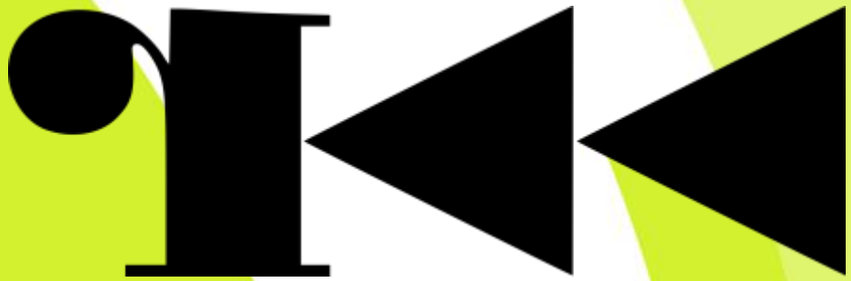
riscure



CON

2016

Rhme

CTF which runs on 5v over USBQ

Eduardo Novella

Riscure

1. Side Channels (smartcards, PayTV chipsets, IoT,…)
2. Fault Injection (smartcards, PayTV chipsets, IoT,…)
3. Embedded Devices (gas meters, routers, STB, IoT,…)
4. Software (TEE, HCE, DRM, and all related to 1,2,3)

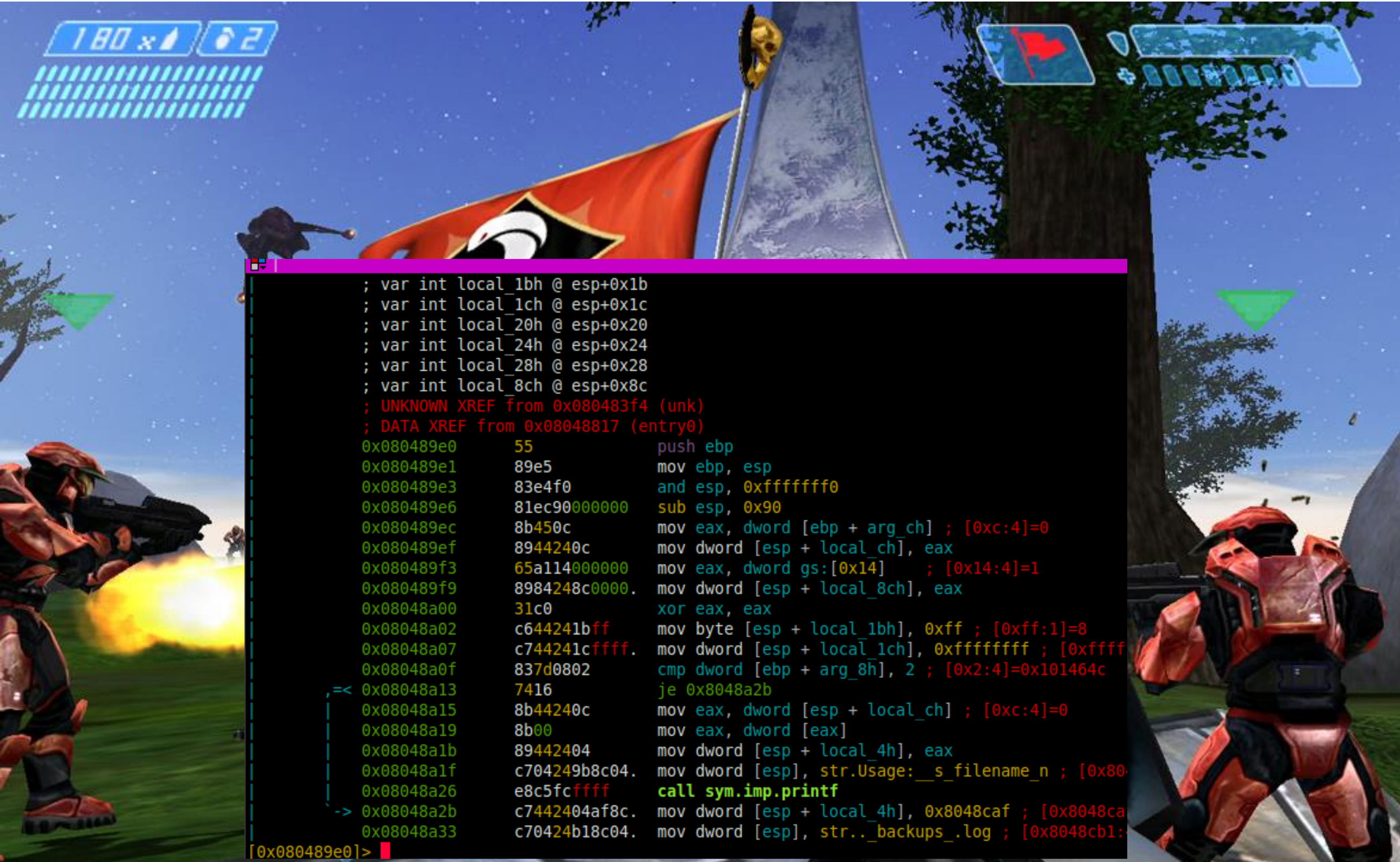
Agenda

1. What is the RHme 2015?
2. Development
3. Benefits
4. RHme 2016

What is


CTF


180 x
2
160.2m
60
bungie.net

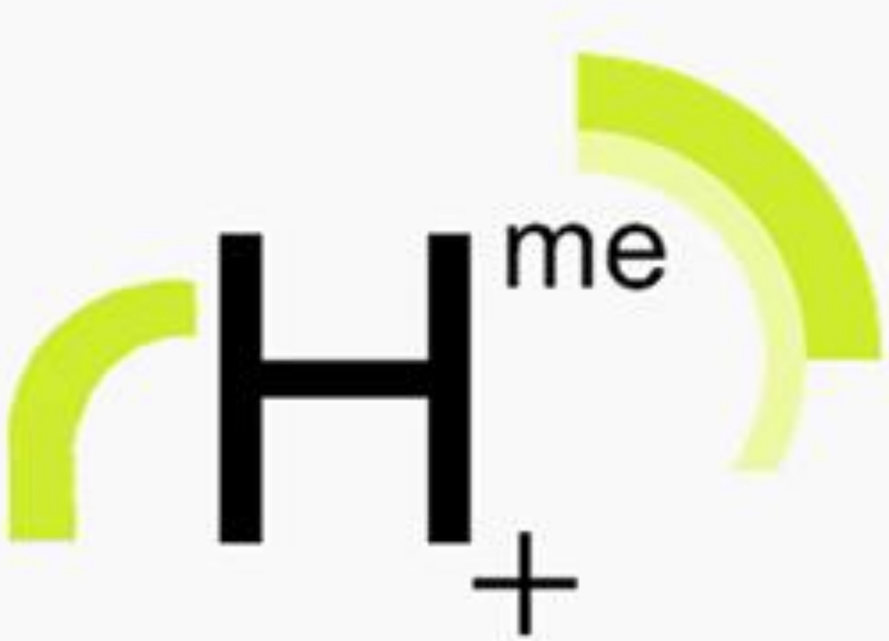



```
            ; var int local_1bh @ esp+0x1b
            ; var int local_1ch @ esp+0x1c
            ; var int local_20h @ esp+0x20
            ; var int local_24h @ esp+0x24
            ; var int local_28h @ esp+0x28
            ; var int local_8ch @ esp+0x8c
            ; UNKNOWN XREF from 0x080483f4 (unk)
            ; DATA XREF from 0x08048817 (entry0)
            0x080489e0      55              push ebp
            0x080489e1      89e5            mov ebp, esp
            0x080489e3      83e4f0          and esp, 0xfffffff0
            0x080489e6      81ec90000000    sub esp, 0x90
            0x080489ec      8b450c          mov eax, dword [ebp + arg_ch] ; [0xc:4]=0
