Security Vulnerabilities of Popular Smart Home Appliances

Fida Hussain, Abhaya Induruwa (Retired), Man Qi
School of Engineering, Technology and Design
Canterbury Christ Church University
Canterbury, United Kingdom
e-mail: fh51@canterbury.ac.uk; beko539@gmail.com; man.qi@canterbury.ac.uk

***Abstract*—A Smart Home (SH) essentially is a communication network that connects smart devices, sensors and actuators, enabling the owner to locally and remotely access, monitor and control them. However, SHs are currently facing increasing challenges due to the underlying home automation systems, which are affected by network security issues. This paper presents an SH testbed comprising SH devices that employ IEEE 802.11 standard protocol for communication. Comprehensive tests were conducted using the testbed that incorporated popular SH devices with the aim to observe and understand vulnerabilities that exist in smart device networks when they are attacked using different types of attacks, such as Eavesdropping, Denial of Service (DoS), and Man-In-The-Middle (MITM). This paper presents the details of the SH testbed and reports and discusses the findings obtained from these experiments.**

Keywords-Smart Homes; device vulnerabilities; Smart Home Testbed; Eavesdropping; DoS; MITM attacks.

I. INTRODUCTION

SH is a user-oriented home communication system where gadgets are interconnected through a local network and exposed to the Internet, so that it can be remotely controlled from anywhere through the Internet by using network or mobile devices (smartphone or tablet). Gadgets on a SH network permit the authentication of a user to control different tasks, such as temperature control, adjusting the lighting, locking-unlocking of doors, and security access to the home from a distance [1]. Different apps can be installed on a smartphone or other devices connected to the network, or the user can use a timer programme and set up a schedule.

Some smart home appliances come with artificial intelligence (self-learning skill) so they can learn homeowner behaviour over time and alert the user or react by making necessary changes when something out of the ordinary happens [2][3]. They will alert the user if they detect suspicious activities for example, when motion is detected in the home when the user is away. Smart Homes face different challenges due to issues and features related to home automation systems. These include home automation standards, high installation costs, varying consumer inexperience with technology, additional and support costs, limited cooperation of smart devices manufacturers, complex user interfaces and security challenges from different security threats [2].

Connecting the SH to the Internet gives the user almost 24x7 access to it, subject to the availability of Internet. This allows the attacker from either locally, or remotely anywhere in the world to target the SH [4]. Such an attacker can scan for certain vulnerabilities related to a specific device or can keep searching until a particular vulnerability they are looking to exploit is found.

Internet of Things (IoT) devices that are used in SHs use different Wireless Local Area Network (WLAN) protocols, such as Bluetooth, ZigBee, Z-Wave, and IEEE 802.11. Due to convenience, most smart devices in SHs use IEEE 802.11variants. The legacy IEEE 802.11, released in 1997 and clarified in 1999, is now obsolete but the newer variants based largely on Orthogonal Frequency Division Multiplexing (OFDM) have witnessed continuous growth in popularity [5]. In current times, WLAN 802.11n through to 802.11ah are the more popular and successful indoor wireless solutions, having progressed as a key enabling technology to cover smaller to large organisations, public area hot-spots and so on [6]. The IEEE 802.11 standardisation committee has actively pursued to publish new draft modifications to integrate with up-to-date technologies and current challenges. However, there are currently different security challenges facing IEEE 802.11 based WLANs, such as Eavesdropping, DoS, MITM attacks, and so on.

For the purpose of the study reported in this paper, the SH testbed has been created by using different SH devices, which use the IEEE 802.11 standard protocol to communicate. To find vulnerabilities present in these devices forming the SH network, different types of attacks have been performed. The rest of this report is organised as follows.

Section II is a literature review. Section III is a summary of different types of attacks and their importance to a SH application. Section IV describes the smart devices used in developing the SH testbed. Section V presents the results that were achieved by performing different experiments (different attacks) using the SH testbed. Finally, Section VI closes the paper with conclusions and some ideas for future work.

II. REVIEW OF RELATED WORK

Alsahlany, Almusawy and Alfatlawy [7] analysing the risk of a fake Access Point (AP) attack against Wi-Fi networks, discuss the security issues of the Wi-Fi user, such as those posed by fake APs. They have carried out experiments by creating fake APs to launch a MITM attack to sniff, capture and analyse the victim's traffic. However, their scope is somewhat limited as the work focuses only on a fake AP attack against Wi-Fi networks, but the chances that the user would connect to the fake AP are rather low.

Jose and Malekian [4] 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 SH testbed

ISBN: 978-1-61208-837-2

to carry out experiments to find vulnerabilities and apply suggested security measures.

Kilincer, Ertam and Şengür [8] propose an automated technique to detect and prevent fake AP attacks in a network with IoT devices. In the experiment, they use a Single Board Computer (SBC) and a wireless antenna (ODROID module). The whole operation has been divided into three stages. In the first stage, a fake AP broadcast has been created. The second stage is to scan the surroundings using the SBC and Wi-Fi modules and in the last stage, to prevent detecting fake AP broadcasts. The fake AP has been assigned to an unauthorised Virtual Local Area Network (VLAN). This research is limited and focuses on fake AP attack detection and prevention, but the data collection about the network and some of the attacks are still possible without connecting to it.

