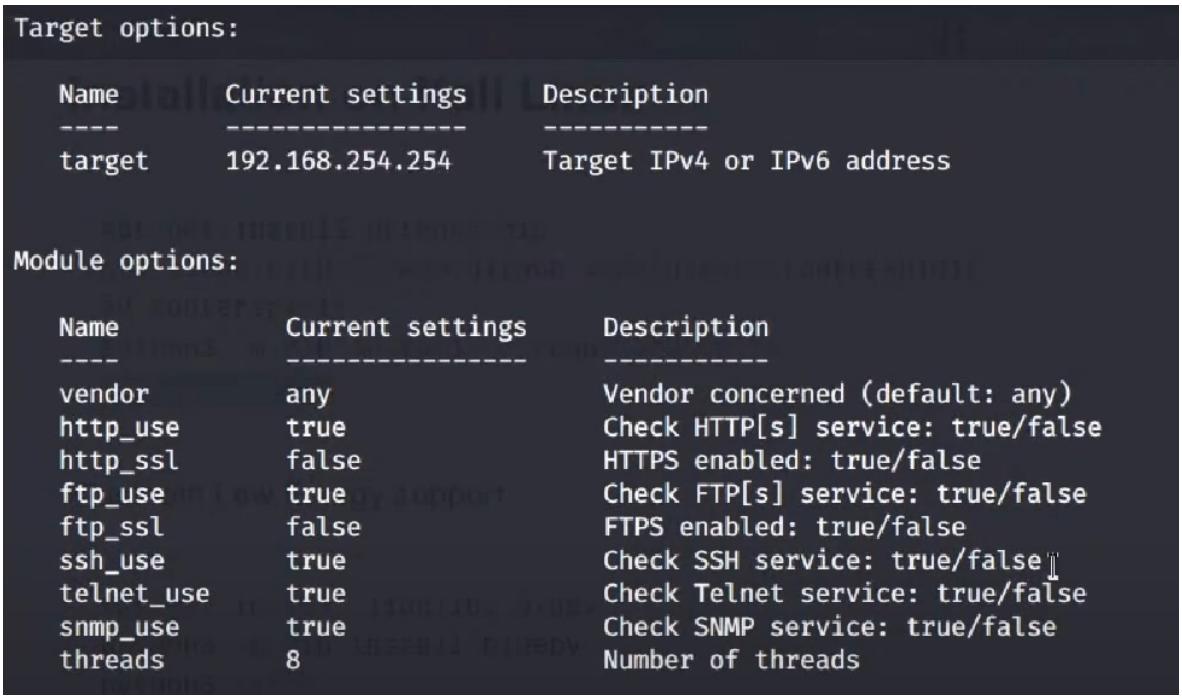

Figure 21 showing target options

STEP 7 AS soon as target is entered and all target options are verified then run routersploit to check for the available exploits

