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, Kent
United Kingdom
About the Presenter:

- Fida Hussain is currently a full time PhD student at Canterbury Christ Church University working on IoT to develop security framework for Smart Home Automation.

- Fida has published a book chapter on Intrusion Detection System (IDS) on Smart Home security “Hybrid Intrusion Detection System for Smart Home Applications” published in Developing and Monitoring Smart Environments for Intelligent Cities, IGI Global 2021.


- Fida worked for three years as IT Consultant for hospitality company since 2014 to 2017 after graduating with MSc in Computing from Canterbury Christ Church University in 2012.
Today’s Agenda

1. Introduction
2. Review of related work
3. Network security threats for IoT in the SH
   a. Eavesdropping attacks
   b. Denial of Service (dos) De-authentication attacks
   c. MITM(Man-In-The-Middle) attacks
4. Methodology (Smart Home testbed)
5. Results
6. Conclusions and future work
Introduction

Smart Home (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).

https://www.presentationload.com/smart-home-oxid.html
Introduction

Source: Josh Jackman (theecolexperts)

There are 2.22 million smart homes in the UK.

A smart home could save you:
£450 and 8 days every year

The Internet of Things’ global revenue: 72.6 billion

Whilst the connected products market continues to grow, you can make savings too. With a spare 8 days and £450, you could treat yourself to an all-inclusive trip to the Balearic Islands. Work smarter, not harder.

By 2023, 16.7% of global households will own a smart device

If you're still trying to work out the benefits of creating your own smart home, 15.3 million Brits have a smart home device - and 98% of them are satisfied! If you're looking to save time and money, smarten up your home.

https://www.theecolexperts.co.uk/smart-home/statistics
Review of related work

1. Risk analysis of a fake access point attack against Wi-Fi network
2. Smart Home Automation Security: A Literature Review
3. Automated Fake Access Point Attack Detection and Prevention System with IoT Devices
4. Vulnerability Analysis of IP Cameras Using ARP Poisoning
5. Vulnerabilities in IoT Devices for Smart Home Environment
6. Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study
1. By 2021, **35 billion IoT devices** will be installed around the world (Source: techjury)

2. The shipment volume of global Wi-Fi (Wireless Fidelity) enabled devices in 2019 reached 3.05 billion (Source: Research and markets)

<table>
<thead>
<tr>
<th>Wireless Protocols</th>
<th>Wi-Fi</th>
<th>ZigBee</th>
<th>Z-Wave</th>
<th>Bluetooth</th>
<th>6LoWPAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standardization</td>
<td>IEEE 802.11a/b/g</td>
<td>IEEE 802.15.4</td>
<td>Proprietary</td>
<td>IEEE 802.15.1</td>
<td>IETF</td>
</tr>
<tr>
<td>Frequency band</td>
<td>2.4 GHz, 5 GHz</td>
<td>868/915MHz, 2.4 GHz</td>
<td>900 MHz</td>
<td>2.4GHz</td>
<td>868MHz, 900MHz and 2.4 GHz</td>
</tr>
<tr>
<td>Range, m</td>
<td>46 m/ 92 m</td>
<td>10-100</td>
<td>30</td>
<td>1, 10, 100</td>
<td>20</td>
</tr>
<tr>
<td>Security algorithm</td>
<td>WEP, WPA, WPA2</td>
<td>AES-128</td>
<td>AES-128</td>
<td>E0, E, E21, E22, E3, 56-128 bit</td>
<td>AES-128</td>
</tr>
<tr>
<td>Topology</td>
<td>one-hop</td>
<td>star, tree, mesh</td>
<td>star, mesh</td>
<td>p2p, scatternet</td>
<td>mesh</td>
</tr>
<tr>
<td>Channel bandwidth</td>
<td>22MHz</td>
<td>0.3/0.6MHz, 2MHz</td>
<td>300kHz, 400kHz</td>
<td>1MHz</td>
<td>600kHz, 2MHz, 5MHz</td>
</tr>
</tbody>
</table>
Network security threats for IoT in the SH

1. Eavesdropping attacks
2. Denial of Service (DoS) De-authentication attacks
3. MITM (Man-In-The-Middle) attacks
Network security threats for IoT in the SH

Eavesdropping attack

1. Eavesdropping attack is an important first step to launch any type of attack on IoT device
2. To sniff the network traffic in wireless networks
3. Illegally impersonating a legal IoT device to gather information via sniffing
Denial of Service (DoS) De-authentication attacks

1. It is the pre-connection of the DoS attack
2. Device send deauthentication frame to leave the network
3. Frames are unencrypted
4. Attacker can easily spoof these frames
Network security threats for IoT in the SH

MITM(Man-In-The-Middle) attack

- MITM attack can be implemented through different ways but in the testbed, it has been implemented by using two methods,
  1) Fake Access Point (AP)
  2) by using ARP poisoning
Methodology (Smart Home testbed)
Tools and applications used

1. Kali Linux is operating on the attacking machine
2. Alfa AWUS036NHA 2.4 GHz and Alfa AWUS036ACH 2.4 & 5 GHz
3. Airodump-ng
4. Man-In-The-Middle framework (MITMf) tool
5. Using a scanning tool, such as NMAP, to know the MAC address of the target device
6. To analyses the data packets Wireshark has been used
Results (Sniffing or spoofing)

1. Collecting information in this stage is important in order to launch a further attack

2. On the target device sniffs all the traffic without a connection to an AP
Results (De-authentication attack)

1. Airodumpng with MAC address of AP is needed to be launched.

2. Shows the MAC address of the connected device to the target AP
Results (De-authentication attack)

Successful launch of de-authentication for a certain defined time period
## Results (De-authentication attack)

### Table 2. Results of De-authentication attack

<table>
<thead>
<tr>
<th>IoT Appliances</th>
<th>De-authentication Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Echo</td>
<td>Connection interrupted and unable to disable its connection from the AP.</td>
</tr>
<tr>
<td>Google Home</td>
<td></td>
</tr>
<tr>
<td>Amazon Echo Dot</td>
<td></td>
</tr>
<tr>
<td>Android Mobile (Model no.SM-G935F, SM-G930F) Nest Cam Indoor Security Camera</td>
<td>Connection interrupted and disabled it sometimes from the connected AP.</td>
</tr>
<tr>
<td>DYNAMODE DYN-630 Iphon4 Apple Raspberry pi-3 Sony Xperia Tablet</td>
<td>Connection interrupted and disabled it from the connected AP.</td>
</tr>
</tbody>
</table>
Results (Men In The Middle Attack)

- There are different ways to implement MITM attacks but in the testbed, it has been implemented by using two methods
  1) Fake Access Point
  2) By using ARP poisoning
Fake Access Point

Figure 5. Victim connected to fake AP
By using ARP poisoning

1. In Kali Linux, MITMf tool was used to perform ARP poisoning.

2. Using a scanning tool, such as NMAP, to know the MAC address of the target device.

3. To further capture and analyses the data packets, the attacker can use Wireshark.
Conclusions and future work

- This paper demonstrates that due to vulnerabilities remaining in some SH devices they are prone to attacks such as eavesdropping, DoS and MITM.
- If adequate security measures are not taken it could have serious implications for SH devices.
- It is hoped to use the testbed in the future to study how SH devices can be secured from these attacks.
The end

Thank you and any questions?