            0x080489ef      8944240c        mov dword [esp + local_ch], eax
            0x080489f3      65a114000000    mov eax, dword gs:[0x14]    ; [0x14:4]=1
            0x080489f9      8984248c0000.   mov dword [esp + local_8ch], eax
            0x08048a00      31c0            xor eax, eax
            0x08048a02      c644241bff      mov byte [esp + local_1bh], 0xff ; [0xff:1]=8
            0x08048a07      c744241cffff.   mov dword [esp + local_1ch], 0xffffffff ; [0xffff
            0x08048a0f      837d0802        cmp dword [ebp + arg_8h], 2 ; [0x2:4]=0x101464c
        ,=< 0x08048a13      7416            je 0x8048a2b
        |   0x08048a15      8b44240c        mov eax, dword [esp + local_ch] ; [0xc:4]=0
        |   0x08048a19      8b00            mov eax, dword [eax]
        |   0x08048a1b      89442404        mov dword [esp + local_4h], eax
        |   0x08048a1f      c704249b8c04.   mov dword [esp], str.Usage:__s_filename_n ; [0x80
        |   0x08048a26      e8c5fcffff      call sym.imp.printf
        `-> 0x08048a2b      c7442404af8c.   mov dword [esp + local_4h], 0x8048caf ; [0x8048ca
            0x08048a33      c70424b18c04.   mov dword [esp], str._backups_.log ; [0x8048cb1:
[0x080489e0]>
```