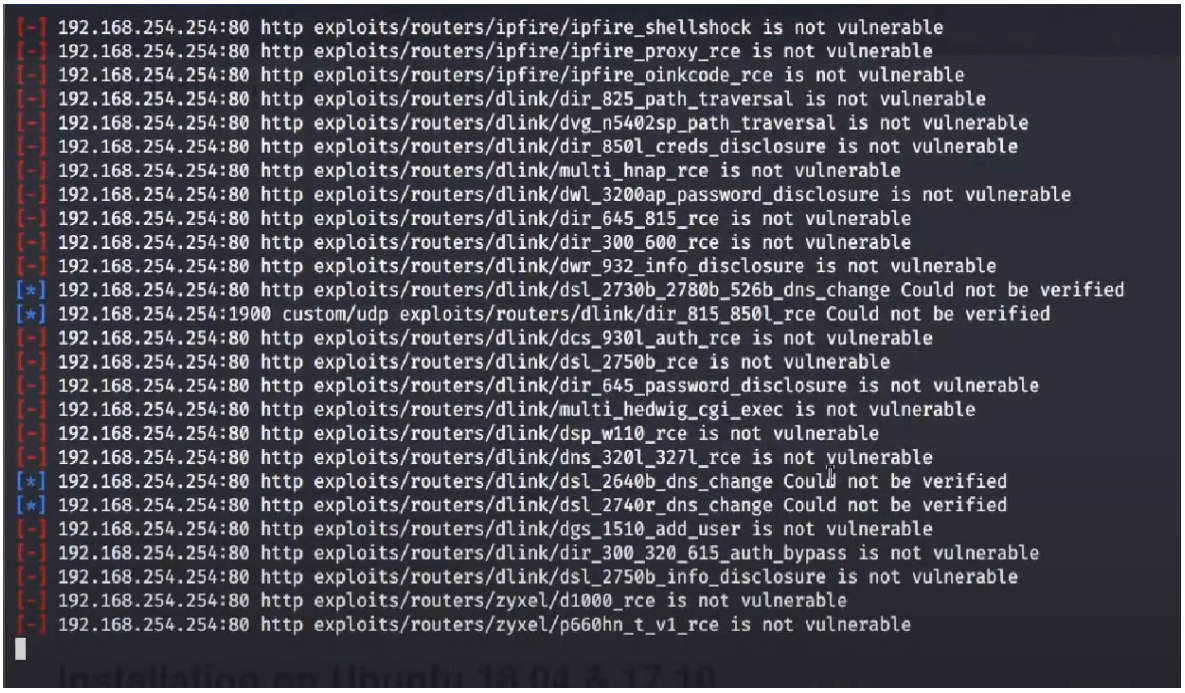

Figure 22 showing scanning process of routersploit

STEP 8 analyze the results for any vulnerability and other information such as router model etc.

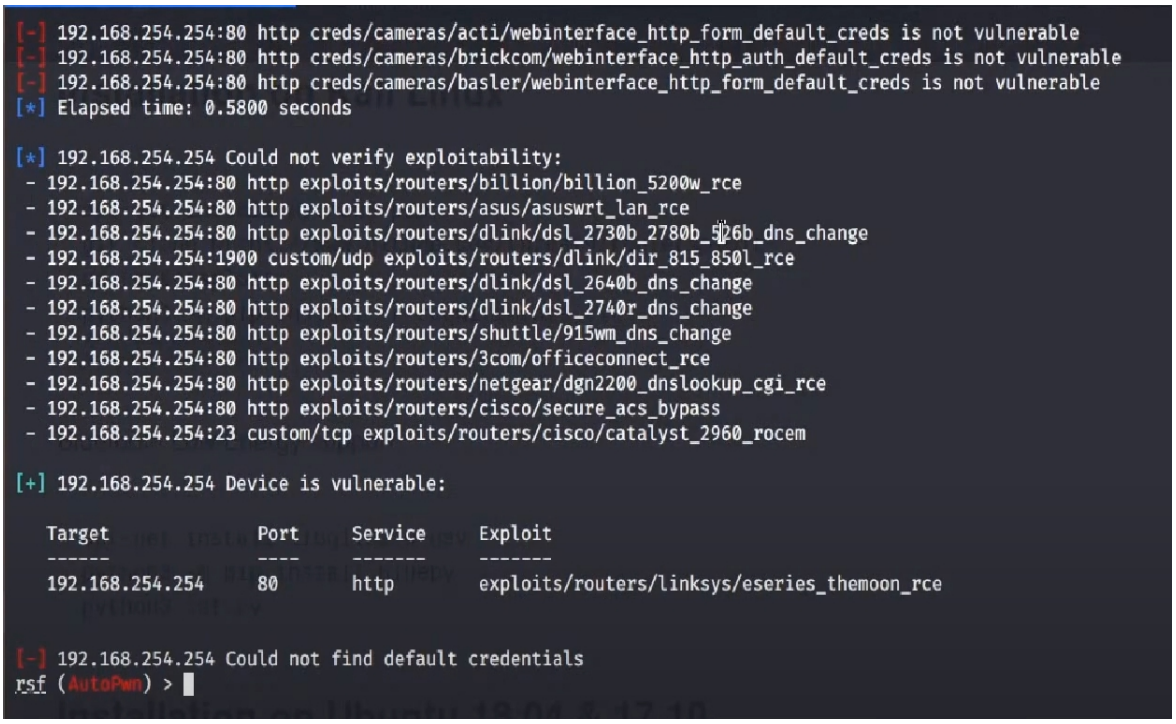

Figure 23 showing results of the scan .

After analysis of results we found that router is a linksys router and it is vulnerable to exploit .(exploits/routers/linksys/eseries_themoon_rce) .

STEP 9 now we can use the exploit to penetrate the router for this use command (use exploits/router/linksys/eseries_themoon_rce) | set target 192.168.254.254 and then give run command to execute it .

