Hardsploit

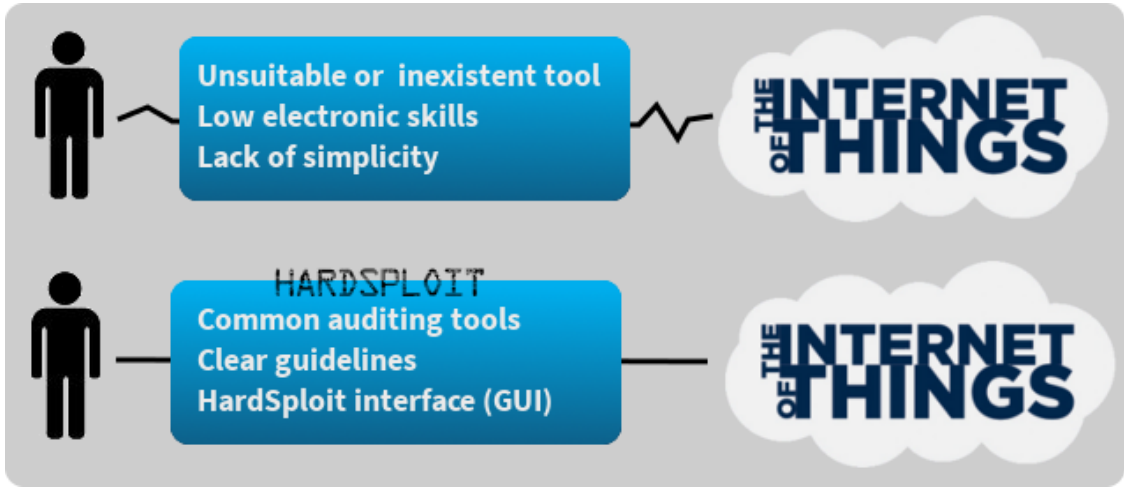
(Hardsploit.io)

Like Metasploit but For Hardware Hacking

32C3CFP Submission

What is Harsploit?

- A Framework for Hardware Pentest or electronic designers
- Open Source
- Hardware + Software
- More details on Hardsploit.io

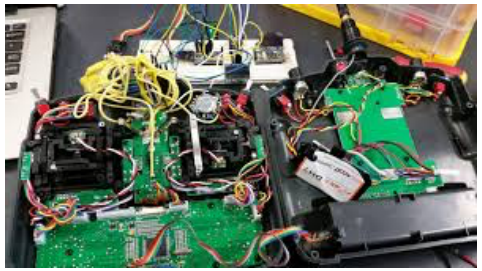


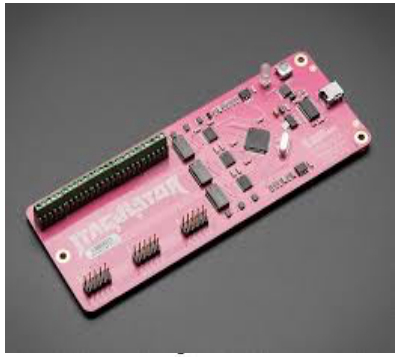
Why we choose to create HardSploit? (1/2)

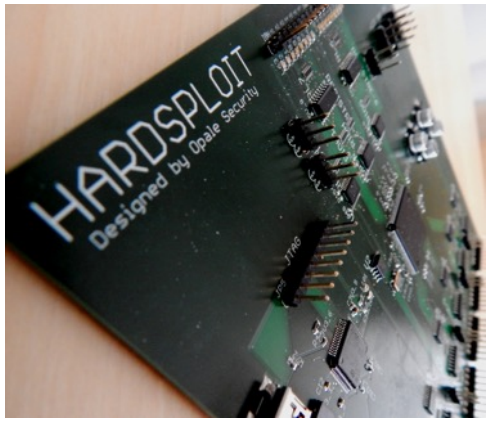
- Facilitate the audit of electronic systems for industry ‘security’ workers
  - Consultant, Auditor, Pentesters, Product designer etc.
- Increase the level of security (and trust!) of new communicating products designed by industry

Why we choose to create HardSploit? (2/2)