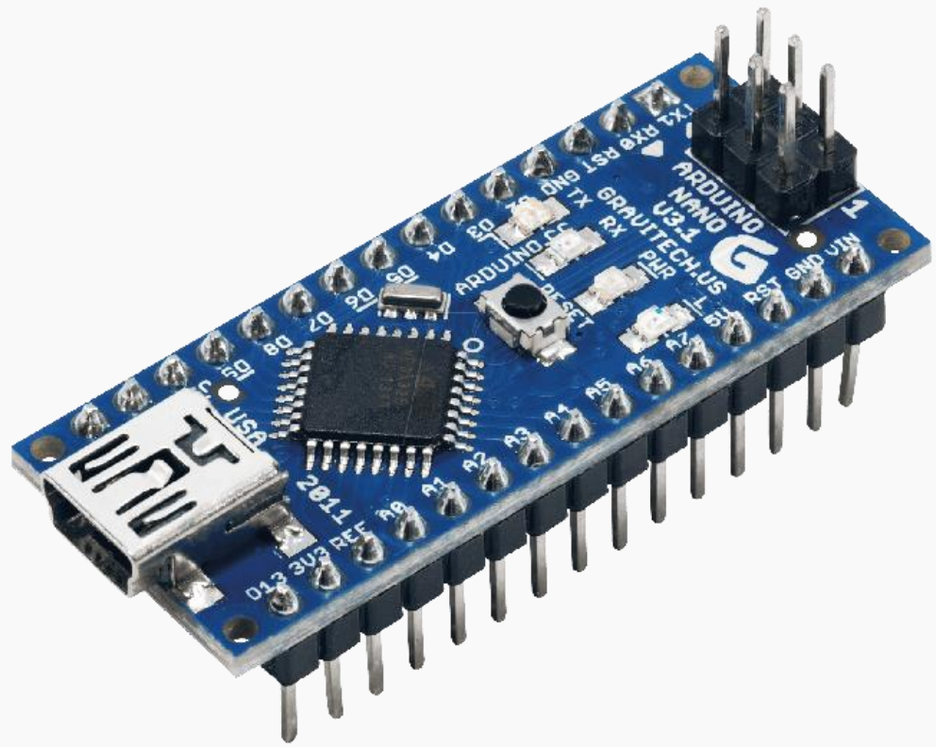

180
2
ARDUINO
UNO
DIGITAL (PWM~)
POWER
ANALOG IN
160.2m
60
bungie.net


180 x
2
160.2m
60
ARDUINO
UNO
bungie.net

Riscure Hack ME challenge



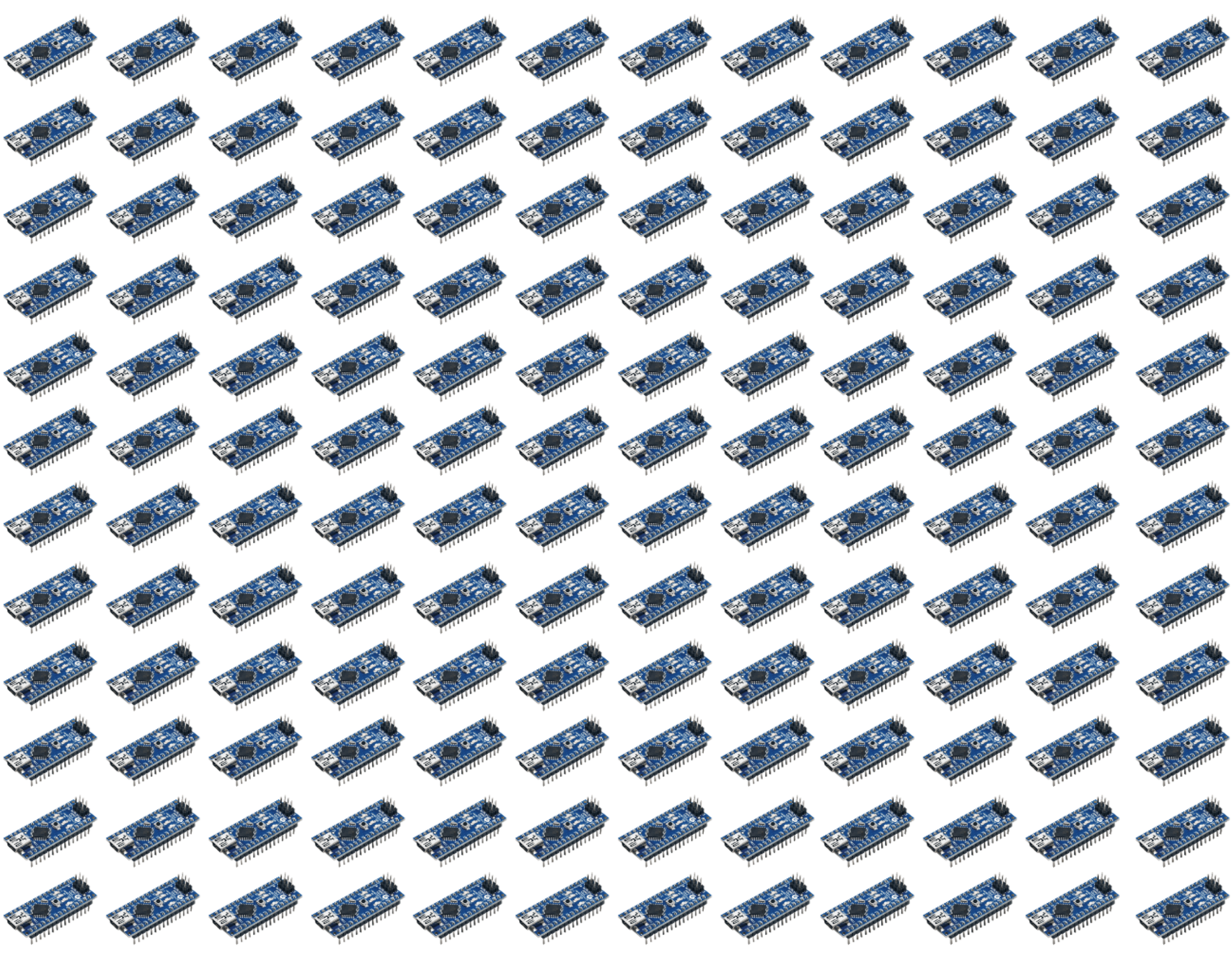
- CTF challenge running in an Arduino Nano clone
- First hardware CTF ever published