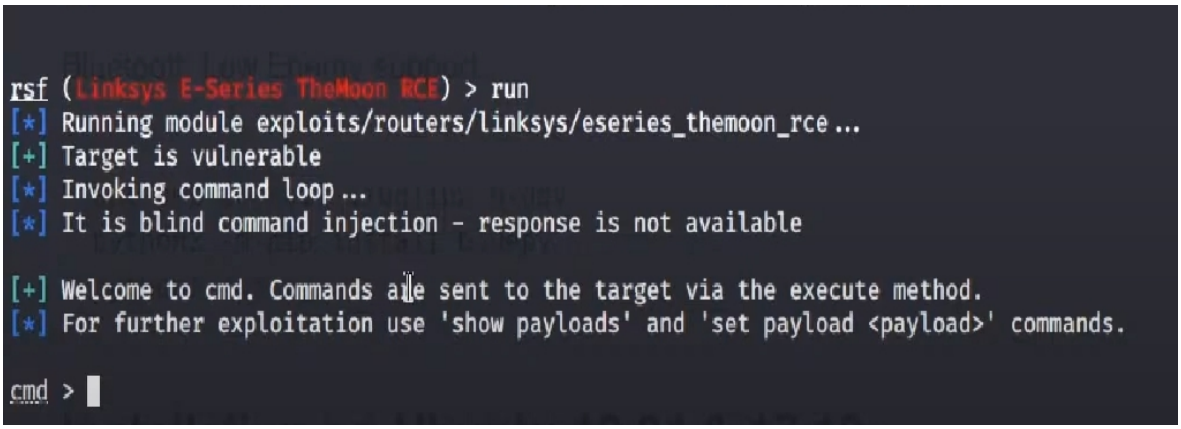

Figure 24 showing vulnerability

The device is also vulnerable to blind injection(Blind SQL injection arises when an application is vulnerable to SQL injection, but its HTTP responses do not contain the results of the relevant SQL query or the details of any database errors.) what it basically means is I can run and execute any command it will run and work but I cannot see it since our target is a embedded device a router .

If it is vulnerable to blind injection it is vulnerable to payloads and backdoor but for the sake of ethical aspect I'm not infecting someone else home router with a backdoor as I don't have permission to do so .

Experiment results the device is vulnerable to

- exploit (exploits/router/linksys/eseries_themoon_rce)
- Vulnerable to blind injection
- Vulnerable to payloads and backdoor.

ATTACKING THE SLEEP TRACKER DEVICE

Previously while scanning the network we fond two devices on the network which is using http protocol . out of which one was the router and there was one more unknown device after few searches I found that its a sleep tracker .

```
PORT   STATE SERVICE
80/tcp open  http
MAC Address: B0:35:9F:CF:7D:E9 (Intel Corporate)

Nmap scan report for gateway.frontierlocal.net (192.168.254.254)
Host is up (0.0017s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: C0:89:AB:48:E9:A0 (Arris Group)

Nmap done: 256 IP addresses (8 hosts up) scanned in 9.78 seconds
```

Figure 25 showing sleep tracker device in network

AT the time of attack I was having no idea how to penetrate a sleep tracker so I tried a denial of service attack and to my surprise it worked .and to do so I used metasploit tool

This is a single step attack

Open metasploit and type the command "use auxiliary/dos/tcp/synflood", from that the "RHOST 192.168.254.179" and "RPORT 80" was configured. In order to execute the experimental attack, the command "exploit" was executed

RESULT OF THE EXPERIMENT

When the attack was performed the network enabled device, the Sleep Tracker, started to behave strange. According to the results viewed in the graphic user interface of the Sleep Tracker by the owner , there was a lack of heart rate and breathing rate during the attack and the inadequate collection of data was showed with some delay. The breathing rate was presented as a blue graph and heart rate was presented as a green graph . Further the device shut down.

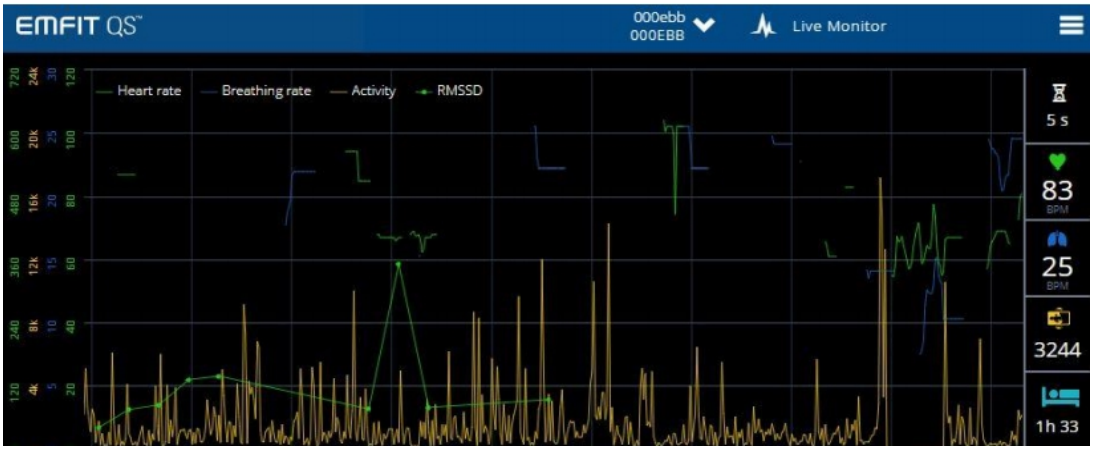

Figure 26 showingResult from Denial of Service-attack. The result presented in the graphic user interface for the Sleep Tracker

