KEYNTERCEPTOR

Press any key to continue...

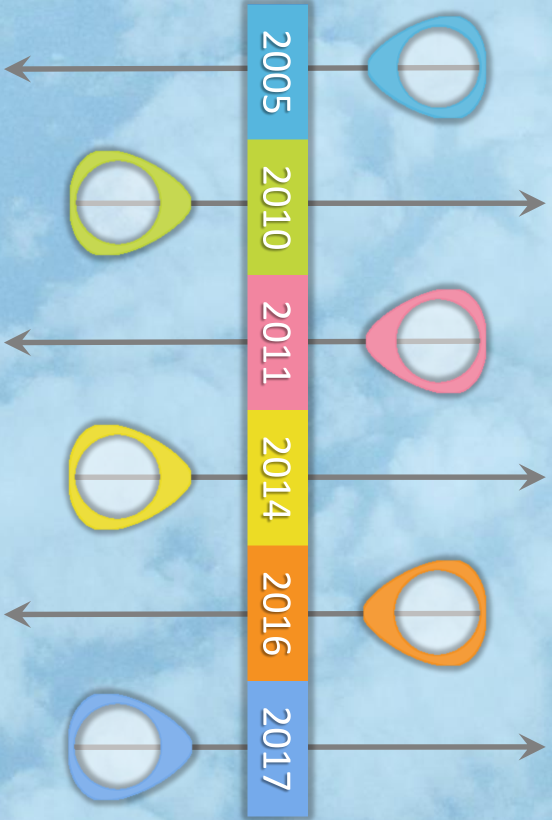
Niels van Dijkhuizen [NebulaH] 2018

This presentation

About me

- Existing USB HID attacks / tools
- What's wrong with them?
- Available protections / mitigations
- My implant PoC
- Putting it into an attack scenario
- Demo-time...

Existing USB HID attacks / tools



KeyGhost USB keylogger

PHUKD - Irongeek
HAK5 USB Rubber Ducky

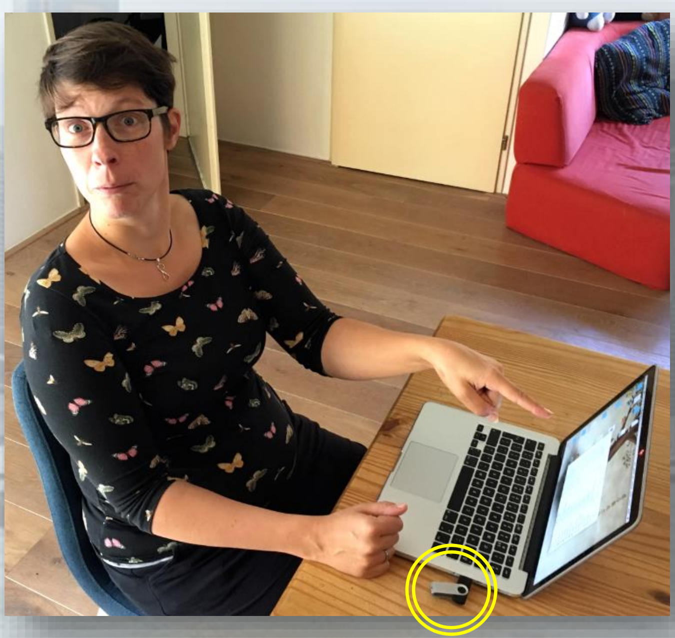
Keylogger/PHUKD Hybrid

BadUSB - Karsten Nohl
USBDriveby - Samy Kamkar

BadUSB 2.0
David Kierznowski

HAK5 Bash Bunny
Cactus WHID injector

What's wrong with it?



Kind of in-your-face!

What's wrong with it?