Doughty, Israr and Adeel, [9] have studied vulnerabilities in six different Internet Protocol (IP) cameras by performing various attacks using Address Resolution Protocol (ARP) poisoning. Their findings show that IP cameras are still vulnerable to ARP poisoning and spoofing, and the criminals can take advantage of it. Due to the lack of security in devices and applications, they remain insecure to ARP poisoning. At the end of their research, they suggest methods of preventing ARP poisoning. Their research is limited to some IP cameras, and not to other SH devices where ARP poisoning attack is possible when used as part of an SH network.

Yoon, Park and Yoo [10] analyse security vulnerabilities in SHs in IoT environments and propose countermeasures. Although they talk about different vulnerabilities and countermeasure, such as trespass, monitoring and personal information leakage, DoS/ Distributed Denial of Service (DDoS) attacks and falsification, all of which are possible to happen in SHs, they have not set up an SH testbed to carry out experiments to find the sugested vulnerabilities and study how to prevent them with counter measures.

Davis, Mason and Anwar [11] conducted vulnerabilities and security posture studies of smart home IoT devices. They conducted their own vulnerabalities experiments that compared security posture between well known and less known vendors through misuse and abuse case analysis. Based on their analysis, the main finding was the need for a stronger focus on the security posture of lesser known vendor devices. Their approach utilised software engineering modeling methods, such as use cases, misuse cases, and abuse cases. These use cases were defined based on the device functionality and assumptions of interconnectivity by the manufacturer. However an SH testbed was not setup to carry out these experiments.

III. NETWORK SECURITY THREATS FOR IOT IN THE SH

Based on their key features, wireless protocols can be further divided into different communication protocols, such as ZigBee, Wireless Fidelity (Wi-Fi), Z-Wave, IPv6 Low-power wireless Personal Area Network (6LoWPAN), Bluetooth, etc. [12]. The properties and key features of these protocols are shown in Table I. Due to high bandwidth and fast speed, wireless is most used everywhere [13], and most IoT devices use a wireless connectivity protocol. The work reported in this paper is based on IoT devices that use Wi-Fi connectivity (IEEE 802.11x). Due to the high use of IEEE 802.11x by different devices nearly everywhere, including IoT in houses, hospitals, and hotels, they attract a lot of attention of attackers to launch different types of attacks either remotely or locally for different motives. Some of the common types of local attacks that are still dangerous to local IoT devices are eavesdropping (aka sniffing or spoofing), de-authentication, and man-in-the-middle, which are further explained in the next sections.

TABLE I. WIRELESS PROTOCOLS AND THEIR FEATURES

Features	**Wireless Protocols**				
	Wi-Fi	**ZigBee**	**Z-Wave**	**Bluetooth**	**6LoWPAN**
Standardisation	IEEE 802.11a/b/g	IEEE 802.15.4	Proprietary	IEEE 802.15.1	IETF
Frequency band	2.4GHz, 5GHz	868/915 MHz, 2.4GHz	900MHz	2.4GHz	868MHz, 900MHz and 2.4GHz
Range (m)	46/ 92	10-100	30	1, 10, 100	20
Security algorithm	WPA, WPA2	AES-128	AES-128	E0, E1, E3, E21, E22 56-128 bit	AES- 128
Topology	one-hop	star, tree, mesh	star, mesh	p2p, scatternet	mesh
Channel bandwidth	22MHz	0.3/0.6 MHz, 2MHz	300kHz, 400kHz	1MHz	600kHz, 2MHz, 5MHz

A. *Eavesdropping Attack*

This is also known as sniffing or spoofing attack. It is used to sniff the network traffic in wireless networks that connect IoT devices via Bluetooth, IEEE 802.11x, or Radio Frequency Identification (RFID). It is carried out by illegally impersonating a legal IoT device to gather information via sniffing [14]. Eavesdropping attack is an important first step before launching any type of attack on IoT devices. For example, by the launch of this attack an attacker can obtain passwords, credit card numbers, emails, documents, browsing history, login details, File Transfer Protocol (FTP) login details, FTP documents, web addresses, and other confidential information, that users or devices may normally send over the network [15].

This kind of attack is performed to gain illegal access to information to launch de-authentication or man-in-the-middle attack [16]. It gathers all types of traffic including encrypted traffic. A tool, such as Sniffer may be used to sniff packets to gather information. It is impossible to detect and penetrate vulnerabilities on the system's (i.e., computer's) wireless adapter. Therefore, to manage and monitor IEEE802.11 b/g/n devices' traffic, two types of wireless adapters, namely ALFA AWUS036NHA 2.4 GHz and ALFA AWUS036ACH 2.4 & 5 GHz were used. These wireless adapters have been used as they are compatible with IEEE802.11 b/g/n traffic, and work with a maximum connection rate of 150 Mbps [7]. When devices are communicating with each other using wireless protocols, their Medium Access Control (MAC) addresses are encrypted.