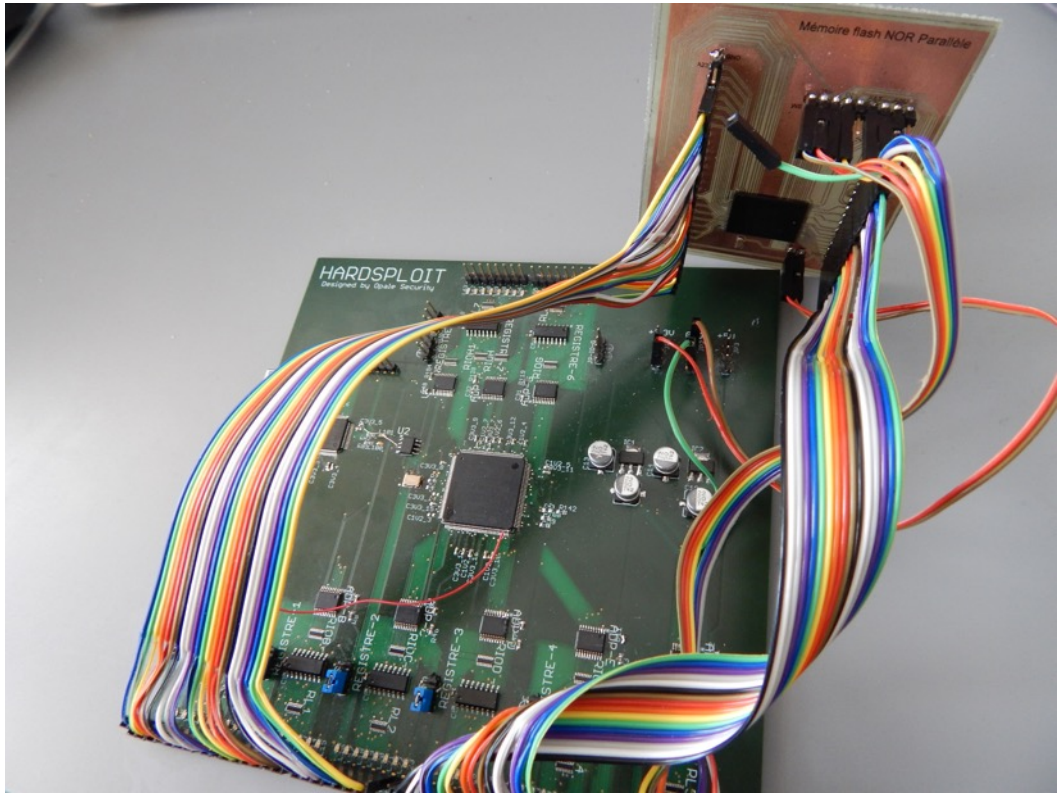
- To create a « all in one tools » for Hardware Hacking