Requires either:

- An unlocked and unattended computer
- Very good social engineering skills

- Many payloads require direct internet access

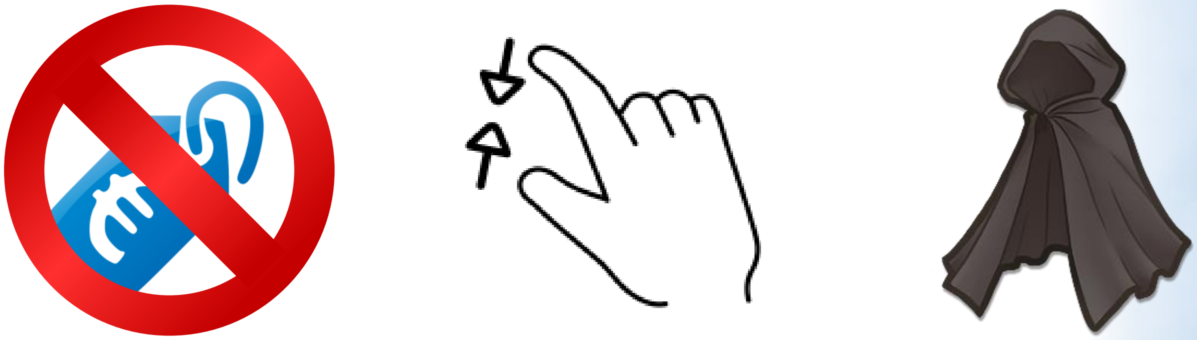
- Protection available

Available protection mechanisms

USG	Robert Fisk
USBProxy	Dominic Spill
USBGuard	Daniel Kopeček
GoodDOG	Tony DiCola
Beamgun	Josh Lospinoso
USB keyboard guard	G Data
Duckhunt	Pedro M. Sosa
Linux patches	GRSecurity

A new implant?

a HID attack that works with locked machines and bypasses known protection mechanisms