It is known in packet communications basics that a MAC address makes sure that a packet is delivered only to the right destination (identified by the recipient's MAC Address). This in turn leads to the question how a device can receive a packet which is not destined for it? In sniffing, since Wi-Fi packets are present all around in an area within a specific range, i.e., the wireless footprint, the external wireless adapter is used by the attacker after changing the setup from 'manage mode' to 'monitor mode'. Doing this makes it possible to capture all the packets in the surrounding Wi-Fi range.

To change a wireless adapter from manage mode to monitor mode, an open-source tool called Airodump-ng, which also includes an Aircrack-ng package, has been used. Aircrack-ng is a tool used for analysing network security, especially by monitoring, attacking, testing and cracking Wi-Fi networks [7][17][18].

Once the attacker selects a specific network to target, the attack is launched by giving a specific AP MAC address, a channel with monitor mode to write (save) the data in a file so it can be analysed later. By analysing the saved file some useful information, such as manufacturer's name and MAC address of all devices that are connected to that specific AP, can be found. A de-authentication attack can be launched by a tool called Aireplay-ng [7], which enables the attacker to disconnect specific devices by using their MAC addresses.

B. Denial of Service (DoS) De-authentication attacks on 802.11 based networks

DoS is a challenging attack on computing devices, caused by bombarding with requests during a certain period, forcing the target devices to crash, go-slow, or shutdown altogether [19]. As IoT devices are limited in resources, DoS attacks may cause more damage to them [20]. Most IoT devices use low priced hardware with low-cost deployment of IEEE 802.11-based networks. Due to their popularity, IoT devices (roughly 30 billion devices in use in 2020) and 802.11 networks are attacked by the largest number of attackers [20][21]. Researchers are working hard to fix these vulnerabilities in 802.11 networks by bringing out different security standards in the protocol, such as Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP), 802.11i, 802.1x [22]. Even so, there are still some vulnerabilities that are not yet dealt with by any of these security standards. One such attack is the de-authentication attack. 802.11 networks can operate in infrastructure mode (i.e., devices communicating with one another by first going through an access point) or in ad-hoc (peer to peer) mode. An 802.11 network, when operating in infrastructure mode, needs the wireless device to connect to an AP before the data messaging takes place. In this process the device needs to validate itself to the AP before communicating with the AP. If either the client device or the AP wants to disconnect itself from the other, they send a de-authentication frame to leave the network. When client devices and AP are communicating with each other these frames are unencrypted, and an attacker can easily spoof these frames, which have the unencrypted MAC addresses of the devices and the AP. Using them, the attackers can easily launch a DoS attack (de-authentication attack) to disassociate the client device from the AP.

In a pre-connection type of attack, where the attacker is not part of the network, a DoS attack that targets communication between the AP and the gadget is launched allowing the attacker to disconnect the gadget from the network for a certain period of time defined by the attacker. The attacker sends a packet to the AP and the target device, therefore it will disconnect the device for a defined period of time. This kind of attack can be used to disable SH IoT devices, such as a Closed Circuit Television (CCTV) IP camera, gateway, smartphone, or any other device present in home automation to gain access to the home without notice [23]. In this, the attacker sends packets to the router by pretending that it is a target device using the spoofed MAC address. In the meantime, the attacker is pretending to be a router to the target and is telling it to re-authenticate itself. This is a kind of ethical hacking attack performed by placing different gadgets like Amazon Echo, Google Home, Android smartphone, iOS phone, Android tablet and IP Dynamode Camera.

This kind of attack is useful to the attacker in many ways. It is very useful in social engineering exercises where you could disconnect clients from the target network, and then call the user and pretend to be a person from the IT Department and trick them to install a virus or a backdoor. The attacker can also create another fake access point and persuade the gadgets to connect to the fake access point to spy on them, sniff and spoof their traffic. Besides, it is also possible to launch a man- in-the-middle attack because the attacker would have gathered all the useful information. This kind of attack can also be used to capture the handshake, which is vital when it comes to WPA cracking.

C. MITM (Man-In-The-Middle) attack

It is the type of attack where the attacker successfully changes the communication between two parties (i.e., sender and receiver), where the sender and receiver believe that they are communicating with a genuine party but the entire communication is controlled by the attacker. MITM can be known by different names like Bucket-brigade attack, Fire brigade attack, Monkey-in-the-middle attack, Session hijacking or Transmission Control Protocol (TCP) hijacking. Before the MITM attack is lunched, the communication traffic is only monitored and read. This is a passive act, but it gathers plenty of information to launch the subsequent attacks.

