Research security of smart home devices

Realization document

Bachelor in electronics-ICT CCS

Names: Sander Van Dessel &
Joey Van Erum

Academiejaar 2019-2020

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

1 INTRODUCTION

This document includes what we did during our internship. Our main goal was doing research on the security of smart home devices and using the results of this research to create a paper. The paper included in this document while however not be the final result.

While we were doing our research we found out that there wasn't a guide that was useful for our project (some were missing commands, out-dated etc.), so we created our own guide which is also freely available on GitHub.

2 INSTALL GUIDE

First, we have the install guide for you that we used to read the data from the smart devices.

Packet sniffer install guide

Prerequisites

Requirements:

- A raspberry pi 3 or newer
- A power supply for your raspberry pi
- A MicroSD card of at least 8GB
- An Ethernet cables
- A MicroSD Adapter (Optional)

Raspberry Pi basic setup

Now that you have all your hardware, we should first start with installing Raspbian on your raspberry pi. This can easily be done by downloading Raspbian (preferably the lite version) from the official raspberry pi website:
https://www.raspberrypi.org/downloads/raspbian/
Here you can click the download link for Raspbian Buster lite. You will also need a program to "install" the OS on your MicroSD. We used balenaEtcher. You can install this program by going to:
https://www.balena.io/etcher/
and downloading + installing the program. When the program is installed and the MicroSD is attached to your computer you can "burn" the OS by opening balenaEtcher. Click Select image and select the zip you just downloaded (Raspbian buster). Select the target (Your micro-SD) and click flash. Wait a couple of minutes until the program is ready.

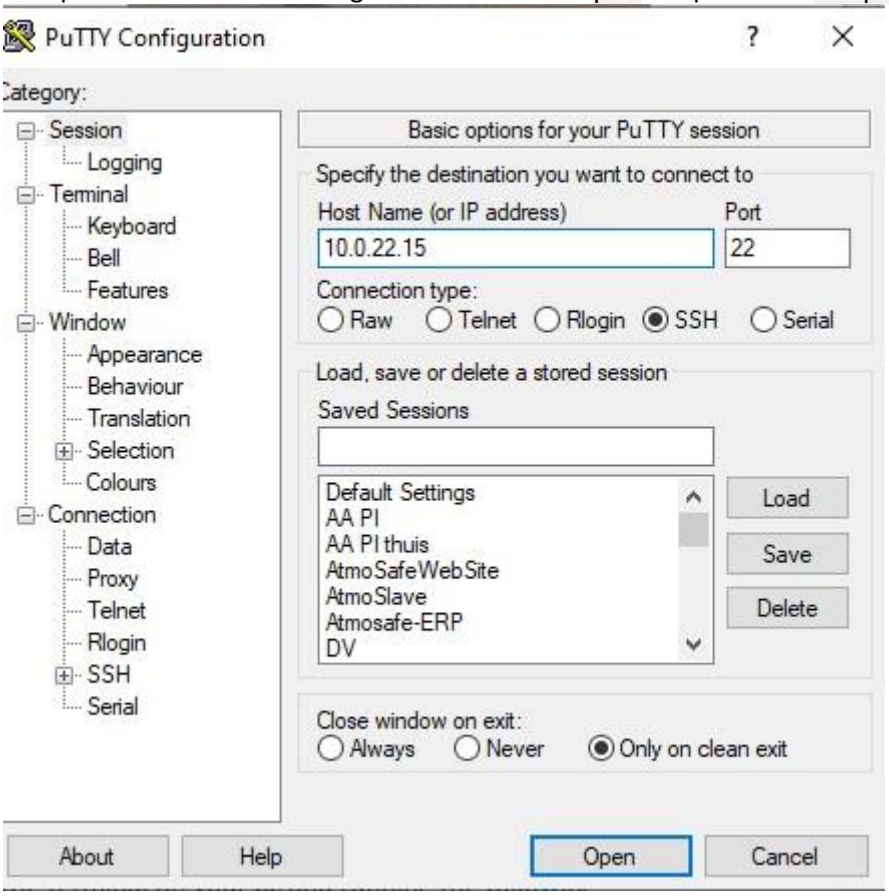
Now you will have to open your micro-SD card's home folder. Add an empty file called SSH without an extension to enable SSH on your Raspberry Pi. Eject the SSD and insert it into your Raspberry Pi. Connect the pi to its power supply and the router.

You can find your raspberry pi's IP by opening the terminal on your pc and running the following command:

```
Ping raspberrypi
```

Once you obtain the IP from your Pi you can access it remotely by using Putty. You can download this program here: https://www.putty.org/

Open Putty, enter the IP from your raspberry pi, port 22 and select SSH. A new window will open. Accept the certificates and log in with username: `pi` and password `raspberry`



Install RaspAP and hostapd

Open the terminal from your raspberry pi and run the following command:

```
sudo cp
/etc/wpa_supplicant/wpa_supplicant.conf /etc/wpa_supplicant/wpa_sup
plicant.conf.sav
sudo cp /dev/null /etc/wpa_supplicant/wpa_supplicant.conf
```

Finally, edit in the file `/etc/wpa_supplicant/wpa_supplicant.conf` and add the following lines:

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
```

The Wi-Fi interface has now been made available.
Now we will install hostapd and a user-friendly interface by using RaspAP (for more info, go to https://github.com/billz/raspap-webgui)

The installation of RaspAP can easily be done by running a single command and following the steps shown in the terminal.