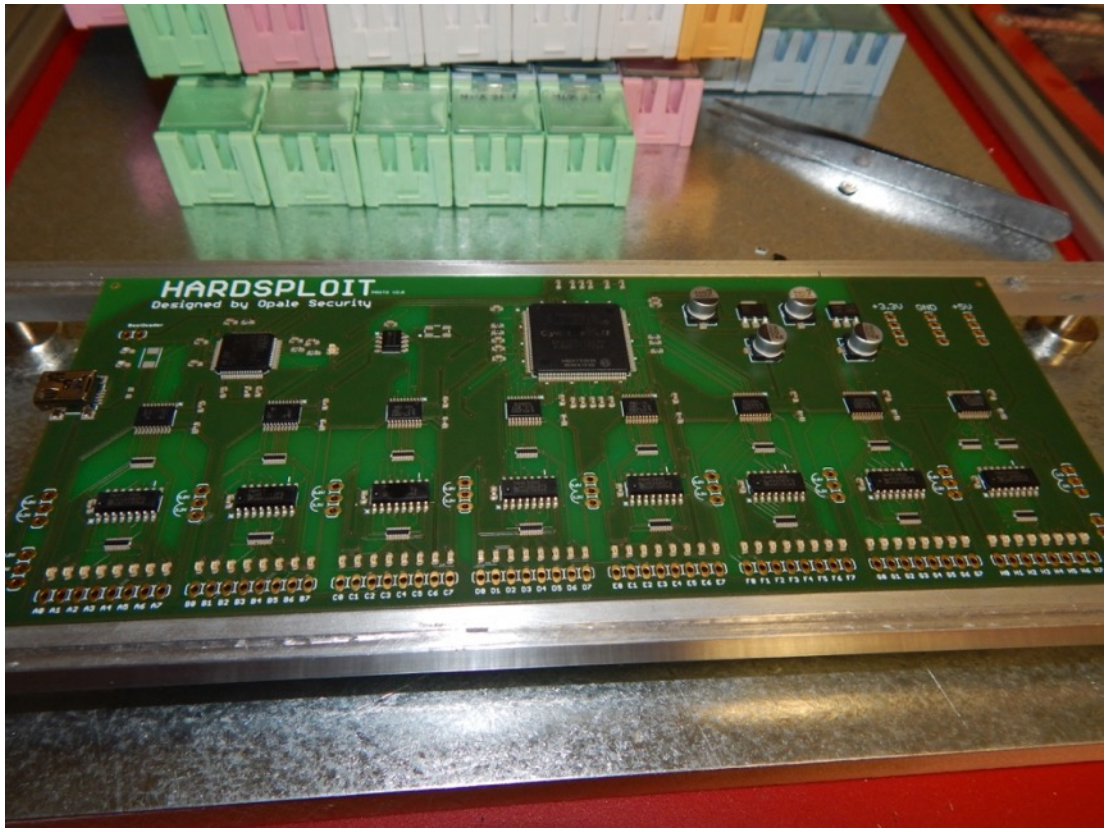




Some Hardsploit prototypes photos



Proto V1

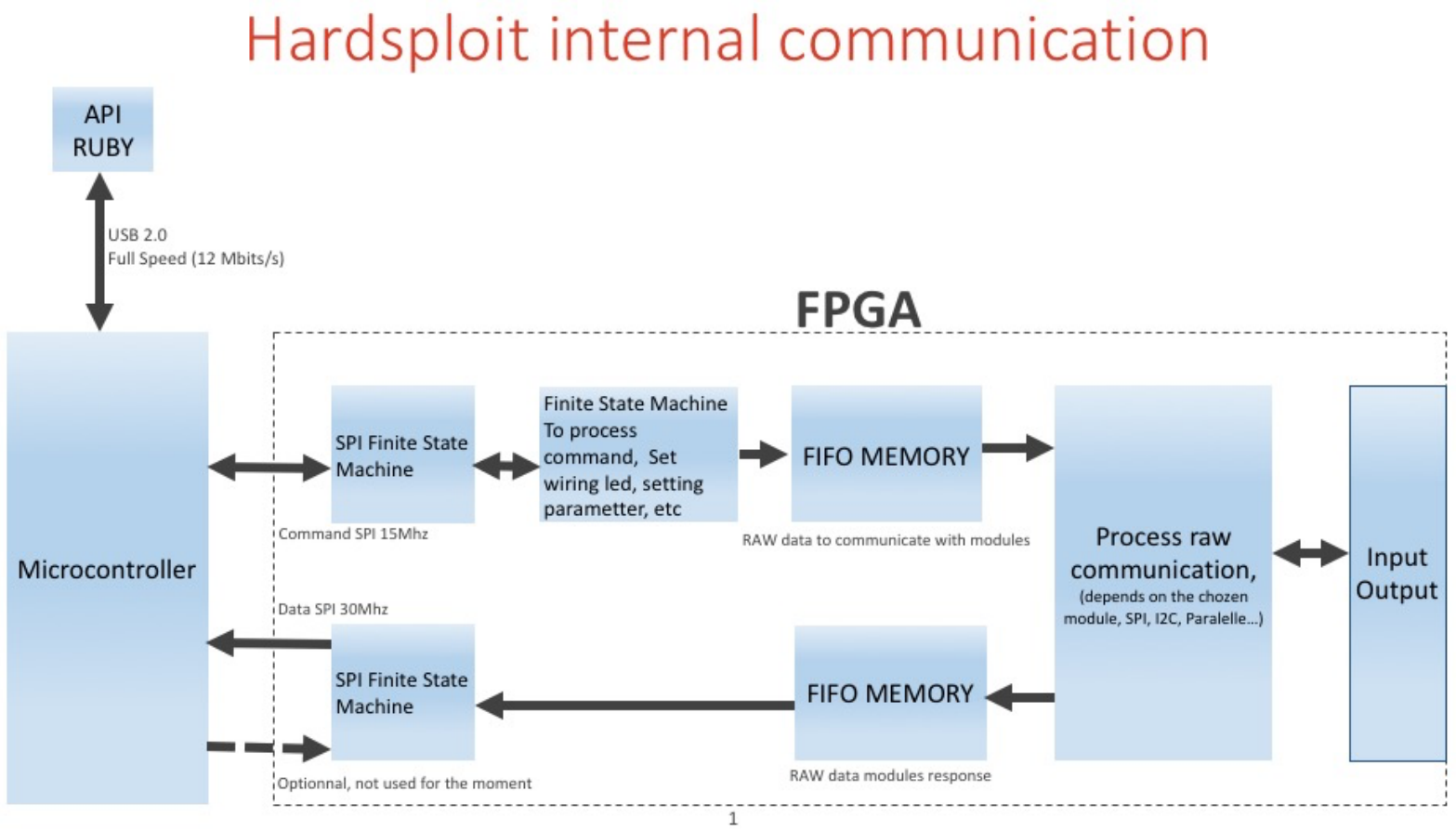


Final form factor on 20 06 2015

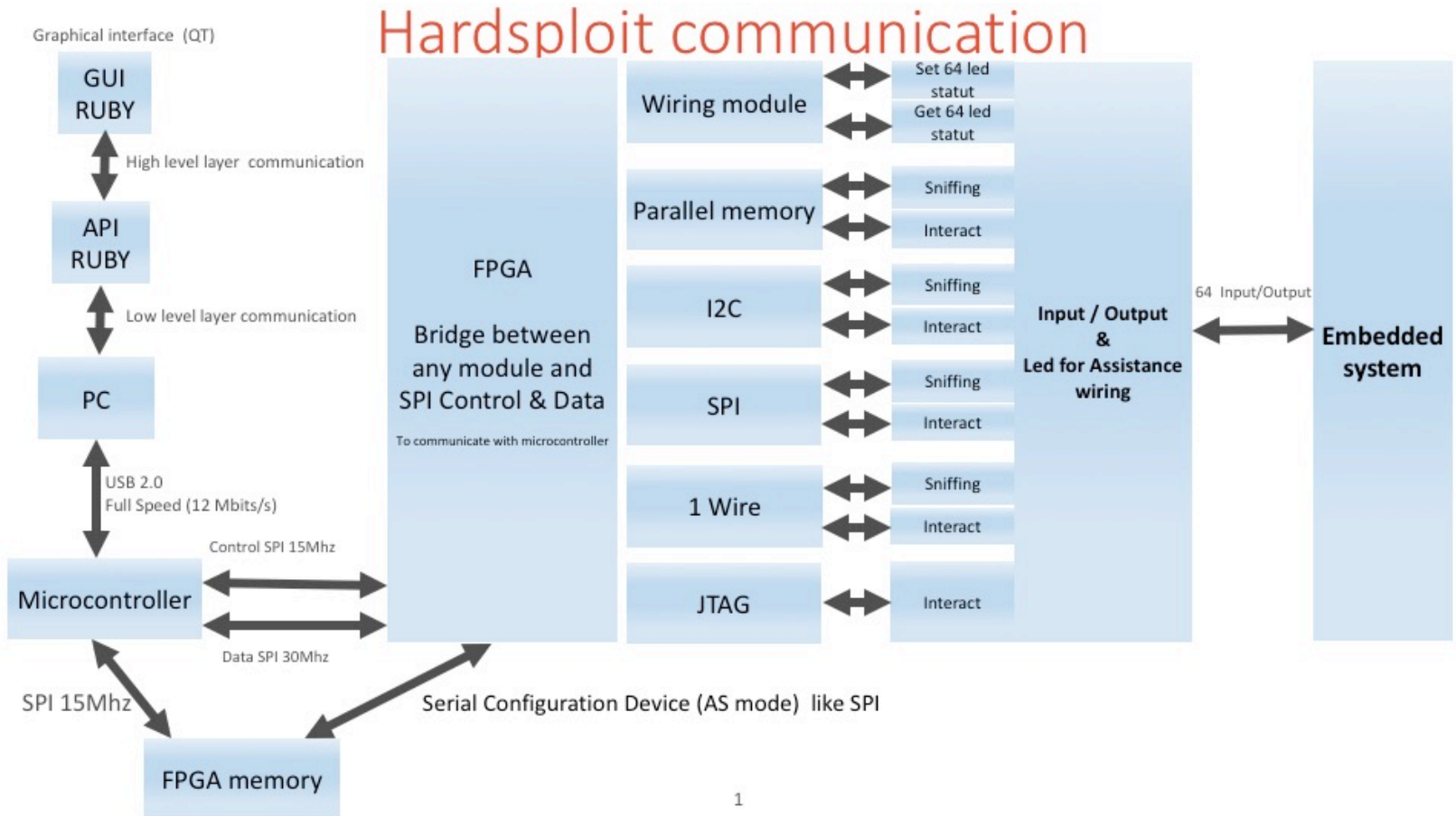