CHAPTER -V RESULTS AND CONCLUSION

RESULTS

At the end of this thesis we were able to satisfy the aim of the experiment that was to find bugs and vulnerability in smart homes and IOT devices used in smart homes to minimize and mitigate the vulnerability for future.

BUGS and vulnerability found in main network was

- ✓ It was vulnerable to Denial of service attack .
- ✓ It was vulnerable to Man in the middle attack.
- ✓ Weak password which was easy to crack .

BUGS and vulnerability found in the router was

- ✓ It was vulnerable to exploit (exploits/router/linksys/eseries_themoon_rce).
- ✓ It was vulnerable to blind injection .
- ✓ It was vulnerable to payloads and backdoors (Trojan horse).

BUGS and vulnerability found in sleep tracker device

- ✓ It was vulnerable to Denial of service attack .

CONCLUSION

At the end of our experiments we were able to answer the all question of our objective question which are-

What are the common communication technologies used in the context of a smart home?

As a result of this works literature study, the common used communication technologies are technologies that appear often in journals. ZigBee, Z-Wave and Wi-Fi, KNX RF, Bluetooth LE and Thread. All these communication technologies are wireless and can provide the user with a working smart home environment. All network enabled devices with any of this communication technology implemented are fully connected and provides the user efficiency, comfort and safety.

What are the security threats found in the communication technologies in the context of smart homes and what are their consequences?

The results of this are presented in the Theory chapter for each communication technology in the context of a Smart home. They are all vulnerable for attacks of different sort. Based on the reported literature, several problems were identified to the Smart Homes regarding the security aspect. The devices used in Smart Homes are often categorized as low-constrained, which makes it difficult to implement the combination to provide full security and proliferation due to low energy consumption, computation power and memory. That is the main reason that security mechanisms such as TLS or DTLS are not used consequently and resulting in security problem for the communication protocol.

On the basis of work done in this thesis I can suggest few security policies which will make smart home network more efficient and less vulnerable

Firstly all smart home network should work on thread network instead of wifi according to my analysis thread is more secure than wifi.

As a future tool to mitigate attacks and threats for the smart home a security policy could be a good choice. Security policies has a crucial role in organizations and workplaces, since it is a guide how to manage and maintain, how use the tools, network and whom should have access to assets. As a suggestion a security policy in a Smart Home could be formed as follow.

• Integrate safety in the construction phase Security should be evaluated as an essential part of any network-connected device. It is still very common for safety to be overlooked when products are to be launched from the companies.

• Advance security updates and management of vulnerability Through patching, security updates and vulnerability handling strategies, the security can be strong already in the design phase. This means e.g. that the default password is replaced and that the updates are scheduled.

• Built on proven security practice Many of already used practices which are used in the common IT and network security is a good starting point when implementing security in the Smart Home area. This can identify possible vulnerabilities and help to recover from damages and disruptions to the network enable devices.

• Prioritize security measures in relation to its consequences It is important to know where specific security measures should be targeted in the system, by focusing on consequences of disruptions or malicious activities it can tell where the focus of the security should be directed.

• Support the transparency over the Smart Home system If possible, developers and manufacturers need to know the supply chain. This means relative to Smart Home security that they need to know if there is any vulnerability with software or hardware provided by the vendor outside their organization. Increased collaboration and awareness can help manufacturers and consumers to discover where and how security measures should be implemented

• Connect carefully and thoughtfully Smart Home consumers should consider if a permanent connection is necessary, considering the risks of a disturbance. By this is meant that perhaps some units do not have to be used continually, when battery or similar is used.

CHAPTER VI REFERENCES

[1] M. Schiefer, ”Smart Home Definition and Security Threats,” 2015 Ninth International Conference on IT Security Incident Management & IT Forensics, 2015.

[2] R. Lutolf, ”Smart Home concept and the integration of energy meters into a home based system,” Seventh International Conference on Metering Apparatus and Tariffs for Electricity Supply 1992, pp. 17-19, 1992.