```
wget -q https://git.io/voEUQ -O /tmp/raspap && bash /tmp/raspap
```

In our case there was the need for some extra configuration before the network became available. If it is already available, you can skip the following steps:

Open the following file:

```
sudo nano /etc/hostapd/hostapd.conf
```

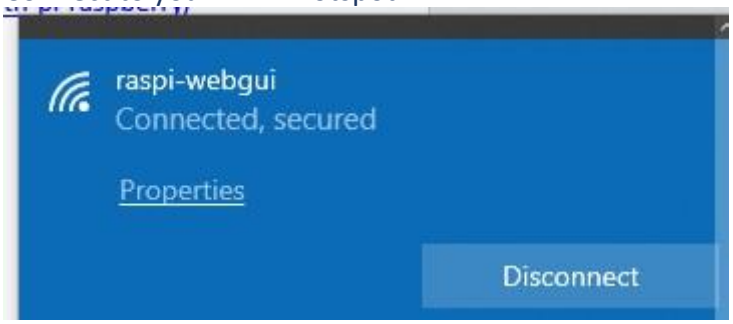
And add the following line:
```
logger_syslog=-1
```

Run the following command
sudo cat /var/log/syslog | grep hostapd

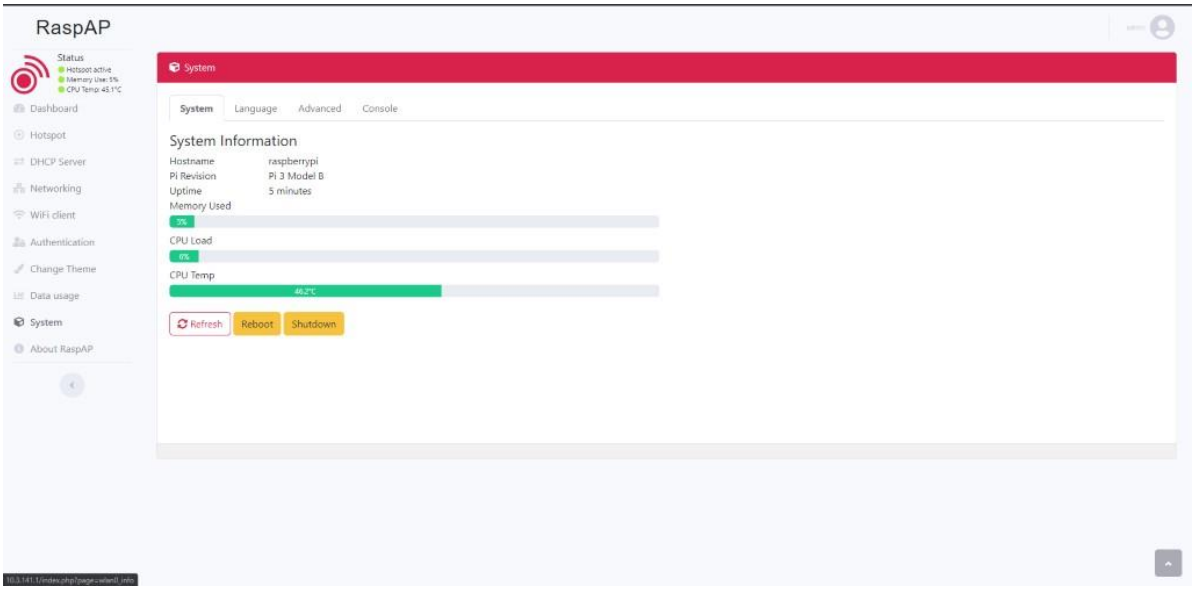
And:
```
sudo systemctl unmask hostapd
sudo systemctl enable hostapd
sudo systemctl start hostapd
```

restart your raspberry pi with the `sudo reboot`command.

Connect to your Wi-Fi hotspot



Now a network called “raspi-webgui” should be available. When you connect to this Wi-Fi-network on your pc, you can access the interface by browsing to `10.3.141.1`. (The default Wi-Fi password is `ChangeMe`). The default username and password for the interface are:
Username: `admin`
Password: `secret`



The console can also be accessed by browsing to your Raspberry Pi’s IP-address obtained in the first step (while connected to the same router).

Installing TCPDump

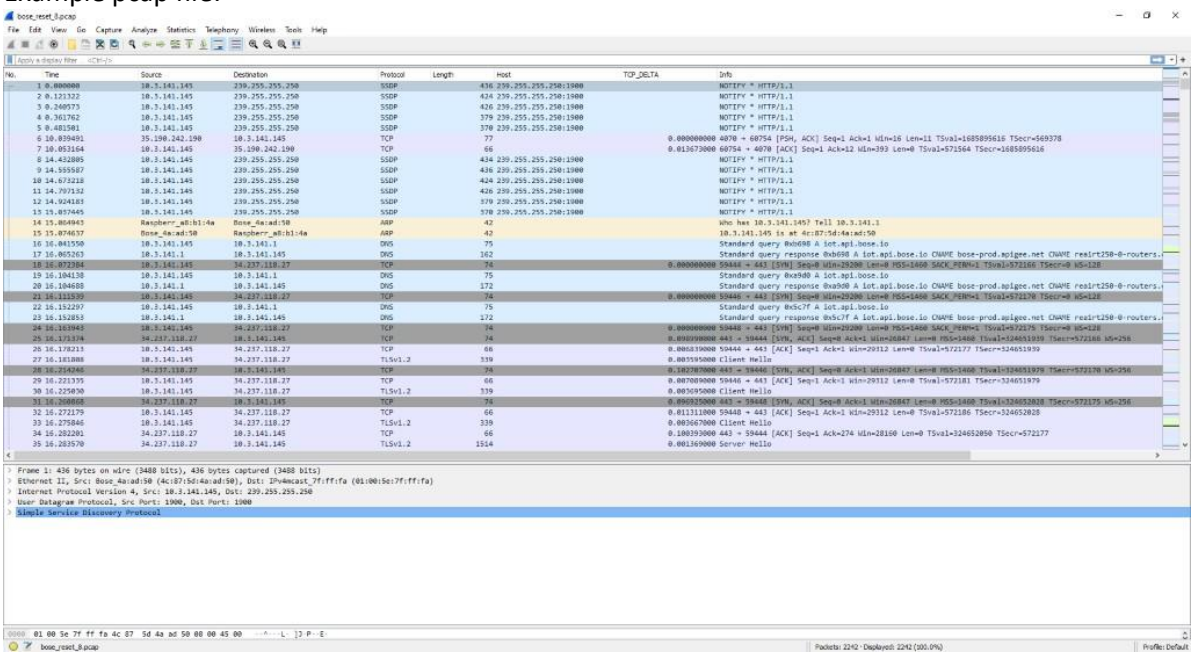
The last step to creating a packet sniffer is installing TCPDump. This tool is installed with the following command:

```
Sudo apt-get install tcpdump
```

When the installation finishes you can start to capture traffic from every device connected to the network of your raspberry pi. We recommend capturing data by specifying your host and creating a pcap fie which later can be analyzed with Wireshark.
Example:

```
sudo tcpdump host 10.3.141.145 -i wlan0 -w test
```

This command captures all network packet going from and to the device 10.3.141.145 and creates a file called test.
Example pcap file:



This guide is also available at : https://github.com/SanderVanDessel/Raspberry-Pi-Packet-sniffer
Sources:
https://howtoraspberrypi.com/create-a-wi-fi-hotspot-in-less-than-10-minutes-with-pi-raspberry/

https://danielmiessler.com/study/tcpdump/

3 PAPER

Investigating consumer smart home vulnerability

Torben Svane
Halmstad University
School of Information Technology
Halmstad, Sweden
00 46 705 13 61 40
Torben.svane@hh.se

Sander Van Dessel
Thomas More University
of Applied Sciences
Department of Data Science,
Protection & Security
Geel, Belgium

Joey Van Erum
Thomas More University
of Applied Sciences
Department of Data Science,
Protection & Security
Geel, Belgium

ABSTRACT

This paper examines vulnerabilities in various common smart home devices, specifically risks and security challenges they may entail for the consumer. Investigations have focused on exploring if earlier reported risks still exist in the current (2019 - 2020) versions of hardware. Although many of earlier reported risk seem fixed in later device updates, there are however still potential risks present in some of the tested devices.

CCS Concepts

• Human-centered computing → Ubiquitous and mobile computing → Ubiquitous and mobile devices. • Security and privacy → Security in hardware.

Keywords

Data security; safety features; smart home devices, Belgium.

1. INTRODUCTION

Smart home devices seem to become increasingly popular, with sales growing from USD 55B (2016) to 174B in 2025 [1]. Today, household devices range from e.g. smart fridges to home assistants and house locks [2]. Major brands such as Amazon and Google are also broadening their product range to include devices such as smart speakers that respond to voice commands [3].

There are however expressed many concerns about the high rate of "smartification" [4]. It has been said (although not verified) that "everything connected to the Internet can probably be hacked" [5]. Because of the wide range of settings and control methods that can deployed, risks such as identity theft and ransomware increase [6].

Smart home technologies came on market in the early 2000s [7]. Since then, the range of devices and volume of sales has grown rapidly. Global smart home market statistics and forecasts vary, but most report at least 100% growth 2016 to 2022 [8]; the US speaker market has grown from 7% (2017) to 31% (2019) [ibid.].

CSW'2021, August 13–15, 2021, Stockholm, Sweden.

DOI: http://dx.doi.org/10.1145/12345.67890

Smart home technology is also known as Home automation [9] and denotes the use of devices that are connected to a network (most often, a local network and the Internet). The devices use sensors and other appliances connected to IoT and can be remotely configured, monitored and accessed. They can also provide services according to the needs of the users. With smart home devices users are able to control and monitor their devices from apps on their smartphones even when not home. Through such services, a user may e.g. adjust the home thermostat so that a home will be warm and perhaps with music playing upon your arrival. Smart home technology has also been reported beneficial for people with special needs, as it helps them with accommodating [10-11].

Some of the more common smart home devices are [12]:

1. Indoor and outdoor security cameras
2. Doorbells
3. Lights
4. Locks
5. Thermostats
6. Speakers
7. Smoke and Carbon Monoxide detectors
8. Smart irrigation systems

In the reported study, speakers and a light bulb have been evaluated, together with media streaming units and a router. The latter device will probably not (in itself) be considered a smart device but is central in the communication with all the others.

2. LITERATURE REVIEW

Testing network security is not new [see 13-14 for overviews]. In later years, many studies have focused on smart homes in specific, as a novel, hence vulnerable, area of application [15-16].

As stated in [14], "Billions of IoT devices are expected to populate our environments and provide novel pervasive services by interconnecting the physical and digital world." The increased connectivity of all such everyday objects may, besides offering new smart services in homes, also open for criminal, malicious attacks, or for information collection about the user (without consent) [17]. These threats are even further augmented by the resource constraints and heterogeneity of low-cost IoT devices, which make current host-based and static perimeter-oriented defense mechanisms unsuitable for dynamic IoT environments. [14]

The general availability of free Internet tools for intrusion detection (but also exploration of networks and devices) has long been seen as a risk [18]. Reports on smart home threats and vulnerability are found in thousands. A database search (May 27, 2020) on the key-phrase "security risks smart home", filtered for peer-review, articles and journals, and from 2015 and onwards generated more than 3,000 hits.

There are several articles/studies published on types of devices examined in this study, e.g. on speakers [19], TVs [20], and voice-controlled devices such as Google Assistant and Amazon Alexa [21]. Many more will no doubt be published in the years to come. If one thing is obvious from the literature review, it will be that there are many more challenges to meet, and many more studies needed to explore and exploit vulnerability in what many end users consider being "safe" devices [22].

3. TOOLS AND DEVICES

3.1 Software packages

A range of publicly available packages have been used, to mimic earlier reported work. Tests have been run on traditional computers (Windows, Linux) as well as on e.g. a Raspberry Pi setup. Many of the packages used in this study are described in length in [23].

3.1.1 TCPDump

This tool will detect packages from a certain device or adapter [24]. It was installed on a Raspberry Pi unit and used for "man in the middle" [25] attacks which allowed monitoring of data sent from the smart device being tested. For more on this tool, see [26-27].

3.1.2 Wireshark

Wireshark [28] is a tool for analyzing data packets. Different from TCPDump, this is a GUI tool that allows for isolating streams such as an entire conversation during a TCP session. Several reports discuss this tool in greater detail, e.g. [29-30].

3.1.3 Routersploit

Routersploit [31] is a tool that searches for exploits (modules that take advantage of identified vulnerabilities) for embedded devices. For more details on this tool, see [23, 32].

3.1.4 Sparta

This is a python GUI application [33] (rather than a separate tool) that makes it easier to see where there are weaknesses in a network. For example, several stages from Nmap (used to discover open ports on hosts) [34] will display potential connections.

3.1.5 Miranda

Miranda [35] is used to find devices that use UPnP and extract information from packages sent with UPnP. For other work, see [36].

3.2 Devices

Security concerns were tested in different smart home devices. The aim was to investigate a smaller selection of fairly common devices, rather than aiming at a broader set of available products.