An MITM attack can be implemented through different ways, but in the testbed, it has been implemented by 1) using fake access point, and 2) by using ARP poisoning. A fake access point can be set up by using the information, such as MAC address, channel, and Service Set Identifier (SSID), that was gathered by sniffing and spoofing. Using a tool called Mana-toolkit in Kali Linux, a fake AP will be configured to have the same setup as the target AP, such as identical user name AP, but it will be a network without encryption and that broadcasts a strong signal by using a Network Interface Card (NIC), [1] such as ALFA AWUS036ACH, with an external antenna. Before connecting target devices to the fake AP, a DoS (de-authentication) attack is launched to disable devices on the target network. When the target devices connect to the fake AP then the whole traffic will be going to the man-in-the-middle and it will make it easier to steal the information from the compromised devices. Method 2, ARP poisoning, is an attack performed on a LAN, where the attacker falsely advertises the MAC addresses of the default gateway and the target device and fools both devices to connect to the attacker. The ARP poisoning is only possible when the attacker is part of the target network. ARP poisoning can be carried out using a tool called Man-In-The-Middle framework (MITMf). MITMf is a powerful tool that can be used to intercept and modify the flow of packets between the victim and AP because the flow of the packet is now through the attacker. As all the traffic is going through the MITM, the attacker knows about the victim using the Internet.

IV. Developing the Smart Home Testbed

To practically test, analyse and understand the security of SHs, an expert needs to develop an SH testbed containing a mix of different, random, IoT devices that are commonly found in a modern smart home. For this purpose, the testbed shown in Figure 1 has been developed by incorporating a range of devices representing home gateways, IP cameras, various smart phones and tablets, programmable single board computer, all connecting to the home router. The particular devices chosen are Amazon Echo, Amazon Dot, Google Home, smart IP Camera (IP Dynamode White DYN-630), IPhone4, Sony Xperia Tablet, and Nest Cam Indoor Security Camera. Amazon Echo, Amazon Dot, and Google Home are home gateways that allow voice control. They are all very popular and millions of people use them in their homes in everyday life to ease their life [24]. Amazon Echo and Google Home are smart speakers with the 'assistant features', using which the user can ask about the weather, news, use them as a search engine, in addition to controlling other smart devices that are connected to them. IP Dynamode White (DYN-630) is a wireless camera that has a range up to 8 metres. Among its features are zoom, motion detection, video support control, two-way voice talkback, and an external alarm which sends information directly to the server via email or FTP. With all these functionalities and an affordable price, it makes it perfect to use in a SH. Google Nest Cam Indoor Security Camera with a good quality picture (1080p), viewing angle with 130 diagonal degrees, private and secure communication (128-bit AES encryption, TLS, 2048-bit RSA private keys, Perfect Forward Secrecy) is more advanced than IP Dynamode. However, it is more expensive than IP Dynamode White (DYN-630). Sony Xperia Tablet Z LTE and Samsung Galaxy s7 edge are used as a user interface to install different SH apps to control and monitor systems. The Raspberry Pi 3 used in the SH testbed is a low cost, yet powerful, programmable computer. Among its many useful features is the General Purpose Input Output (GPIO) interface that is being used to create IoT solutions for the smart home. The testbed also includes an iPhone4. Although quite a few years old now, this is a smart device that is increasingly being used as DIY security cameras in SHs [25][26]. The use of old iOS devices in SHs is an attractive proposition, but such appliances open up vulnerabilities and introduces security threats in SHs making it very important to understand how SH security landscapes are impacted with such use. It is in this context an old, but popular device, such as iPhone4 is included in the testbed.

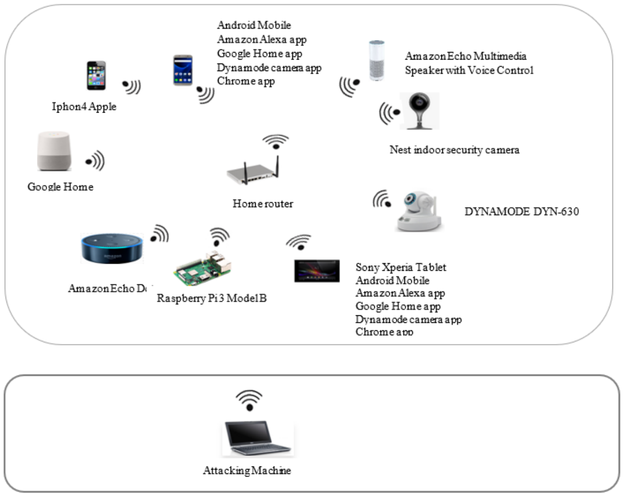
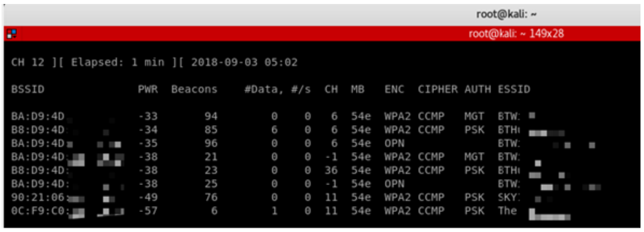


Figure 1. Smart Home Testbed

After developing this testbed, different security tests were carried out. As it is impossible to detect and penetrate vulnerabilities on the system through a local wireless adapter in a laptop, two types of wireless adapters namely ALFA AWUS036NHA 2.4 GHz and ALFA AWUS036ACH 2.4 & 5 GHz were used to manage and monitor the devices' Wi-Fi traffic. Kali Linux is operating on the attacking machine. In the eavesdropping, de-authentication and fake Access Point attacks, it is playing the role of the outside attacker and in the ARP poisoning attack, it plays the role of an internal actor.