Hardware Features

- All-in-one tool dedicated for Hardware Hacking
- 64 I/O channels
- Adjustable target voltage for level translation: 3,3V & 5V
- FGPA Cyclone II for versatile and powerfull electronic hardware hacking modules
- USB interface for direct connection to GUI
- Easy-to-use GUI & Console mode integrated in the Metasploit Framework

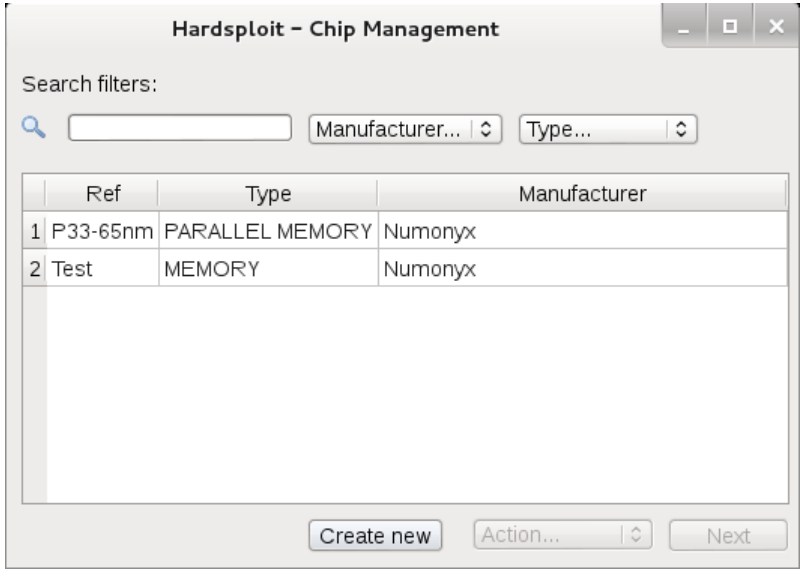
Internal design (1/2)