[3] J. Bugeja, A. Jacobsson och P. Davidsson, ”On Privacy and Security Challenges in Smart Connected Homes,” 2016 European Intelligence and Security Informatics Conference, 2016.

[4] U. LLC, ”Cybersecurity Considerations for Connected Smart Home Systems and Devices,” UL LLC, Northbrock , 2017.

[5] E. W. Wildauer och F. H. d. Silva, ”Ethical, Social, Privacy, Secuirty and Moral Issues in an ESociety,” i Information Systems and Technologies (CISTI), 2013.

[6] J. Bugeja, A. Jacobsson och P. Davidsson, ”Smart Connected Homes,” i Internet of Things A-Z; Technologies and Applications, Wiley-IEEE Press, 2018, pp. 359-381.

[7]M. R. Alam, M. B. I. Reaz och M. A. M. Ali, ”A Review of Smart Homes—Past, Present, and Future,” IEEE Transactions on Systems, Man, and Cybernetics, vol. 42, nr 6, pp. 1190-1203, 2012.

[8] D. Schatz, R. Bashroush och J. Wall, ”Towards a More Representative Definition of Cyber Security,” The Journal Digital Forensics, Security and Law, vol. 12, nr 2, pp. 53-74, 2017.

[9] D. C. Lévy-Bencheton(ENISA), M. E. Darra(ENISA), M. G. Tétu(Trusted Labs), D. G. Dufay(Trusted Labs) och D. M. Alattar(Trusted Labs), ”Secuirty and Resilience of Smart Home Environments - Good Praticies and Recommendations,” ENISA, Heraklion, 2015.

[10] M. N. Anwar, M. Nazir och K. Mustafa, ”Secuirty Threats Taxonomy: Smart-Home Perspecitve,” i 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA), 2017.

[11] National Cybersecuirty and Communication Integration Center , ”Attack Possibilities by OSI Layer,” U.S Department of Homeland Secuirty , 2014. [13] D. Kaur och P. Singh, ”Various OSI Layer attacks and Countermeasure to Enhance the Performance of WSNs During Wormhole Attack,” ACEEE Int. J. on Network Security , vol. 5, nr 1, pp. 62-67, 2014.

[12]M. A. B. Karnain och A. P. D. Z. B. Zakaria, ”A review on ZigBee Secuirty Enhancement in Smart Home Environment,” International Conference on Information Science and Security (ICISS), 2015.

[13] A. K. Ray och A. Bagwari, ”Study of Smart Home Communication Protocols, Secuirty and Privacy Aspects,” International Conference on Communication Systems and Network Technologies, vol. 7, 2017

[14] Cisco , ”IEEE 802.11ax: The Sixth Generation of Wi-Fi,” Cisco, 2018.

[15]] G. Lyon, ”Nmap: The Network Mapper,” [Online]. Available: https://www.nmap.org

[16] T. Nguyen, D. Nguyen, B. Tran, H. Vu and N. Mittal, “A Lightweight Solution for Defending Against Deauthentication/Disassociation Attacks on 802.11 Networks,” IEEE , pp. 185-190, 2008.

[17] R. Trimananda et al., “Vigilia: Securing Smart Home Edge Computing,” Third ACM/IEEE Symposium on Edge Computing, pp. 74-89, 2018

[18] F. Kilincer, F. Ertam and A. Şengür, "Automated Fake Access Point Attack Detection and Prevention System with IoT Devices," Balkan Journal of Electrical & Computer Engineering, vol. 8, no. 1, 2020.

[19] J. Melnick, “Top 10 Most Common Types of Cyber Attacks,” Netwrix Blog, 2020. [Online]. Available from: https://blog.netwrix.com/2018/05/15/top-10-most-commontypes-of-cyber-attacks/#Eavesdropping%20attack

[20] A. K. Sikder, G. Petracca, H. Aksu, T. Jaege and U. Selcuk, “A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications,” vol. 30, no. 3, pp. 291-319, 2018

[21] G. J. Brajones, C. J. Murillo, J. F.V. Valdés and L. F. Valero, “Detection and Mitigation of DoS and DDoS Attacks in IoTBased Stateful SDN: An Experimental Approach,” Sensors , vol. 20, no. 3, pp. 1-18, 03 02 2020

[22] Gates, J. J. McNutt, J. B. Kadane, and M. I. Kellner. “ Scan detection on very large networks using logistic regression modeling, ” i n ISCC ’06: Proceedings of the 11th IEEE Symposium on Computers and Communications, 2006, pp 402 – 408