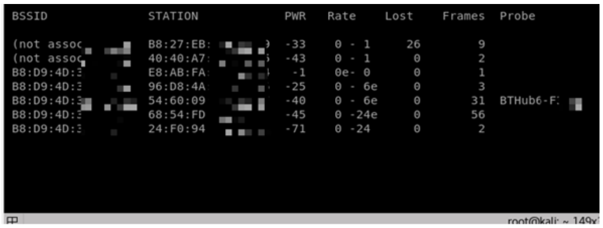
V. Results

To get the results of these attacks, the attacker needs to go into monitor mode, which is called sniffing or spoofing (passive attack) where it sniffs all the traffic without a connection to an AP or to ad-hoc network. Collecting information in this stage is important in order to launch a further attack on the target device. All the APs and connected devices can easily be identified in a limited range. Figure 2 shows the features of the APs and devices that are connected to these APs after executing the Airodump-ng tool in the neighbouring area, and it provides us with very useful



```
CH 12 ][ Elapsed: 1 min ][ 2018-09-03 05:02

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

BA:D9:4D [redacted]  -33       94        0    0   6  54e  WPA2 CCMP   MGT  BTW [redacted]
B8:D9:4D [redacted]  -34       85        6    0   6  54e  WPA2 CCMP   PSK  BTH [redacted]
BA:D9:4D [redacted]  -35       96        0    0   6  54e  OPN              BTW [redacted]
BA:D9:4D [redacted]  -38       21        0    0  -1  54e  WPA2 CCMP   MGT  BTW [redacted]
B8:D9:4D [redacted]  -38       23        0    0  36  54e  WPA2 CCMP   PSK  BTH [redacted]
BA:D9:4D [redacted]  -38       25        0    0  -1  54e  OPN              BTW [redacted]
90:21:06 [redacted]  -49       76        0    0  11  54e  WPA2 CCMP   PSK  SKY [redacted]
0C:F9:C0 [redacted]  -57        6        1    0  11  54e  WPA2 CCMP   PSK  The [redacted]
```

Figure 2. Features of the Access Points



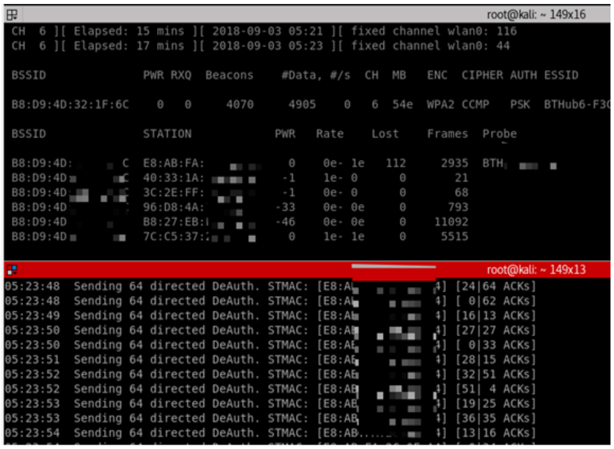
```
BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not assoc[redacted]  B8:27:EB:[redacted]  -33    0 - 1     26       9
(not assoc[redacted]  40:40:A7:[redacted]  -43    0 - 1      0       2
B8:D9:4D:3[redacted]  E8:AB:FA[redacted]    -1   0e- 0       0       1
B8:D9:4D:3[redacted]  96:D8:4A[redacted]   -25    0 - 6e     0       3
B8:D9:4D:3[redacted]  54:60:09[redacted]   -40    0 - 6e     0      31  BTHub6-F[redacted]
B8:D9:4D:3[redacted]  68:54:FD[redacted]   -45    0 -24e     0      56
B8:D9:4D:3[redacted]  24:F0:94[redacted]   -71    0 -24      0       2
```

Figure 3. MAC addresses of the connected devices

information. The first column shows the Basic Service Set IDentifier (BSSID) also called the MAC address of all APs in the surrounding area. The AP signal strength (PWR) is shown in the second column in decibels (db). The highest db value means the AP is nearest to the attacker. Information about the channel of the AP is important where the CH column exposes the information about the AP in the channel they operate. Most APs are using encryption keys for connection but some of them are open and do not have an encryption key. ENC column shows whether encryption is being used. OPN indicates an open connection. The last column shows the Extended Service Set Identification (ESSID), the names of APs that are broadcasting.

The detailed information that has been obtained and shown in Figure 2 can be used to launch a de-authentication attack (DoS) on each individual IoT that is connected to the specific AP. To launch a de-authentication attack, the MAC addresses of the target AP and the IoT device connected to it are required. To obtain the MAC addresses of the connected devices to AP, Airodump-ng with MAC address of AP is needed to be launched.