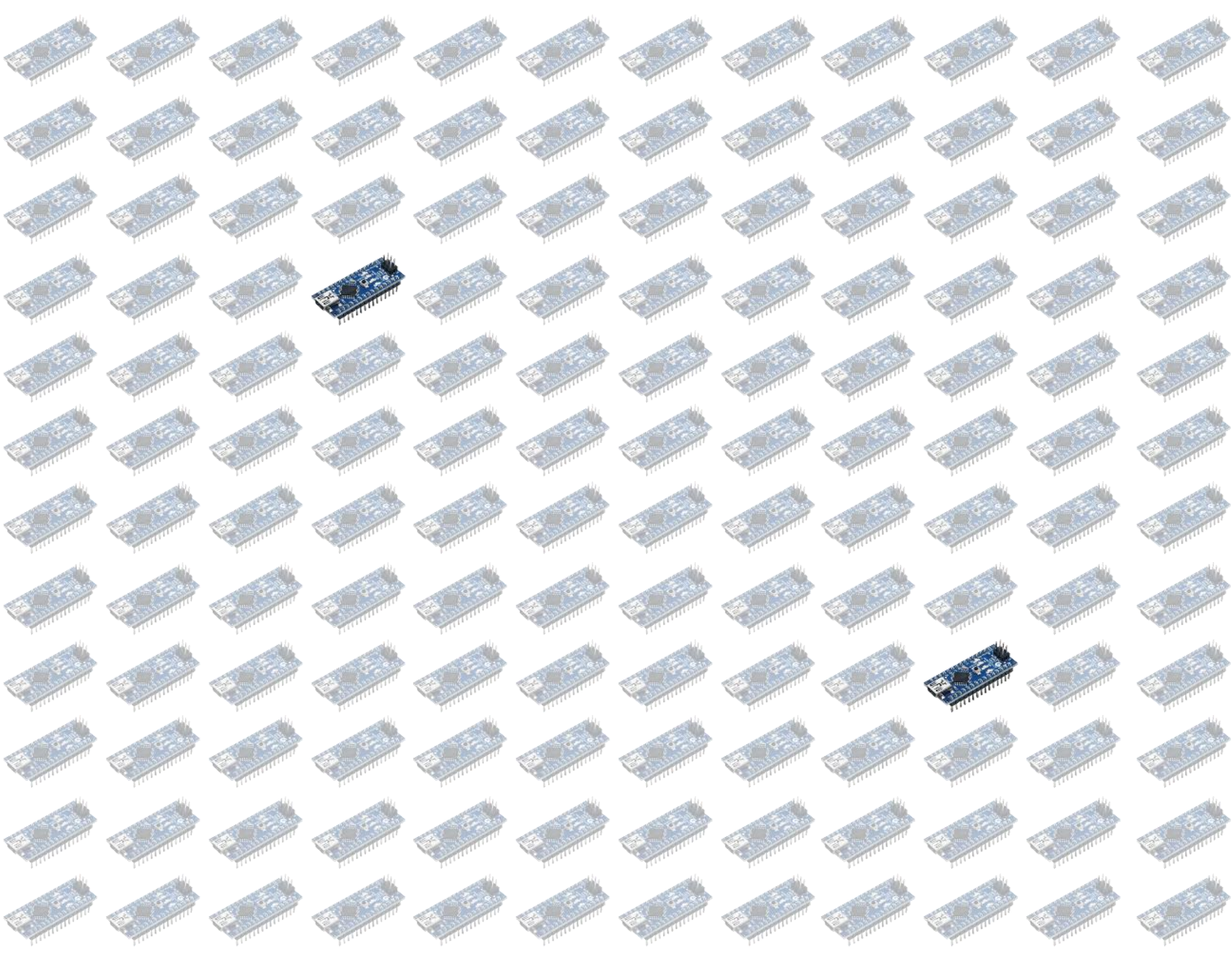


Riscure Hack ME challenge

- The goal of the game is to extract 3 secret keys by solving different challenges of increasing difficulty.
- Each challenge can be solved in many ways.
- Software and hardware exploitation techniques can be used.