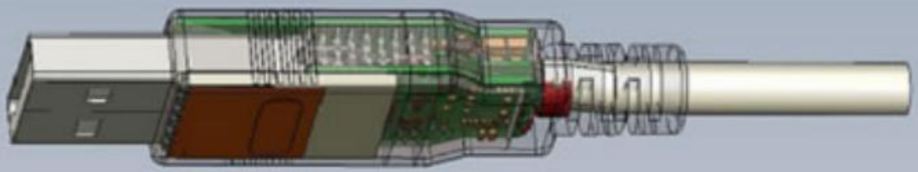
Design requirements

1. The implant should be in-line with the keyboard and the host.

2. The implant should have notion of real-time.

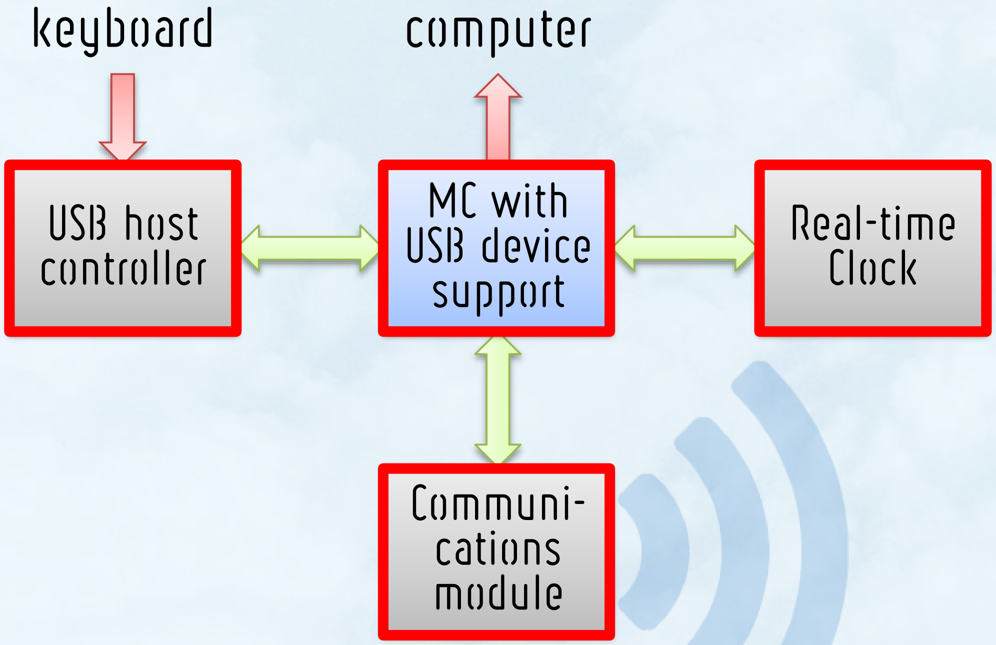
and spice it up a bit…

3. The implant could use an over the air communication channel.



NSA COTTONMOUTH-I, MOCCASIN

Hardware diagram