3.2.1 Bose 300 Home Speaker

This device is manufactured by Bose Corporation [37]. The product was launched summer of 2019 and has Google Assistant [38] and Alexa [39] built in. The Bose 300 can be connected to a home network using Wi-Fi, which enables usage of Google Assistant, Alexa, Apple Airplay 2 [40] and a mobile app called Bose Music to control it. Controls include e.g. an equalizer, assigning presents to the 6 buttons on top, managing which device that may connect via Bluetooth and enabling integrated music services (e.g. Spotify, Deezer, Amazon music, etc.). The speaker also has a touch button on top that can be used to turn off the microphone. This is however a touch button - and not a physical switch.

There are four ways to play audio on the speaker: using the aux port, connect via Bluetooth or Wi-Fi, and use voice commands.

3.2.2 Google Home Speaker

The Google Home speaker is part of a more extensive system developed by Google [41]. The unit uses voice commands to interact with Google Assistant services. The product was introduced to the consumer market in November 2016, followed by more Google Home products that were released in 2017-2019 [42]. The user must install the Google Home app to configure the device.

3.2.3 TP-Link Archer C50

The Archer C50 is a Wi-Fi Router from TP-Link [43] and became available on the market in the autumn of 2017. It allows for a total of 1200 Mbps available bandwidth and supports guest network access. The guest network can also be used by signing up through Facebook. The device can be controlled using a mobile app called TP-Link Tether. This app allows network management, and includes: Filters, applying updates, listing all connected devices, sharing a Wi-Fi, setup of SSID and password for the device, etc. The device also allows for a web UI to manage similar (in some cases, extended) settings.

3.2.4 Nvidia Shield

This device (from Nvidia, [44]) connects to your TV and enables the user to stream e.g. shows, movies, and games.

3.2.5 Google Chromecast

A Google Chromecast unit connects to a TV via HDMI and gives access to multiple streaming services, e.g. Netflix and YouTube. It is controlled through the Google Home app [45].

3.2.6 LIFX Light Bulb

The range of home devices has been expanded in recent years. Among new appliances with connectivity are home lighting. The LIFX light bulb [46] is a smart bulb which has the possibility to change color using an app or by integration with a system such as Google Home. Security lighting issues also covers smart cities [47].

3.2.7 Samsung Smart TV (2015 and 2019)

The last devices tested were Samsung [48] smart TVs: a 32-inch unit (UE32) from 2015 and a Samsung Q9 (55-inch) from 2019.

The devices used in this study allows for some pairing comparisons (speakers, streaming devices, different manufacturing years

for TVs). The remaining two represents a common component in any smart home (router) and a fairly new addition (light bulb) that may seem to be a "simple" device but is connected, and can hence be used as an entry point to network explorations.

4. RESULTS FROM TESTING

The next section will present results from the tests. First will be a list of open ports and comments to their use (and potential risk). This will be followed by examples of data that can be detected.

4.1 Bose 300 Home Speaker

The Bose speaker was found to have passable security with three open ports. User data could also be collected (but not passwords.)

4.1.1 Open Ports

The box had two open ports: http and zeroconf. It was also found that ftp, rtsp and realserver ports sometimes were open (but regularly switched from open to filtered).

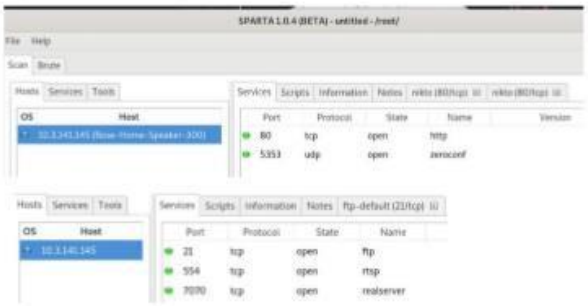


Figure 1. Detecting open ports (Bose 3000 Home Speaker).

4.1.2 Data Packages

The unit also sends numerous packages trough the network, such as connectivity checks every 5 minutes, and extensive information about songs played on Spotify, Deezer and radio.

bf
{"errors":null,"duration":
0,"countryCode":"BE","isAllowed":false,"ipAddress"
:"157.52.108.83","zipCode":"2390","city":"Malle","s
tate":"0","latitude":51.299,"longitude":
4.711,"firstError":null}

Figure 2. Displaying user data (Bose 3000 Home Speaker).

{"batch_result":[{"id":
700694201,"name":"nardinel","lastname":"","firstname":"","email":"[redacted]@gma
il.com","status":
0,"birthday":"0000-00-00","inscription_date":"2015-05-04","gender":"","link":"http:\/\/
www.deezer.com\/profile\/700694201","picture":"http:\/\/api.deezer.com\/user\/
700694201\/image","picture_small":"http:\/\/cdn-images.deezer.com\/images\/user\/
56x56-000000-80-0-0.jpg","picture_medium":"http:\/\/cdn-images.deezer.com\/images\/
user\/250x250-000000-80-0-0.jpg","picture_big":"http:\/\/cdn-images.deezer.com\/
images\/user\/500x500-000000-80-0-0.jpg","picture_xl":"http:\/\/cdn-
images.deezer.com\/images\/user\/
1000x1000-000000-80-0-0.jpg","country":"US","lang":"EN","is_kid":false,"explicit_content_l
evel":"explicit_display","explicit_content_levels_available":
["explicit_display","explicit_no_recommendation","explicit_hide"],"tracklist":"http:\/\/
api.deezer.com\/user\/700694201\/

Figure 3. Displaying user data (Bose 3000 Home Speaker).

4.2 Google Home Speaker

Testing a different brand speaker made way for comparisons. The Google unit seemed to be a well secured device. Apart from music service (provider) information and data about which current music piece was being played, no further data sharing was detected.

4.2.1 Open Ports

Some ports were detected open, but only ones needed for device functionality. When trying to connect to these ports all attempts were immediately terminated.

Figure 4. Detecting open ports (Google Home Speaker).

4.2.2 Data Packages

The testing was unable to detect and interpret personal data packages from the Google Home device, apart from music player type and music currently listened to. The other packages seemed highly secured (encrypted).

'=1#rs=Casting: Homicide (feat. Eminem).=.!.....x.-.....
8ce495a5a6735f34bd2dbd808#cd=564251B78DC79E1
'=1#rs=Casting: Homicide (feat. Eminem)...!.....x.-.....I
5C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.
368ce495a5a6735f34bd2dbd808#cd=564251B78DC79I

Figure 5. Displaying user data (Google Home Speaker).

4.3 TP-Link Archer C50

Most home configurations will include a router hence it seemed to be a logical device type to include in the testing.

4.3.1 Open Ports

Upon router reset, a port scan was performed to detect all ports set open by default. Four ports were found open. Most important was the SSH port. There are many reports on breaches committed through such ports (e.g. brute force attacks) because if breached it allows for almost full control of the device [49-50].

Figure 6. Open ports (TP-Link Archer C50 Router)

4.3.2 *Exploits*

An Internet search for exploits (and listing of tools) was also performed. The acquired information was tested on the device. Some of the Internet information was found not valid anymore.

4.3.2.1 *Default Credentials*

After reset, the default credentials could be accessed with the tool Routersploit. This operation enabled full control of the router's GUI, and possibilities to adjust any of the initial settings.