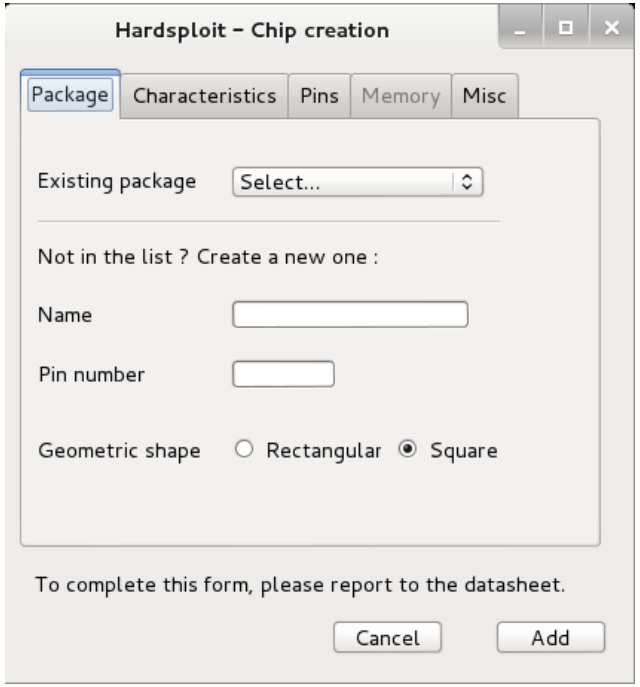


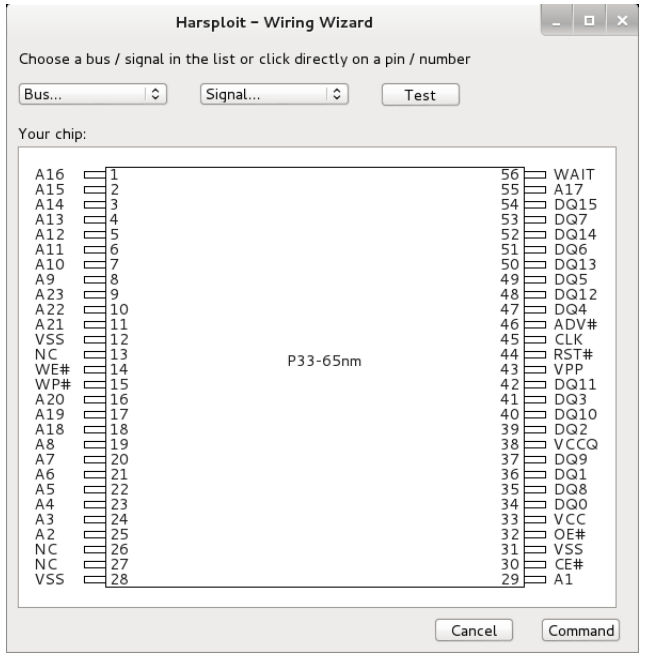
Internal design (2/2)