Teensy 2.0: Arduino-based MC

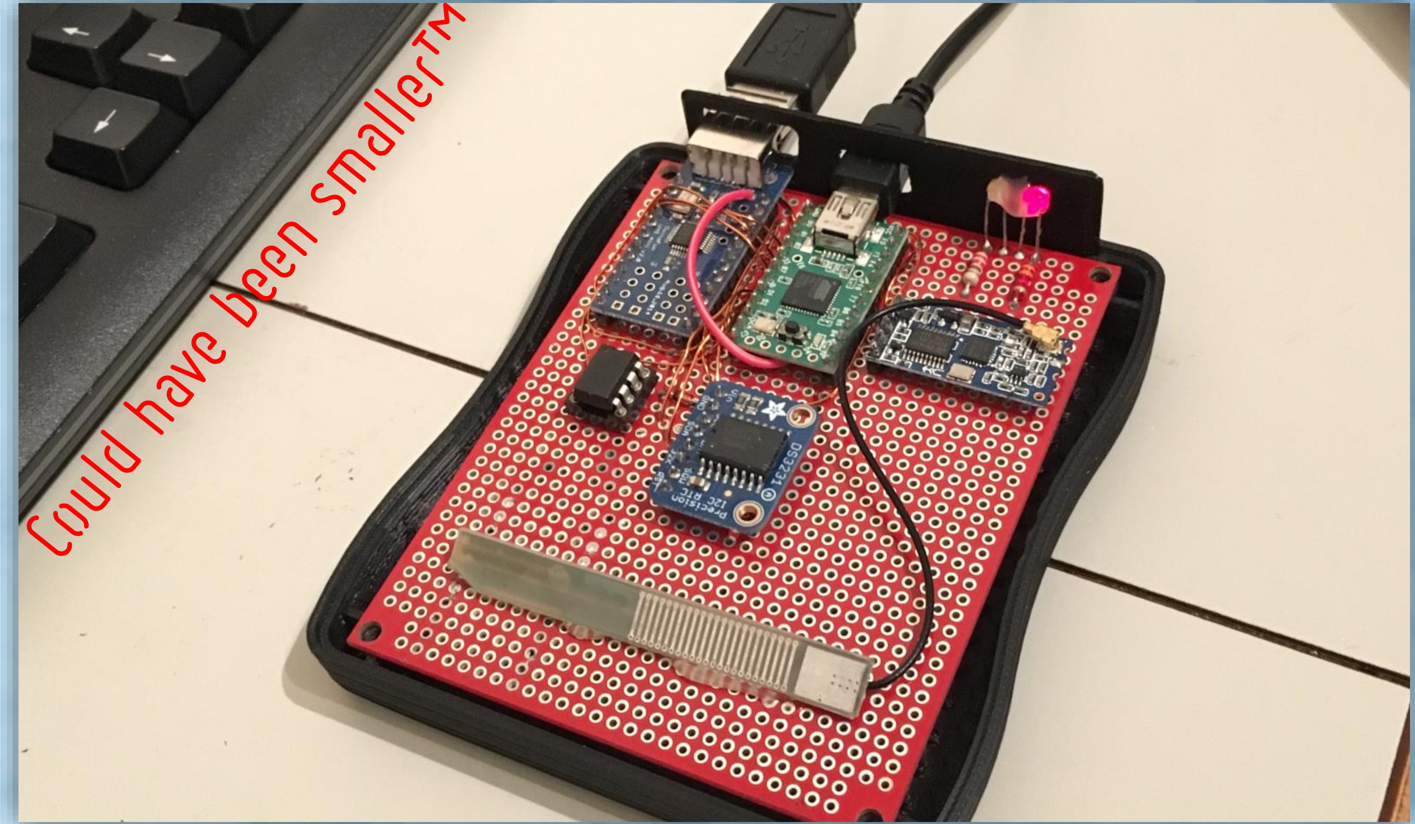
Maxim MAX3421E

Maxim DS3132

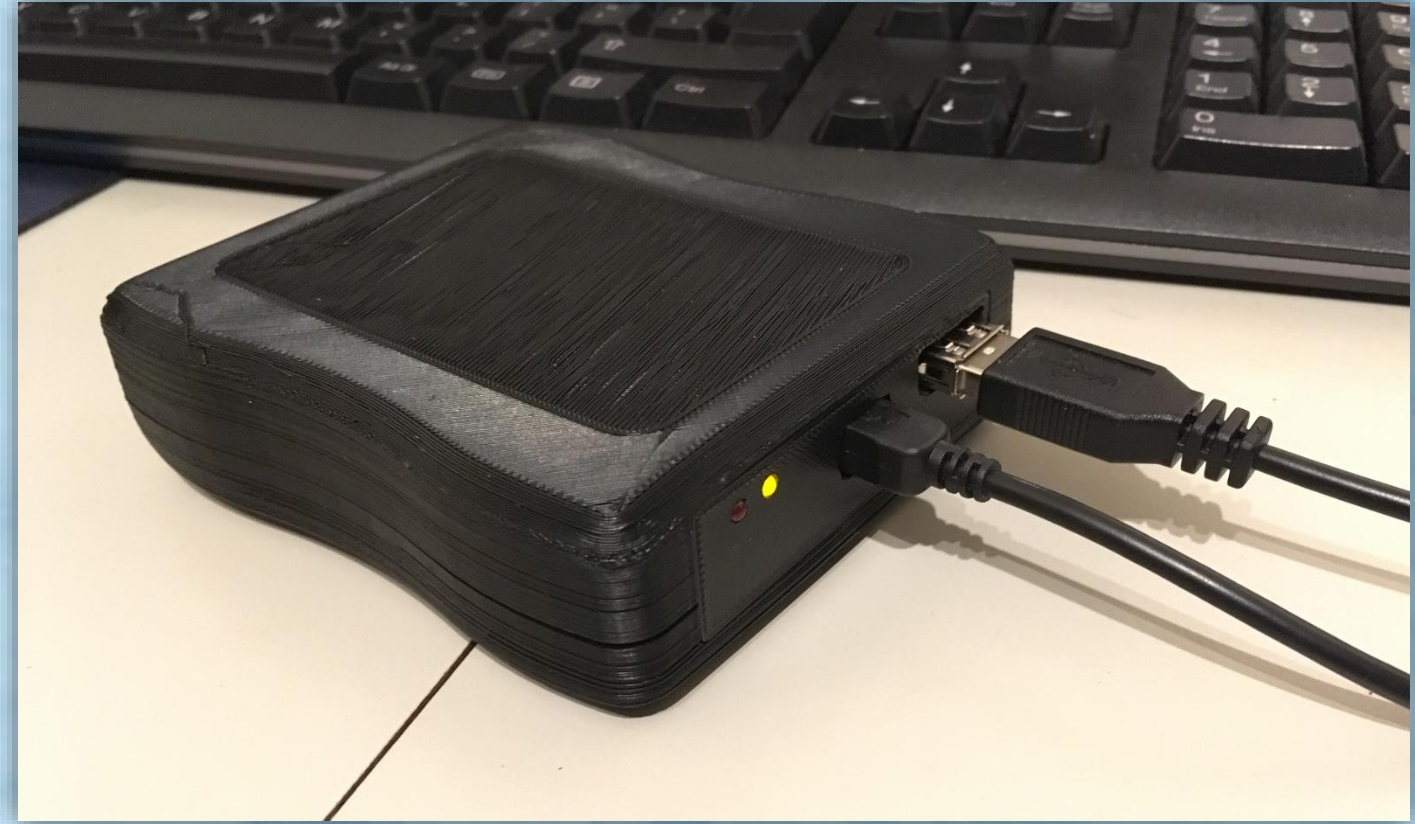
433Mhz UART

EEPROM (nvram)