```
rsf (AutoPwn) > back
rsf > search tplink
creds/routers/[illegible]/ssh_default_creds
creds/routers/[illegible]/telnet_default_creds
creds/routers/[illegible]/ftp_default_creds
exploits/routers/[illegible]/archer_c2_c20i_rce
exploits/routers/[illegible]/wdr842nd_wdr842n_configure_disclosure
exploits/routers/[illegible]/wdr740nd_wdr740n_backdoor
exploits/routers/[illegible]/wdr740nd_wdr740n_path_traversal
rsf > use creds/routers/tplink/ssh_default_creds
rsf (TP-Link Router Default SSH Creds) > set threads 10
[+] threads => 10
rsf (TP-Link Router Default SSH Creds) > target 192.168.1.1
[-] Unknown command: 'target'
rsf (TP-Link Router Default SSH Creds) > set target 192.168.1.1
[+] target => 192.168.1.1
rsf (TP-Link Router Default SSH Creds) > run
[*] Running module creds/routers/tplink/ssh_default_creds...
[*] Starting default credentials attack against SSH service
[*] Elapsed time: 2.1580 seconds
[+] Credentials found!

   Target          Port     Service     Username     Password
   ------          ----     -------     --------     --------
   192.168.1.1     22       ssh         admin        admin

rsf (TP-Link Router Default SSH Creds) >
```

Figure 7. Using exploits for access (TP-Link Archer C50).

Enabling a physical reset may be difficult without direct access to the router but the tests showed that access to configuration and the GUI was possible through freely available tools.

Figure 8. GUI access (TP-Link Archer C50).

4.3.2.2 *Denial Of Service*

Among exploits found through the Internet search was one that suggested a possible use of Denial of Service (DoS). Attempts to invoke this method were however unsuccessful, indicating that the manufacturer has fixed this potential security breach since it was made publicly known.