Figure 3 shows the MAC address of the connected device to the target AP. It is easy to launch a de-authentication attack after obtaining the required information (MAC Addresses of AP and target device). Figure 4 shows the successful launch of de-authentication for a certain defined time period where the target device is not aware of it. The target will not be able to connect to the AP unless it is restarted, or the end period defined by the attacker has been reached. As shown in Table II, the voice control of Amazon Echo, Google Home, and Amazon Echo Dot has strong resistance to a de-authentication attack. Although a de-authentication attack was successfully launched on the target devices the attacker was unable to disable the target devices' connections from the target AP.



```
CH  6 ][ Elapsed: 15 mins ][ 2018-09-03 05:21 ][ fixed channel wlan0: 116
CH  6 ][ Elapsed: 17 mins ][ 2018-09-03 05:23 ][ fixed channel wlan0: 44

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

B8:D9:4D:32:1F:6C    0   0     4070     4905    0   6  54e  WPA2 CCMP   PSK  BTHub6-F3C

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B8:D9:4D:[redacted]C  E8:AB:FA:[redacted]      0   0e- 1e    112     2935  BTH[redacted]
B8:D9:4D[redacted]C   40:33:1A:[redacted]     -1   1e- 0       0       21
B8:D9:4D[redacted]C   3C:2E:FF:[redacted]     -1   0e- 0       0       68
B8:D9:4D[redacted]    96:D8:4A:[redacted]    -33   0e- 0e      0      793
B8:D9:4D[redacted]    B8:27:EB:[redacted]    -46   0e- 0e      0    11092
B8:D9:4D[redacted]    7C:C5:37:[redacted]      0   1e- 1e      0     5515
```

```
05:23:48  Sending 64 directed DeAuth. STMAC: [E8:A[redacted]4] [24|64 ACKs]
05:23:48  Sending 64 directed DeAuth. STMAC: [E8:A[redacted]4] [ 0|62 ACKs]
05:23:49  Sending 64 directed DeAuth. STMAC: [E8:A[redacted]4] [16|13 ACKs]
05:23:50  Sending 64 directed DeAuth. STMAC: [E8:A[redacted]4] [27|27 ACKs]
05:23:50  Sending 64 directed DeAuth. STMAC: [E8:A[redacted]4] [ 0|33 ACKs]
05:23:51  Sending 64 directed DeAuth. STMAC: [E8:A[redacted]4] [28|15 ACKs]
05:23:52  Sending 64 directed DeAuth. STMAC: [E8:A[redacted]4] [32|51 ACKs]
05:23:52  Sending 64 directed DeAuth. STMAC: [E8:A[redacted]4] [51| 4 ACKs]
05:23:53  Sending 64 directed DeAuth. STMAC: [E8:AB[redacted]4] [19|25 ACKs]
05:23:53  Sending 64 directed DeAuth. STMAC: [E8:AB[redacted]4] [36|35 ACKs]
05:23:54  Sending 64 directed DeAuth. STMAC: [E8:AB......[redacted]4] [13|16 ACKs]
```

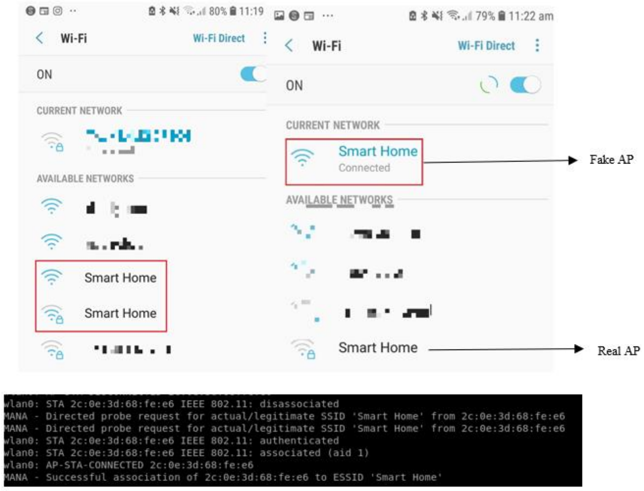
Figure 4. Launch of successful de-authentication attack

TABLE II. RESULTS OF DE-AUTHENTICARTION ATTACK

IoT Appliances	De-authentication Attack
Amazon Echo Google Home Amazon Echo Dot	Connection interrupted. Unable to disable their connection from the AP.
Android Mobile (Model no. SM-G935F, SM-G930F) Nest Cam Indoor Security Camera	Sometimes connection interrupted and device disabled from the connected AP.
DYNAMODE DYN-630 Iphon4 Apple Raspberry Pi 3 Sony Xperia Tablet	Connection interrupted and device disabled from the connected AP

However de-authentication was successful and Android mobile devices (Model nos. SM-G935F, SM G930F) were disabled when they were at roughly 10 metres from the connected AP. Furthermore, Nest Cam Indoor Security Camera was disabled for short duration of time (1 to 2 seconds) by the launching of de-authentication. As shown in Table II, IP DYNAMODE DYN-630, Apple IPhone4, Raspberry Pi 3 with Linux operating system, and Sony Xperia Tablet devices were successfully targeted, the connection was interrupted and the connection from the AP was disabled. This scenario presented the worst security concerns as they allowed every single attempt to drop their connection from any distance within the SH.