EUROPE 2015






CISCO
TM


CISCO
TM


CISCO
TM

Lessons learned

* It is hard to do secure coding
* Clear all the memory after a reset
* **NEVER** trust a third-party library

```
void generate_challenge(void) {
    uint32_t responses[3];
    is_auth_nonce_valid = 1;



                        DEVELOPMENT


    auth_nonce = get_random_uint32_t();
    calculate_response(auth_nonce, &responses[0],
USER_USER,0);
-- INSERT --                    22,32          43%
```

Team

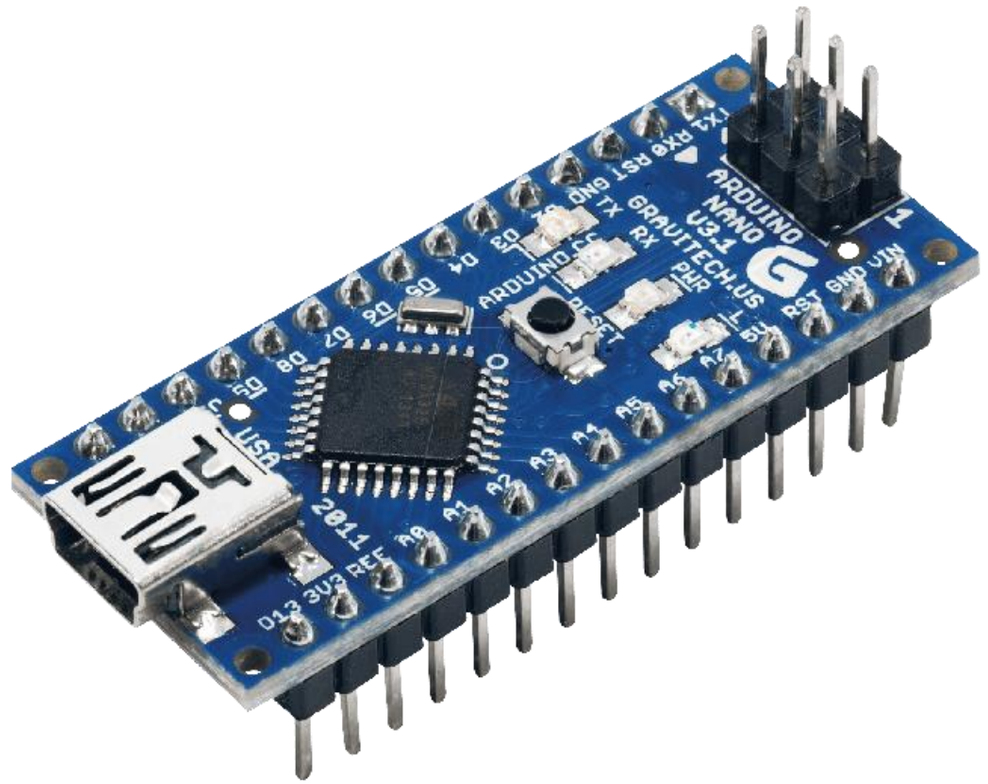
riscure

Alexandru Geana
alegen on r2 irc

Ramiro Pareja
<3 low level stuff

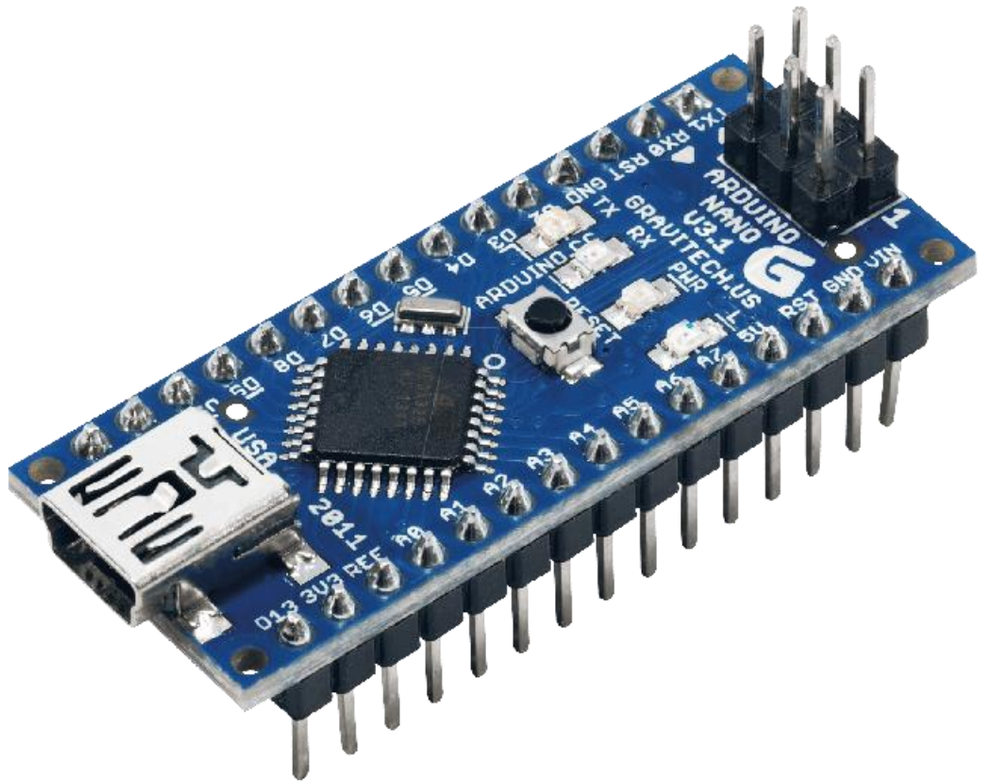
Design criteria / Development goals

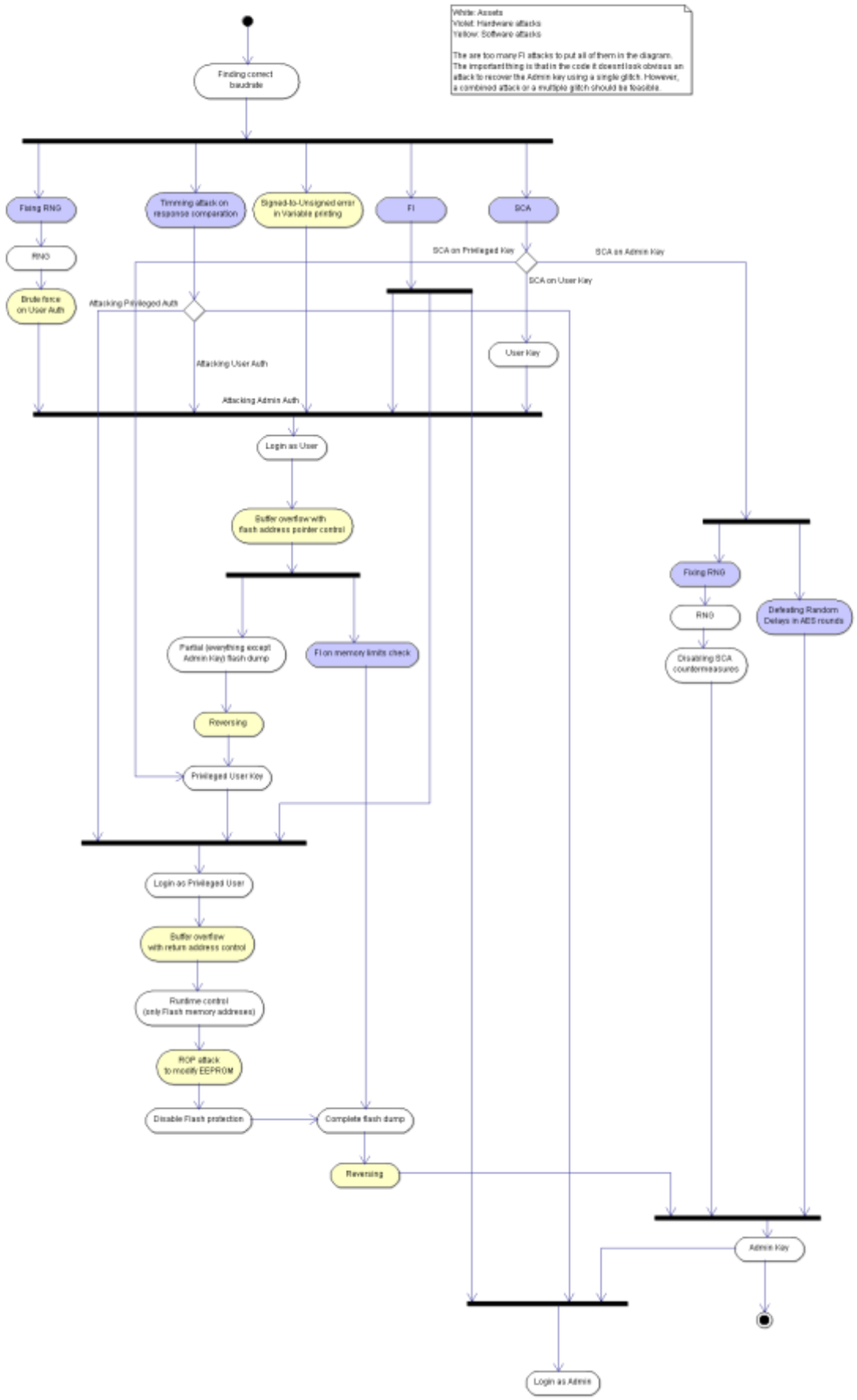
- Hardware:
  - Cheap (1$)
  - Easily available



Design criteria / Development goals

- Hardware:
  - Cheap (1$)
  - Easily available
- Software:
  - FI, SCA and SW solutions
  - Progressive difficulty
  - Contained vulnerabilities