```
root@kali:~/Desktop# python3 exploit_tplinkarcher_c50.py
[+] IP   : 192.168.1.1
[+] Port : 80
[+] Initializing Socket...
[!] Connecting to target...
[!] Sending Request...
[!] Disconnecting Socket...
[+] Initializing Socket...
[!] Connecting to target...
[!] Sending Request...
[!] Disconnecting Socket...
[-] Exploit Failed!
```

Figure 9. Attempting DoS exploit (TP-Link Archer C50).

4.4 NVidia Shield

The next two devices tested are both used for media connectivity. The unit is connected to a TV set and once operational, it allows the user to stream different media services, e.g. Netflix, YouTube, or gaming.

The NVidia Shield was found to have the tightest security of all devices tested. The device exploration did not reveal any personal information. The only data that was detected remotely accessible were pictures of the Netflix series thumbnails.

4.4.1 *Open Ports*

The unit had 3 open (but secured) ports: http, ajp13 and https-alt.

Port	Protocol	State	Name
8008	tcp	open	http
8009	tcp	open	ajp13
8443	tcp	open	https-alt

Figure 10. Open ports (NVidia Shield).

4.4.2 *Data Packages*

Much of the data this device sends is encrypted, but thumbnails loaded by Netflix were readable (which may be seen as a type of personal information). Testing the shield also revealed that connectivity checks were performed every minute.

Figure 11. Netflix thumbnails (NVidia Shield).

4.5 Google Chromecast

The Chromecast, part of Googles Home range of devices has been available on the market since 2013 [45]. With total sales exceeding 55 million (2017) [51], it is a very common device in many homes.

4.5.1 *Open Ports*

Five ports were detected open but secured – all attempts to access them in this study failed. Three were the same as for the NVidia shield (http, ajp13, and https-alt), and two more were cslistener and scp-config.

Figure 12. Open ports (Google Chromecast).

4.5.2 *Data Packages*

During uptime, data seems well secured (no access was found) but a performing a device reset revealed information about the system itself and the network to which it was connected.

With access to such data, there are possibilities to find vital device values, e.g. MAC and IP addresses. Accessing uptime data of the device may also reveal when the user is home or not.

Figure 13. Data access (Google Chromecast).

4.6 LIFX Light Bulb

A light bulb may be seen as a "simple" and "harmful" device compared to the others tested. It has limited functionality – but being part of the network, it may be used as an entry point for other exploration. Studies of smart bulbs (different brands, [52-53]) have revealed a security flaw in the ZigBee [54] protocol. This exploit was however not relevant in tests of this device, as the ZigBee protocol was not used.

4.6.1 Open Ports

Only two ports were found open: http and zeroconf (both secured).

Port	Protocol	State	Name
80	tcp	open	http
5353	udp	open	zeroconf

Figure 14. Open ports (LIFX light bulb).

4.6.2 Data Packages

There were packages send by the device but none of them seemed to contain (for the tests) usable information. The bulb connects to 104.198.46.246 (the LIFX server) using TLSv1.2 and secure TCP.

4.7 Samsung Smart TVs (2015 and 2019)

The set of testing devices also made possible a comparison between two devices from the same manufacturer, but with different release years. This allowed a review whether security had been updated.

Initially, a scan for open ports was performed. Both devices had several ports open. Most notably was UPnP. Using Miranda, information sent with the UPnP service was found. Exploits were also attempted but did not work well as most require physical contact with the device before continuing to work remotely (and all tests in this paper's design were done through networks).

4.7.1 Open Ports

The 2015 unit had 5 open ports. Most interesting was the UPnP port, which has been reported for security breaches [55].

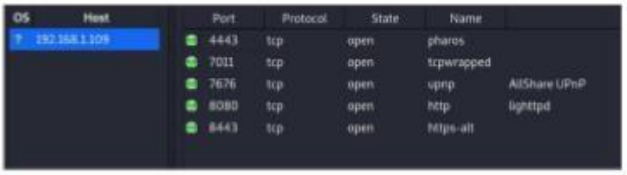


Figure 15. Open ports (Samsung Smart TV 2015).

4.7.2 Data Packages

A data search was done using the Miranda tool on the UPnP ports.

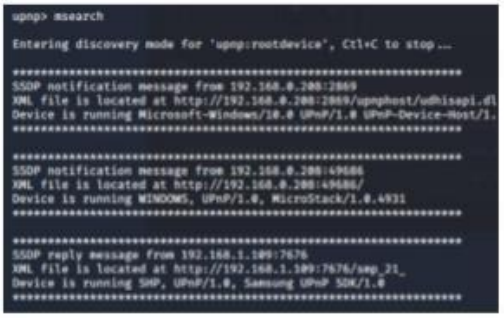


Figure 16. Miranda Search (Samsung Smart TV 2015).

The search enables a user to see which device(s) that will be using UPnP and list them. This means (from a security point of view) that with any device using UPnP, XML files will be readable (as seen in figure 18) and potentially reveal privacy-oriented data.

Figure 17. Miranda information (Samsung Smart TV 2015).

Miranda testing also revealed XML packages. Data included e.g. device type, serial/model number and manufacturer.

Figure 18. XML-file (Samsung Smart TV 2015).

Inspecting the Pcap files indicated that handling of information was not completely secure. The user's search history could simply be found in plain text between the data packets. Figure 19 shows a search for YouTube with the TV's default browser.

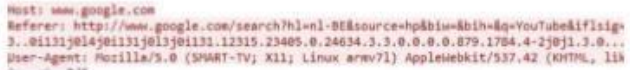
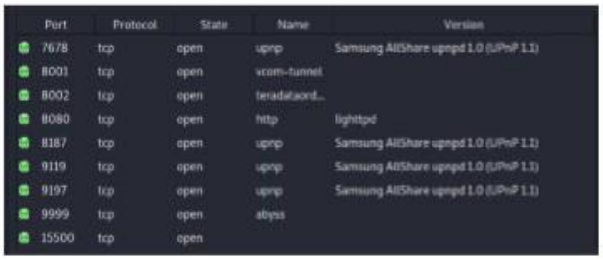


Figure 19. Browser search (Samsung Smart TV 2015).

The 2015 unit was then compared with a more contemporary (2019) device to see if security had improved in later models.

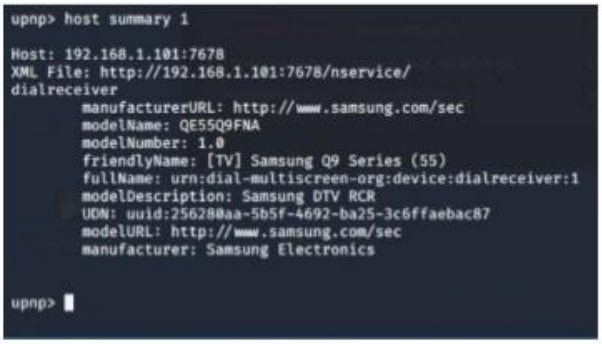
4.7.3 Open Ports (Samsung Smart TV 2019)

The newer unit had more ports open, possibly due to new services from Samsung; an arrangement that may compromise security. Further Miranda testing also detected more UPnP ports than 2015.



Port	Protocol	State	Name	Version
7678	tcp	open	upnp	Samsung AllShare upnpd 1.0 (UPnP 1.1)
8001	tcp	open	vcom-tunnel	
8002	tcp	open	teradataord...	
8080	tcp	open	http	lighttpd
8187	tcp	open	upnp	Samsung AllShare upnpd 1.0 (UPnP 1.1)
9119	tcp	open	upnp	Samsung AllShare upnpd 1.0 (UPnP 1.1)
9197	tcp	open	upnp	Samsung AllShare upnpd 1.0 (UPnP 1.1)
9999	tcp	open	abyss	
15500	tcp	open		

Figure 21. Open ports (Samsung Smart TV 2019).



```
upnp> host summary 1

Host: 192.168.1.101:7678
XML File: http://192.168.1.101:7678/nservice/
dialreceiver
        manufacturerURL: http://www.samsung.com/sec
        modelName: QE55Q9FNA
        modelNumber: 1.0
        friendlyName: [TV] Samsung Q9 Series (55)
        fullName: urn:dial-multiscreen-org:device:dialreceiver:1
        modelDescription: Samsung DTV RCR
        UDN: uuid:256280aa-5b5f-4692-ba25-3c6ffaebac87
        modelURL: http://www.samsung.com/sec
        manufacturer: Samsung Electronics


upnp>
```

Figure 22. UPnP information (Samsung Smart TV 2019).

4.7.4 Data Packages (Samsung Smart TV 2019)

Accessing the UPnP ports revealed an XML file with data such as serial number and MAC-addresses. Figure 23 shows the addresses from each port on the device and the listen frequency. Figure 24 shows data in the XML file for the 2019 unit (as figure 18 does for the 2015 unit).

Figure 23. XML network data (Samsung Smart TV 2019).

```
- <device>
    <deviceType>urn:dial-multiscreen-org:device:dialreceiver:1</deviceType>
    <friendlyName>[TV] Samsung Q9 Series (55)</friendlyName>
    <manufacturer>Samsung Electronics</manufacturer>
    <manufacturerURL>http://www.samsung.com/sec</manufacturerURL>
    <modelDescription>Samsung DTV RCR</modelDescription>
    <modelName>QE55Q9FNA</modelName>
    <modelNumber>1.0</modelNumber>
    <modelURL>http://www.samsung.com/sec</modelURL>
    <serialNumber>20090804RCR</serialNumber>
    <UDN>uuid:256280aa-5b5f-4692-ba25-3c6ffaebac87</UDN>
    <sec:deviceID>NSNSC5ZTTO2RS</sec:deviceID>
    <sec:ProductCap>Resolution:1920X1080,Tizen,Y2017</sec:ProductCap>
  - <serviceList>
```

Figure 24. XML information (Samsung Smart TV 2019).

From looking at the tested user's search history, it may be concluded that the manufacturer has not optimized this access yet, even as information about this is easy to get (e.g. on Internet [56]).