There are different ways to implement MITM attacks, but in the testbed, it has been implemented by using 1) fake access point and 2) ARP poisoning. In this experiment, as shown in Figure 5, the fake AP created is called Smart Home. It is similar to the target AP, but the fake Smart Home AP is without encryption. In this kind of situation, the attacker uses



```
wlan0: STA 2c:0e:3d:68:fe:e6 IEEE 802.11: disassociated
MANA - Directed probe request for actual/legitimate SSID 'Smart Home' from 2c:0e:3d:68:fe:e6
MANA - Directed probe request for actual/legitimate SSID 'Smart Home' from 2c:0e:3d:68:fe:e6
wlan0: STA 2c:0e:3d:68:fe:e6 IEEE 802.11: authenticated
wlan0: STA 2c:0e:3d:68:fe:e6 IEEE 802.11: associated (aid 1)
wlan0: AP-STA-CONNECTED 2c:0e:3d:68:fe:e6
MANA - Successful association of 2c:0e:3d:68:fe:e6 to ESSID 'Smart Home'
```

Figure 5. Victim connected to fake AP

DoS attack to force devices to disconnect from the genuine AP and connect to the fake AP.

In this experiment, an attacker can force the smart devices by using de-authentication attack and target device connect to fake AP as shown in Figure 5. But as it was evident from previous tests, it is hardly possible to disable many devices from the legitimate AP. Also, it would be harder to convince the victim to use the fake AP. For these reasons, it is not highly successful to target the SH by using a fake AP.

ARP poisoning MITM attack is possible when an attacker is part of the network. To launch ARP poisoning in Kali Linux, MITMf tool was used to perform ARP poisoning but before using MITMf, the attacker has to scan the whole network using a scanning tool, such as NMAP to know the MAC address of the target device and the IP address of the default gateway (AP). The target device responds and sends its MAC address. The ARP table, the IP address and MAC address of different devices including the gateway becomes available to the attacker. The attacker knows in detail about the time and what website the victim is using. To further capture and analyse the data packets, the attacker can use Wireshark [7]. This way some other vulnerabilities, such as session hijacking and denial of services can be exploited.

VI. Conclusions and Future Work

The use of wireless Wi-Fi devices is growing day by day with the extensive use of the Internet. If adequate security measures are not taken, it could have serious implications for SH devices. There is the possibility to view, capture and modify the data packets by the attacker using the existing vulnerabilities in SH devices and IEEE802.11 b/g/n traffic captured by nefarious means. The primary contribution of the research work is building and evaluating a testbed suitable for finding security vulnerabilities and threats in SH networks incorporating both new and old IoT devices. The testbed can then be expanded to include many more diverse SH IoT devices as they become available, and explore their vulnerabilities and possible security attacks on them.

This paper demonstrates that due to vulnerabilities remaining in some SH devices they are prone to attacks, such as eavesdropping, DoS and MITM. Throughout the whole experiment, Kali Linux operating system was used with ALFA AWUS036NHA 2.4 GHz and ALFA AWUS036ACH 2.4 & 5 GHz wireless adapters. Eavesdropping attack was used to sniff the network traffic of the wireless network. An open-source tool called Airodump-ng was used to sniff packets to gather information that would allow to mount an attack. The tool gathers some useful information, such as MAC address, channel, and ESSID. This information can later be used to mount DoS and MITM attacks. This kind of attack could be fatal as the IoT device can be disabled for a certain period. For the MITM attack the Mana-toolkit and MITMf were used. The two MITM attack types, i.e., using fake AP and ARP poisoning have been used to target SH devices as they are more effective and can damage SH devices. To avoid de-authentication attack, the device need to have a wired connection to the network, or if the connection is wireless, use the IEEE 802.11w, the amendment adding management frame protection functionality to 802.11 standard. This amendment was brought to provide better protection to control and management frames against forgery, replay and disconnect attacks. Security can also be enhanced by enabling 802.11w/WPA3 combination. Although a fully-fledged discussion on WPA3 is beyond the scope of this paper, it is worth noting that WPA3 secures a device even when weak passwords are used or when an attacker attempts to crack them using brute force techniques. The AP can add Message Integrity Check Information Element (MIC IE) to each management frame it transmits to protect them against any attempt to copy, alter, or replay by invalidating the MIC. To protect broadcast/multicast management frames a new key called Integrity Group Temporal Key (IGTK) is used.