White: Assets
Violet: Hardware attacks
Yellow: Software attacks
The are too many FI attacks to put all of them in the diagram.
The important thing is that in the code it doesn't look obvious an attack to recover the Admin key using a single glitch. However, a combined attack or a multiple glitch should be feasible.
Finding correct baudrate
Fixing RNG
RNG
Brute force on User Auth
Timming attack on response comparation
Signed-to-Unsigned error in Variable printing
FI
SCA
SCA on Privileged Key
SCA as Admin Key
SCA on User Key
Attacking Privileged Auth
Attacking User Auth
Attacking Admin Auth
User Key
Login as User
Buffer overflow with flash address pointer control
Partial (everything except Admin Key) flash dump
FI on memory limits check
Reversing
Privileged User Key
Login as Privileged User
Buffer overflow with return address control
Runtime control (only Flash memory addresses)
ROP attack to modify EEPROM
Disable Flash protection
Complete flash dump
Reversing
Fixing RNG
RNG
Disabling SCA countermeasures
Defeating Random Delays in AES rounds
Admin Key
Login as Admin

What is new

What is new in Rhme 2016?

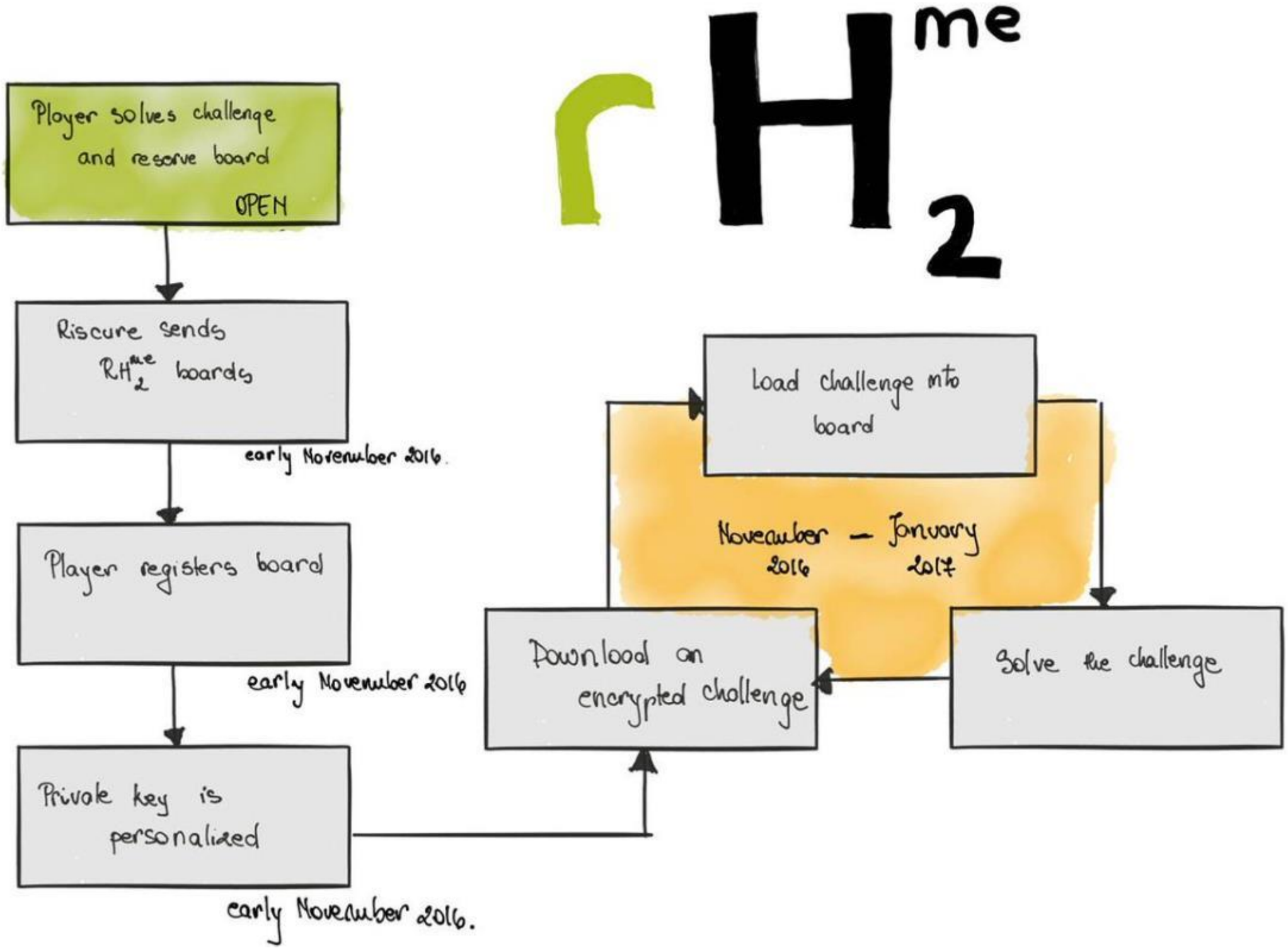
- New game style
- New development framework
- New team
- New hardware?