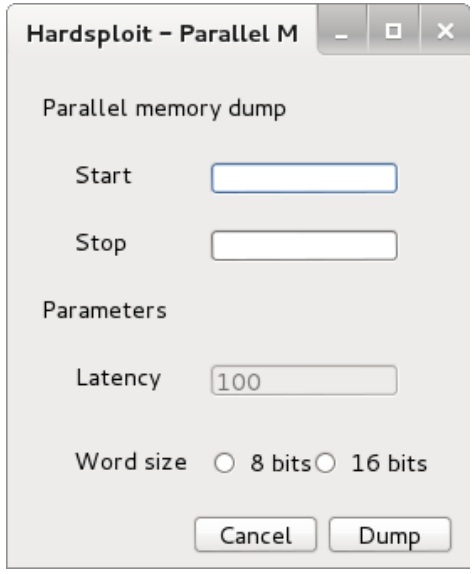


Hardsploit GUI

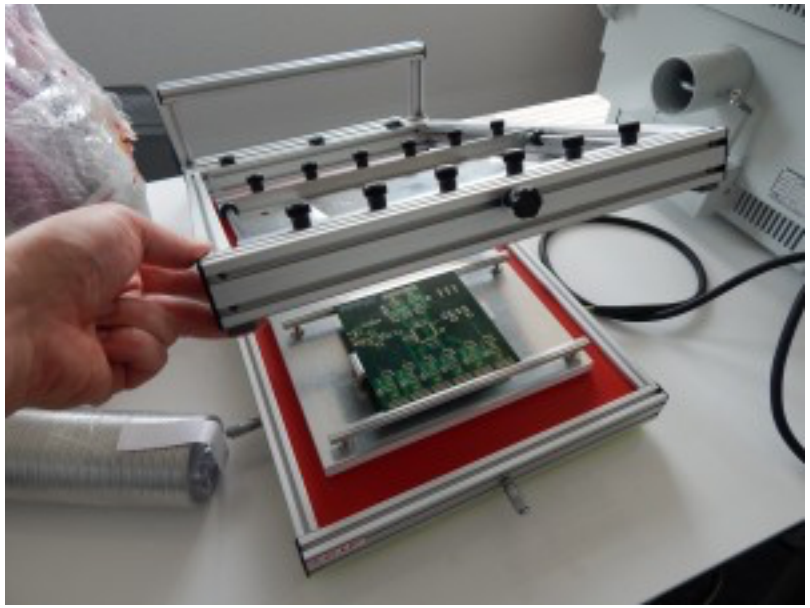


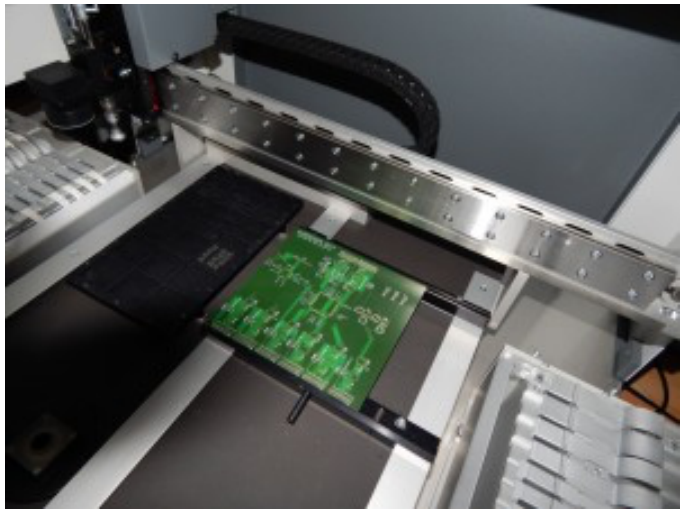


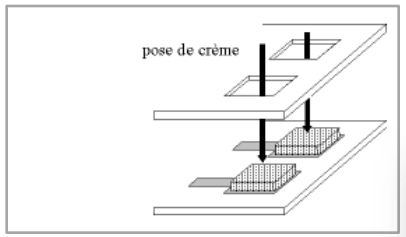


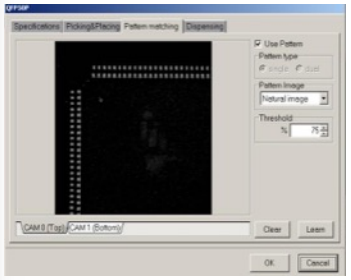


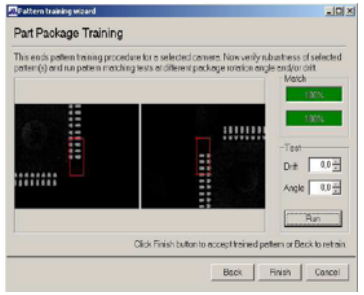
How we create Hardsploit Board !











Hardsploit modules & Framework

- Hardsploit is a tool with software and electronic aspects
- This is a technical and modular plateform (using FPGA)
- To perform security tests on electronic communications interfaces of embedded devices
- It’s a Framework !

- *All-in-one tool for Hardware pentest*

Features

- The main Hardware security audit functions are
  - Sniffer,
  - Scanner,
  - Interact,
  - Dump memory (even paralleles ones)
  - …

  - Hardsploit modules will let hardware pentester intercept, replay and/or and send data via each type of electronic bus used by the target. The level of interaction that pen-testers will depend on the electronic bus features…

Hardsploit modules

- Hardsploit ‘s modules enable you to analyse all sort of electronic bus (serial and parallel type)
- JTAG, SPI, I2C‘s,
- Parallel address & data bus on chip,
- and more others to come in the futur…