```
Host: www.google.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (SMART-TV; Linux; Tizen 4.0) AppleWebKit/537.36 (KHTML,
Accept: image/webp,image/*,*/*;q=0.8
Referer: http://www.google.com/search?q=dogfood&aq=f&aqi=g70&aql=&oq=&gs_rfai=

GET / HTTP/1.1
Host: www.wikipedia.org
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (SMART-
Accept: text/html,application/x
Accept-Encoding: gzip, deflate
Accept-Language: nl-NL
```

Figure 25. Old user search data (Samsung Smart TV 2019).

4.8 Reviewing Tests

The tests run in this study are fairly simple and may not be able to fully penetrate the devices. The aim was to use only simple tools that are readily available, and test commonly used smart home devices. Because of the situation at time of the study (the Covid-19 pandemic) lockdowns forced experiments to be carried out in a home environment, and on available devices - rather than in an advanced, fully equipped forensic laboratory and on more devices.

5. DISCUSSION

From the tests, it would seem as some devices have improved over the years with respect to security – but not all. Some of the earlier security flaws have however been corrected. A reason for doing so may be that neglecting security could be costly if exploited, and consumers may distrust the brand's products. Many reports echo concern in this regard ([57-59].

6. CONCLUSIONS

Even though there is still a potential for improvements (e.g. in the Samsung smart TVs and the router), there are also results that indicate a higher level of security today in the tested devices.

REFERENCES

All internet URL references were checked May 27, 2020.

[1] Marr, B. 2020. The 5 biggest smart home trends in 2020. *Forbes*, Jan. 13, 2020. Article available at https://www.forbes.com/sites/bernardmarr/2020/01/13/the-5-biggest-smart-home-trends-in-2020/#6d1e4999389b.

[2] Blythe, J. M., Johnson, S. D., and Manning, M. 2020. What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science* 9 (1), 2020. DOI= https://doi.org/10.1186/s40163-019-0110-3.

[3] Kozuch, K. 2020. The best Google Home compatible devices in 2020. Available at https://www.tomsguide.com/best-picks/google-home-compatible-devices.

[4] Bello, O., and Zeadally, S. 2019. Toward efficient smartification of the Internet of Things (IoT) services. *Future Generation Computer Systems* (92), March 2019, pp. 663-673. DOI= https://doi.org/10.1016/j.future.2017.09.083.

[5] Thurn, T. 2018. Net neutrality and data security - What do they mean for property management? *Journal of Property Management*, Sep/Oct 2018, 83 (5), pp.34-35.

[6] Jacobsson, A., Boldt, M., and Carlsson, B. 2016. A risk analysis of a smart home automation system. *Future Genera-*

tion Computer Systems (56), March 2016, pp. 719-733. DOI= https://doi.org/10.1016/j.future.2015.09.003.

[7] Aldrich F.K. 2003. Smart Homes: Past, Present and Future. In Harper R. (eds) *Inside the Smart Home*. Springer, London. DOI= https://doi.org/10.1007/1-85233-854-7_2.

[8] Statista Research, 2020. Forecast market size of the global smart home market from 2016 to 2022 (in B USD). Feb. 19, 2020. https://www.statista.com/statistics/682204/global-smart-home-market-size/.

[9] Khedekar, D.C., et al. 2016.Home automation – a fast-expanding market. *Thunderbird Intl Bus Rev*, June 6, 2016. DOI= https://doi-org/10.1002/tie.21829.

[10] Augusti, J., et al. 2018. The user-centred intelligent environments development process as a guide to co-create smart technology for people with special needs. *Universal Access in the Information Society* 17 (2018), pp. 115–130. DOI= https://doi.org/10.1007/s10209-016-0514-8.

[11] Quynh, L., Nguyen, H., and Barnett, T. 2012. Smart homes for older people: Positive aging in a digital world. *Future Internet* 4 (2), 2012, pp. 607-617. DOI= https://doi.org/10.3390/fi4020607.

[12] Lee, B, et al. 2017. Companionship with smart home devices: The impact of social connectedness and interaction types on perceived social support and companionship in smart homes. *Computers in Human Behavior* 75, Oct 2017, pp. 922-934. DOI= https://doi.org/10.1016/j.chb.2017.06.031.

[13] Wei, M., and Kim. K. 2016. An automatic test platform to verify the security functions for secure WIA-PA wireless sensor networks. International Journal of Distributed Sensor Networks 12 (11), 2016. DOI= https://doi.org/10.1177/1550147716676094.

[14] Molina Zarca, A., et al. 2018. Enhancing IoT security through network softwarization and virtual security appliances. *International Journal of Network Management* special issue 2018. DOI= https://doi-org/10.1002/nem.2038.

[15] Shahidi, H. 2019. Comparing security features of Zigbee and Z-Wave communications protocols in IoT devices. Master's Thesis, Halmstad University, Sweden.

[16] van Leeuwen, D., and Ayuk, L. T. 2019. Security testing of the Zigbee communication protocol in consumer grade IoT devices. Master's Thesis, Halmstad University, Sweden.

[17] Goh, L. S., and Nathan-Roberts, D. 2019. Smart home devices: promoting user trust and protecting user data. *Proc of the Human Factors and Ergonomics Soc annual meeting* 63 (1), 2019. DOI= https://doi-org /10.1177/1071181319631525.

[18] Adeynka, O. 2008. Second Asia International Conference on Modelling & Simulation (AMS), Kuala Lumpur, Malaysia, May 2008. DOI= https://doi-org/10.1109/AMS.2008.68.

[19] Hart, L. 2018. Smart speakers raise privacy and security concerns. *Journal of Accountancy* 225 (6).

[20] Bachy, Y., et al. 2019. Smart-TV security: risk analysis and experiments on Smart-TV communication channels. *Journal of Computer Virology and Hacking Techniques* 15, 2019. DOI= https://doi-org/10.1007/s11416-018-0320-3.