Keynterceptor PoC HW

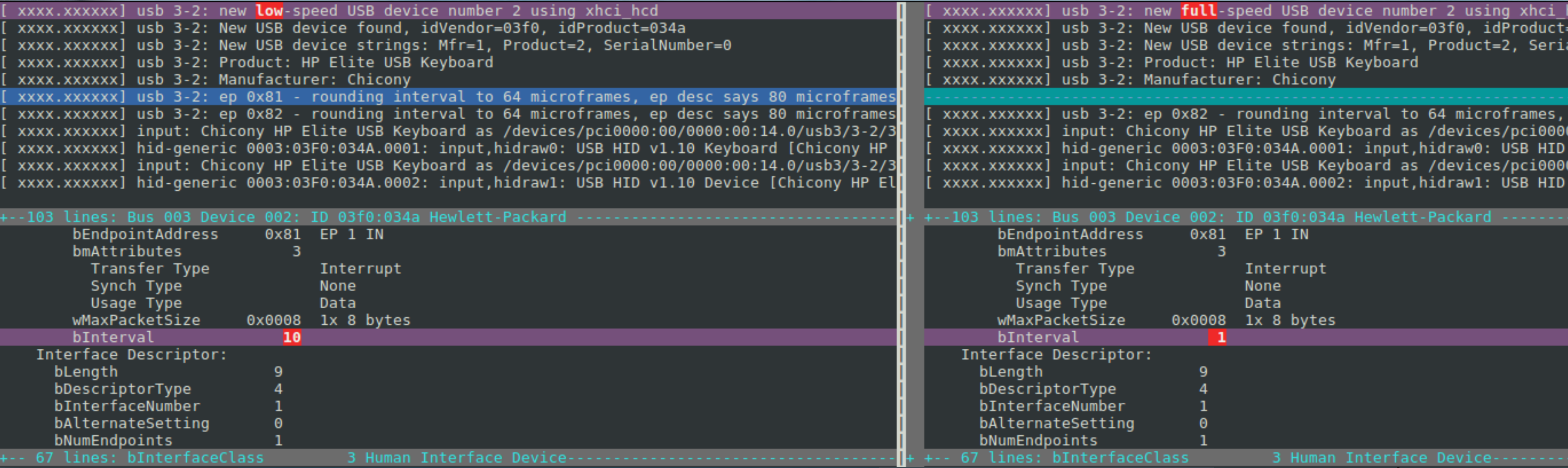


Keynterceptor PoC HW



Bypassing protections: Device cloning

USB Standard Descriptor & USB HID Report Descriptors

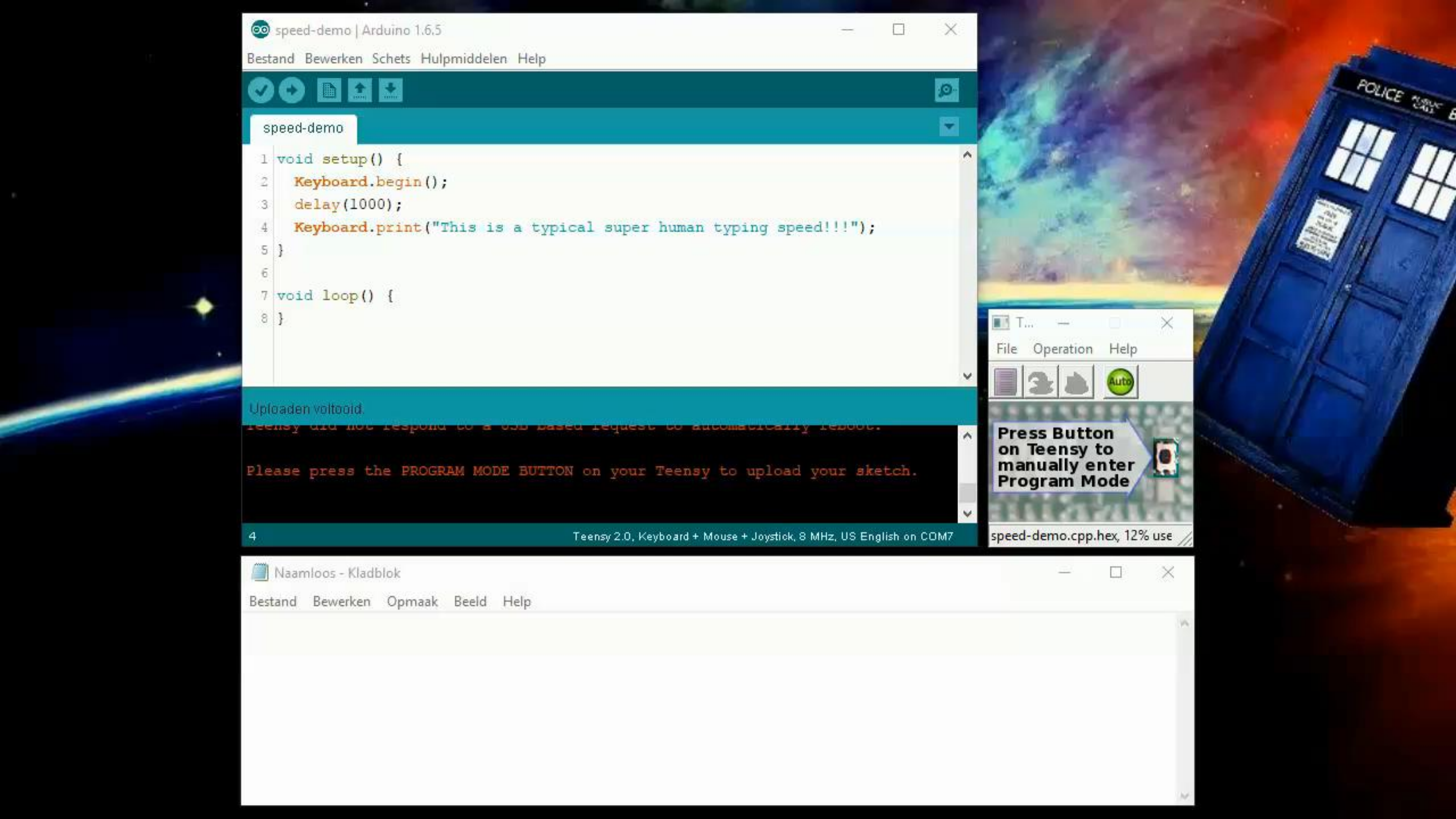


```
[ xxxx.xxxxxx] usb 3-2: new low-speed USB device number 2 using xhci_hcd
[ xxxx.xxxxxx] usb 3-2: New USB device found, idVendor=03f0, idProduct=034a
[ xxxx.xxxxxx] usb 3-2: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[ xxxx.xxxxxx] usb 3-2: Product: HP Elite USB Keyboard
[ xxxx.xxxxxx] usb 3-2: Manufacturer: Chicony
[ xxxx.xxxxxx] usb 3-2: ep 0x81 - rounding interval to 64 microframes, ep desc says 80 microframes
[ xxxx.xxxxxx] usb 3-2: ep 0x82 - rounding interval to 64 microframes, ep desc says 80 microframes
[ xxxx.xxxxxx] input: Chicony HP Elite USB Keyboard as /devices/pci0000:00/0000:00:14.0/usb3/3-2/3
[ xxxx.xxxxxx] hid-generic 0003:03F0:034A.0001: input,hidraw0: USB HID v1.10 Keyboard [Chicony HP
[ xxxx.xxxxxx] input: Chicony HP Elite USB Keyboard as /devices/pci0000:00/0000:00:14.0/usb3/3-2/3
[ xxxx.xxxxxx] hid-generic 0003:03F0:034A.0002: input,hidraw1: USB HID v1.10 Device [Chicony HP El

+--103 lines: Bus 003 Device 002: ID 03f0:034a Hewlett-Packard -----------------------------------
        bEndpointAddress     0x81  EP 1 IN
        bmAttributes            3
          Transfer Type            Interrupt
          Synch Type               None
          Usage Type               Data
        wMaxPacketSize     0x0008  1x 8 bytes
        bInterval              10
      Interface Descriptor:
        bLength                 9
        bDescriptorType         4
        bInterfaceNumber        1
        bAlternateSetting       0
        bNumEndpoints           1
+-- 67 lines: bInterfaceClass         3 Human Interface Device-----------------------------------
```

```
