PROJECT PRESENTATION

SANDER VAN DESSEL, JOEY VAN ERUM

A BIG THANKS TO

Torben Svane

Nathalie Bosschaerts

Tinne Van Echelpoel

TABLE OF CONTENTS

INTRODUCTION

Sander Van Dessel

Joey Van Erum

BACKGROUND

MANY HOUSEHOLDS HAVE SMART DEVICES

SECURITY CONCERNS BECAUSE OF "SMARTIFICATION"

RESEARCH QUESTION

HOW SECURE ARE SMART-HOME DEVICES ?

OBJECTIVES

RESEARCH SECURITY OF SMART HOME DEVICES

CREATE A PAPER FOR ACADEMIC USE

METHODOLOGY

Raspberry Pi setup

Kali Linux

Wireshark

WORKING ABROAD BUT FROM HOME

- The challenges of projects in the era of corona
  - No access to campus equipment
  - Meetings only possible online
  - Workspace and living space are the same
- Challenges of writing academic paper
  - No previous knowledge
  - Lots of (unknown)document regulations

RESULTS

Most devices were secure

6/7 devices

Privacy still an issue

6/7 devices

1 device is secure and protects privacy

Exploits might be possible

RESULTS

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}
0

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

The box sends unencrypted TCP-data with personal information about the user when using Deezer. Figure 3 shows examples of such data: name, email, gender, birthdate, country, and language.

{"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\/
flow","md5_image":"","is_flow_available":false,"type":"user"},

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

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/tplink/ssh_default_creds
creds/routers/tplink/telnet_default_creds
creds/routers/tplink/ftp_default_creds
exploits/routers/tplink/archer_c2_c201_rce
exploits/routers/tplink/wdr842nd_wdr842n_configure_disclosure
exploits/routers/tplink/wdr740nd_wdr740n_backdoor
exploits/routers/tplink/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: 2.1500 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).

```
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).

CONCLUSION

- Always potential for improvement
- Higher level of security

FUTURE RECOMMENDATIONS

ENCRYPT ALL TRAFFIC

NEW UPDATES UNTIL MAJOR SECURITY ISSUES FIXED

ENCRYPT ALL DATA

INVEST MORE IN PRODUCT SECURITY

REFLECTION

- What did we learn
  - Academic paper 101
  - Ways to test devices
  - How to build a packet-sniffer
- What would we do differently
  - Choose a moment without Corona

REFLECTION

- Would we still do this project
  - YES
- Working on an international project
  - Develop English speaking & writing skills
  - Create international (business)contacts

REFLECTION

- Being on exchange
  - New friends and cultures
- Usefulness for future career
  - Very: No other opportunity to work on a research paper
  - Ability to work with a international team
  - Looks good on a CV

QUESTIONS ?