SCA	FI	EXPLOITATION	CRYPTO		
	$200	$200		$200	$200
$400	$400	$400	$400	$400	$400
$600	$600		$600		$600
$800	$800		$800	$800	
	$1000	$1000	$1000	$1000	$1000

Development framework

- Secure bootloader
- Eclipse based development environment
- Challenge template
- Tutorials

Rhme2 timeline



PLAY!

Exploiters (5 boards)

Download now the RHME challenge and try to exploit it:

https://github.com/Riscure/RHme-2015/

Reversers (5 boards)

Sign up for the new RHME2 by solving this easy pre-challenge:

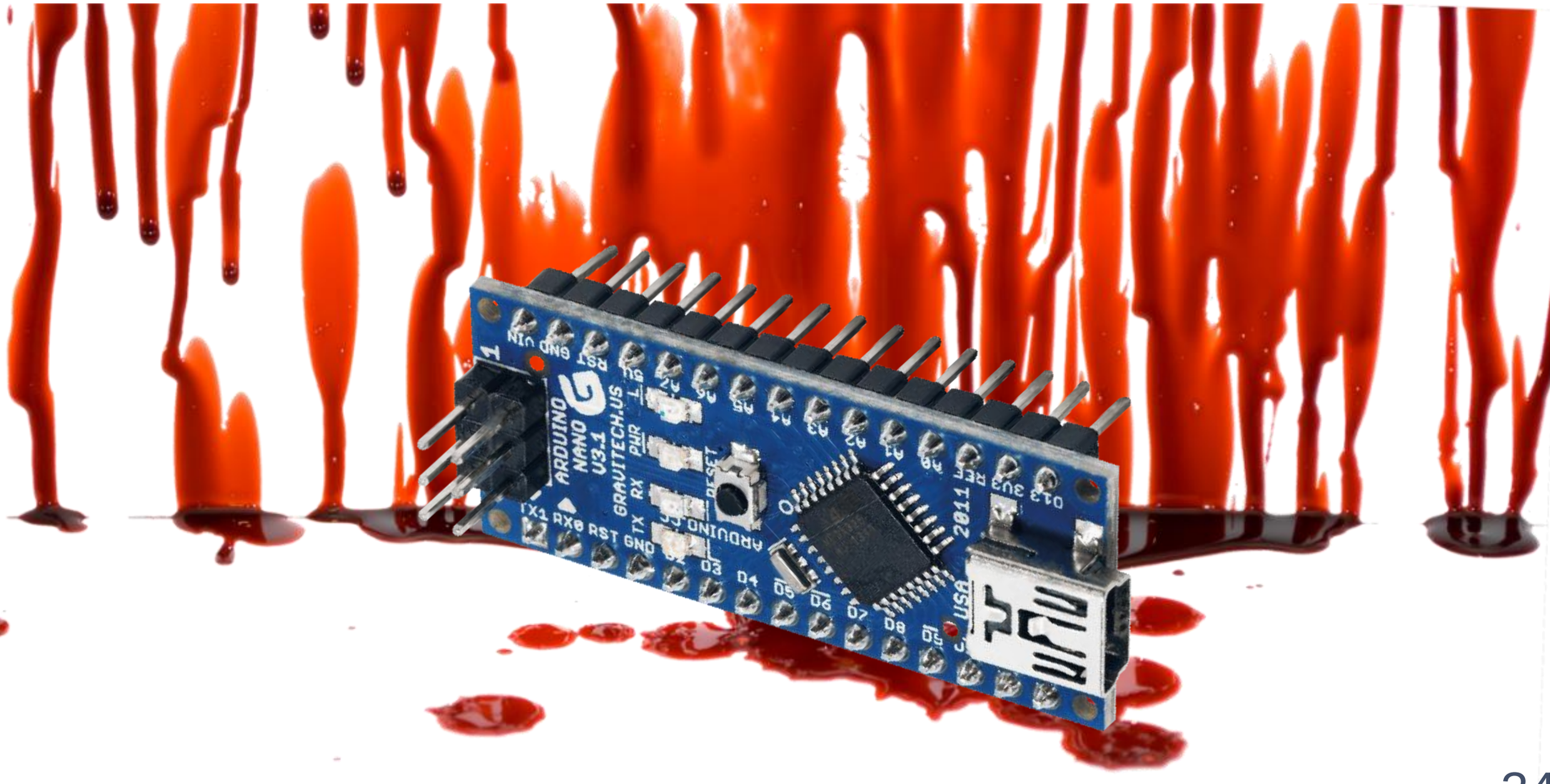
https://github.com/Riscure/RHme-2016/

USE RADARE!

Remember…

- First Send First Receive
- Solutions: eduardo@riscure.com
  - Subject : **[exp|re] r2con rhme**
  - **[name|nickname]**
  - **Flag & full r2 log**
- Ask me for your board during r2con
- If you do not get any board during r2con
  - Solve the pre-challenge rhme2 (<3min) at any time and reserve your board (max 500)

Questions?


ARDUINO
NANO
V3.1
GRAVITECH.US
PWR
RX
TX
RST
ARDUINO.CC
2011
USB