ARP poisoning can be detected through different ways, such as using an open-source packet analyser, e.g., Wireshark, or using proprietary options, such as XArp and command prompt. The easy way to finding an ARP poisoning attack is by opening a command prompt as administrator. Running command ‘arp –a’ will show ARP table IP address and MAC address of connected devices. In this table, if two different IP addresses are displayed with the same MAC address, then it is possible that the network undergoing an ARP poising attack. To prevent this kind of attack, the ARP table needs to be configured with the static IP address and the MAC address. Chances of connecting to fake AP may be low but the SH user needs to be educated to avoid connecting to fake APs and to use a Virtual Private Network (VPN) connection which will encrypt communication between sender and receiver. The testbed will be used to study and understand how future SH devices can be secured from these attacks, and hope to share the knowledge thus created with the community.

References

[1] J. Chen, "*Investopedia,*" 2015. [Online]. Available from: https://www.investopedia.com/terms/s/smart-home.asp. [retrieved: February, 2021]

[2] V. S. Gunge and P. S. Yalagi, "Smart Home Automation: A Literature Review," International Journal of Computer Applications, pp. 6-10, 2016.

[3] K. E. Skouby and P. Lynggaard, "Smart Home and Smart City Solutions enabled by 5G, IoT, AAI and CoT Services," 2014 International Conference on Contemporary Computing and Informatics (IC3I), pp. 874-878, 2014.

[4] A. C. Jose and R. Malekian, "Smart Home Automation Security: A Literature Review," Smart Computing Review, vol. 5, no. 4, pp. 269-285, 2015.

[5] E. Perahia, "IEEE 802.11n Development: History, Process, and Technology," IEEE Communications Magazine, vol. 46, no. 7, pp. 48-55, 2008.

[6] M. S. Afaqui, E. Garcia-Villegas and E. Lopez-Aguilera, "IEEE 802.11ax: Challenges and Requirements for future High Efficiency WiFi," IEEE Wireless Communications, vol. 24, no. 3, pp. 130-137, 2017.

[7] A. M. Alsahlany, A. R. Almusawy and Z. H. Alfatlawy, "Risk Analysis of a Fake Access Point Attack Against Wi-Fi Network," International Journal of Scientific & Engineering Research, vol. 9, pp. 322-326, 2018.

[8] 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.

[9] T. Doughty, N. Israr and U. Adeel, “Vulnerability Analysis of IP Cameras using ARP Poisoning,” 8th International Conference on Soft Computing, Artificial Intelligence and Applications (SAI 2019), June, 2019.

[10] S. Yoon, H. Park and H. S. Yoo, “Security Issues on Smarthome in IoT Environment,” *SpringerLink,* vol. 330, pp. 691-696, 2015.

[11] B. D. Davis, J. C. Mason and M. Anwar, “Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study,” *IEEE Internet of Things Journal,* vol. 7, no. 10, pp. 10102-10110, 2020.

[12] A. N. Gollu and J. Kumar, “Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi,” in *Innovations in Electronics and Communication Engineering: Proceedings of the*, H.S.Saini, Ed., Springer, 2019, pp. 229-239.

[13] F. Hussain and M. Qi, “Integrated Privacy Preserving Framework for Smart Home,” 14th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), pp. 1246-1253, 2018.

[14] L. Xiao, X. Wan, L. Xiaozhen, Z. Yanyong and W. Di, “IoT Security Techniques based on Machine Learning: How do IoT Devices use AI to Enhance Security?,” *IEEE Signal Processing Magazine,* vol. 35, no. 5, pp. 41-49, 2018.

[15] 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-common-types-of-cyber-attacks/#Eavesdropping%20attack [retrieved: February, 2021]

[16] L. Xiao, Y. Li, G. Han, G. Liu and W. Zhuang, “PHY-Layer Spoofing Detection with Reinforcement Learning in Wireless Networks,” IEEE Trans. Vehicular Technology, vol. 65, no. 12, pp. 10037-10047, 2016.

[17] C. N. Klokmose, M. Korn and H. Blunck, “WiFi Proximity Detection in Mobile Web Applications,” p. 123–128, 2014.

[18] I. P. Mavridis, A.-I. E. Androulakis, A. B. Halkias and P. Mylonas, “Real-life Paradigms of Wireless Network Security Attacks,” 15th Panhellenic Conference on Informatic, pp. 112-116, 2011.

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

[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] N. Apthorpe, D. Reisman and N. Feamster, “A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic,” ArXiv Cryptography and Security, vol. abs/1705.06805, 2017.

[22] 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.

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

[24] S. Hornick, S. Santhanam, A. Hill and S. B. Krous, “How Smart Speakers will Reinvent Travel,” 2018. [Online]. Available:https://www.oliverwyman.com/our-expertise/insights/2018/sep/oliver-wyman-transport-and-logistics-2018/how-smart-speakers-will-reinvent-travel.html. [retrieved: February, 2021]

[25] Household Hacker, “How To Turn Your Phones Into WiFi Security Cameras”, https://www.youtube.com/watch?v=y7h8L2zeLdE [retrieved: March, 2021]

[26] H. Luijten, “Use your old iPhone as a Security Camera (IP Camera)”, https://www.tweaking4all.com/mobile-devices/ios/repurpose-old-ios/old-iphone-as-ip-camera/#related [retrieved: March, 2021]