[21] Zhang, N., et al. 2019. Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. 2019 IEEE Symposium on Security and Privacy (SP), Sep 2019, San Francisco, CA, USA. DOI= https://doi-org/10.1109/SP.2019.00016.

[22] Wang, X.; McGill, T.J.; and Klobas, J.E. 2018. I want it anyway: consumer perceptions of smart home devices. *Journal of Computer Information Systems*, 2018. DOI= https://doi.org/10.1080/08874417.2018.1528486.

[23] Tseng, T. W., Wu, C. T., and Lai; F. 2019. Threat analysis for wearable health devices and environment monitoring IoT integration system. IEEE Access (7), Oct 2019. DOI= https://doi-org/10.1109/ACCESS.2019.2946081.

[24] Tool is available at https://www.tcpdump.org/.

[25] Agarwal, M.; Biswas, S.; and Nandi, S. 2015. Advanced stealth man-in-the-middle attack in WPA2 encrypted Wi-Fi networks. *IEEE Communications Letters* 19 (4) , April 2015. DOI= https://doi-org/10.1109/LCOMM.2015.2400443.

[26] Weigle, E., and Feng, W-F. 2020. TICKETing high-speed traffic with commodity hardware and software. PAM2002, Fort Collins, Colorado, March 20, 2002.

[27] Nielson, S. J. 2016. PLAYGROUND: preparing students for the cyber battleground. *Computer Science Edu*, 26 (4), 2016. DOI= https://doi-org/10.1080/08993408.2016.1271526X.

[28] Tool is available at https://www.wireshark.org/.

[29] Heo, G., Park, Y. J., and Park, W. H. 2015. Vulnerability of information disclosure in data transfer section for constructing a safe smart work infrastructure. *Multimedia Tools and Applications* 74 (20), Oct 2015, pp. 8831-8847. DOI= https://doi-org 10.1007/s11042-013-1627-1.

[30] Siboni, S., et al. 2016. Advanced security testbed framework for wearable IoT devices. *ACM Trans on Internet Technology*, Dec 2016. DOI= https://doi-org /10.1145/2981546

[31] See https://tools.kali.org/exploitation-tools/routersploit.

[32] Adamczyk, B. 2018 Security considerations of modern embedded devices and networking equipment. In Gaj, P., Sawicki, M., Suchacka, G., and Kwiecień, A. (eds) Computer Networks. 2018. Comm in Computer and Information Sci. DOI= https://doi.org/10.1007/978-3-319-92459-5_30.

[33] For more on the SPARTA Python GUI, see https://tools.kali.org/information-gathering/sparta.

[34] SPARTA git clone: https://github.com/secforce/sparta.git.

[35] Balyalakshmi, B., et al. 2018. Network vulnerability analysis on brain signal/image databases ssing Nmap and Wireshark tools. IEEE Access (6), Oct 2018. DOI= https://doi.org/10.1109/ACCESS.2018.2872775.

[36] More information about MIRANDA is available at https://tools.kali.org/information-gathering/miranda.

[37] Bose homepage: https://www.bose.com/en_us/index.html.

[38] For an overview, see https://assistant.google.com/.

[39] Alexa and other Amazon smart home devices are presented at https://www.amazon.com/smart-home-devices/.

[40] Apple Airplay page: https://www.apple.com/airplay/.

[41] See https://assistant.google.com/platforms/speakers/.

[42] An overview (not academic, but with numerous references) is https://en.wikipedia.org/wiki/Google_Nest_(smart_speakers).

[43] The TP-Link page for this device is https://www.tp-link.com/se/home-networking/wifi-router/archer-c50/.

[44] Nvidia page: https://www.nvidia.com/en-us/shield/.

[45] There are several versions. More information is found at https://store.google.com/search?q=chromecast.

[46] Company homepage is https://www.lifx.com/.

[47] Lacinak, M., and Ristvej, J. 2017. Smart city, safety and security. *Procedia Engineering* (192), 2017, pp. 522-527. DOI= https://doi.org/10.1016/j.proeng.2017.06.090.

[48] Models are now "old" and not presented on the Samsung page (search needed) https://www.samsung.com/.

[49] Staiwan, D., et al. 2019. Investigating Brute Force attack patterns in IoT network. *Journal of Electrical and Computer Engineering*. DOI= https://doi.org/10.1155/2019/4568368.

[50] Wang, D. et al. 2018. Resetting your password is vulnerable: A security study of common SMS-based authentication in IoT device. *Wireless communications and mobile computing*. 2018. DOI= https://doi.org/10.1155/2018/7849065.

[51] Collins, T. Google has sold 55 million Chromecast devices. CNet blog: https://www.cnet.com/news/google-has-sold-55-million-chromecast-and-chromecast-built-in-devices/.

[52] Morgner, P., Mattejat, S., and Benenson, M. 2017. All your bulbs are belonging to us: Investigating the current state of security in connected lighting systems. https://arxiv.org/abs/1608.03732.

[53] Notra, S. et al. 2014. An experimental study of security and privacy risks with emerging household appliances. *IEEE Conference on Communications and Network Security*, Oct 2014. DOI= https://doi.org/10.1109/CNS.2014.6997469.

[54] Zigbee alliance homepage: https://zigbeealliance.org/.

[55] Esnaashari, S., Welch, I., and Komisarczuk, P. 2013. Determining home users' vulnerability to universal plug and play (UPnP) attacks. *IEEE 27th International Conference on advanced information networking and applications workshops*, Barcelona. DOI= https://doi.org/10.1109/WAINA.2013.225.

[56] https://internetofbusiness.com/samsung-smart-tv-hack/.

[57] Jose, A. C., and Maleikan, R. 2017. Improving smart home security: Integrating logical sensing into smart home. *IEEE Sensors Journal* 17 (13), July, 2017. DOI= https://doi.org/10.1109/JSEN.2017.2705045.

[58] Yassein, M. B., et al. 2019. Smart home is not smart enough to protect you - Protocols, challenges and open issues. 10th International conference on emerging ubiquitous systems and pervasive Networks, Coimbra, Portugal, Nov 2019. DOI= https://doi.org/10.1016/j.procs.2019.09.453.

[59] Dahmen, J., et al. 2017. Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats. *J Reliable Intelligent Environments* 3, 2017, pp. 83-98. DOI= https://doi.org/10.1007/s40860-017-0035-0.