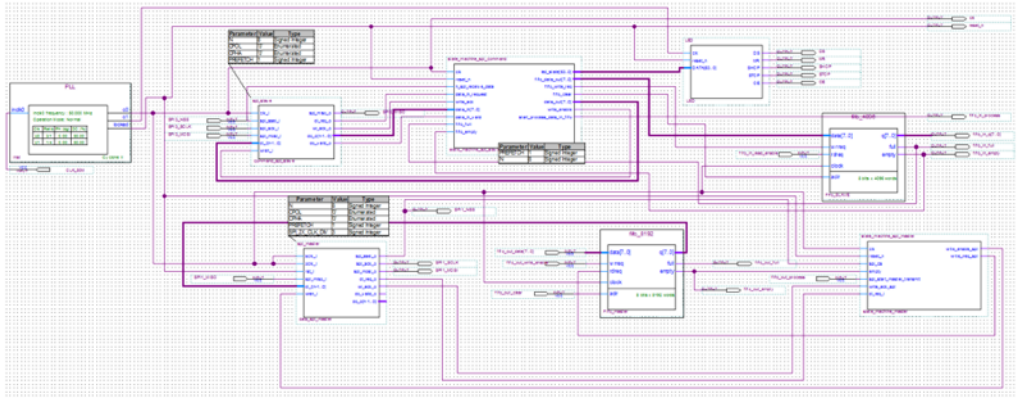
Assisted visual wiring function

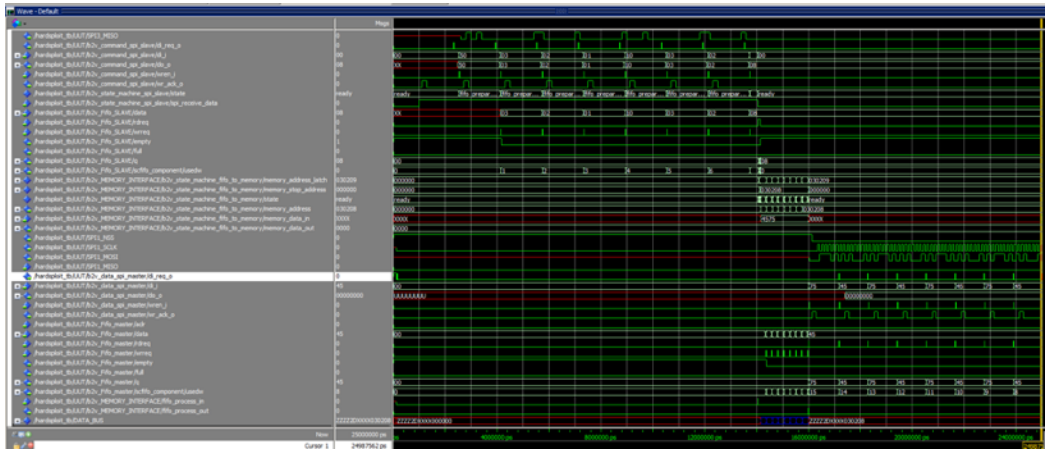
- *No more stress with that tremendous part of Hardware pen testing : You will know what need to be connected and where !*

- We have integrate into the tool an assisted visual wiring function to help you connect easily all wires to the hardware target:
  - GUI will display the pin organization (Pin OUT) of the targeted chip.
  - GUI will guide you throughout the wiring process between Hardsploit connectors and the target
  - GUI will control a set of LED that will turn ON / OFF to let you find the right Hardsploit pin to connect to your target

How a module is designed : parallel memory dump example (1/2)

- We have created a FPGA module that is able to dump most of parallel memory chip.
- It will help security pentesters to dump firmware or all content contained in such memory in an easy way.
- Easier than if creating a dumping function each time … No more arduino like board with plenty of wiring difficulties to connect to your chip, no more trouble to find the right memory command to be able to dump the component in front of you… The GUI will help you achieve that in few click only.
- Faster, as we use high speed FPGA buses and machine state to achieved the dump.





1st result : only 5 to 10 min to read a embedded linux rom of 128MB.

How a module is designed : parallel memory dump example (2/2)

- How to use that funky and (over) hype parallel dumping function ?

- We create a low level API with ruby that let you interact with FGPA module (Harsploit Module) in a simply way.

```ruby
#!/usr/bin/ruby
require_relative 'HardSploitAPI'

def callbackReceive(receiveData)
    print "#{receiveData}\n"
end

def callbackError(receiveData)
    print receiveData  + "\n"
end


HardAPI = HardSploitAPI.new("/dev/ttyACM0",method(:callbackReceive),method(:callbackError))
HardAPI.readByteFromMemory(0x00000000,0x000001FF)
```

Conclusion

- Hope our modest submission could interest your selection commitee and attendees
- Contact : +33 6 45 45 33 81
- Mail : yann.allain@opale-security.com