[ xxxx.xxxxxx] usb 3-2: new full-speed USB device number 2 using xhci_
[ xxxx.xxxxxx] usb 3-2: New USB device found, idVendor=03f0, idProduct=
[ xxxx.xxxxxx] usb 3-2: New USB device strings: Mfr=1, Product=2, Seria
[ xxxx.xxxxxx] usb 3-2: Product: HP Elite USB Keyboard
[ xxxx.xxxxxx] usb 3-2: Manufacturer: Chicony
-----------------------------------------------------------------------
[ xxxx.xxxxxx] usb 3-2: ep 0x82 - rounding interval to 64 microframes,
[ xxxx.xxxxxx] input: Chicony HP Elite USB Keyboard as /devices/pci0000
[ xxxx.xxxxxx] hid-generic 0003:03F0:034A.0001: input,hidraw0: USB HID
[ xxxx.xxxxxx] input: Chicony HP Elite USB Keyboard as /devices/pci0000
[ xxxx.xxxxxx] hid-generic 0003:03F0:034A.0002: input,hidraw1: USB HID

+--103 lines: Bus 003 Device 002: ID 03f0:034a Hewlett-Packard --------
        bEndpointAddress     0x81  EP 1 IN
        bmAttributes            3
          Transfer Type            Interrupt
          Synch Type               None
          Usage Type               Data
        wMaxPacketSize     0x0008  1x 8 bytes
        bInterval               1
      Interface Descriptor:
        bLength                 9
        bDescriptorType         4
        bInterfaceNumber        1
        bAlternateSetting       0
        bNumEndpoints           1
+-- 67 lines: bInterfaceClass         3 Human Interface Device---------
```

Bypassing protections: Human emulation

```
//Add random delays to avoid detection
int r = rand() % 111;
r += 8;
delay(r);
```


speed-demo | Arduino 1.6.5
Bestand Bewerken Schets Hulpmiddelen Help
speed-demo
T...
File Operation Help
Auto
Naamloos - Kladblok
Bestand Bewerken Opmaak Beeld Help
POLICE PUBLIC CALL BOX

```
void setup() {
  Keyboard.begin();
  delay(1000);
  Keyboard.print("This is a typical super human typing speed!!!");
}

void loop() {
}
```

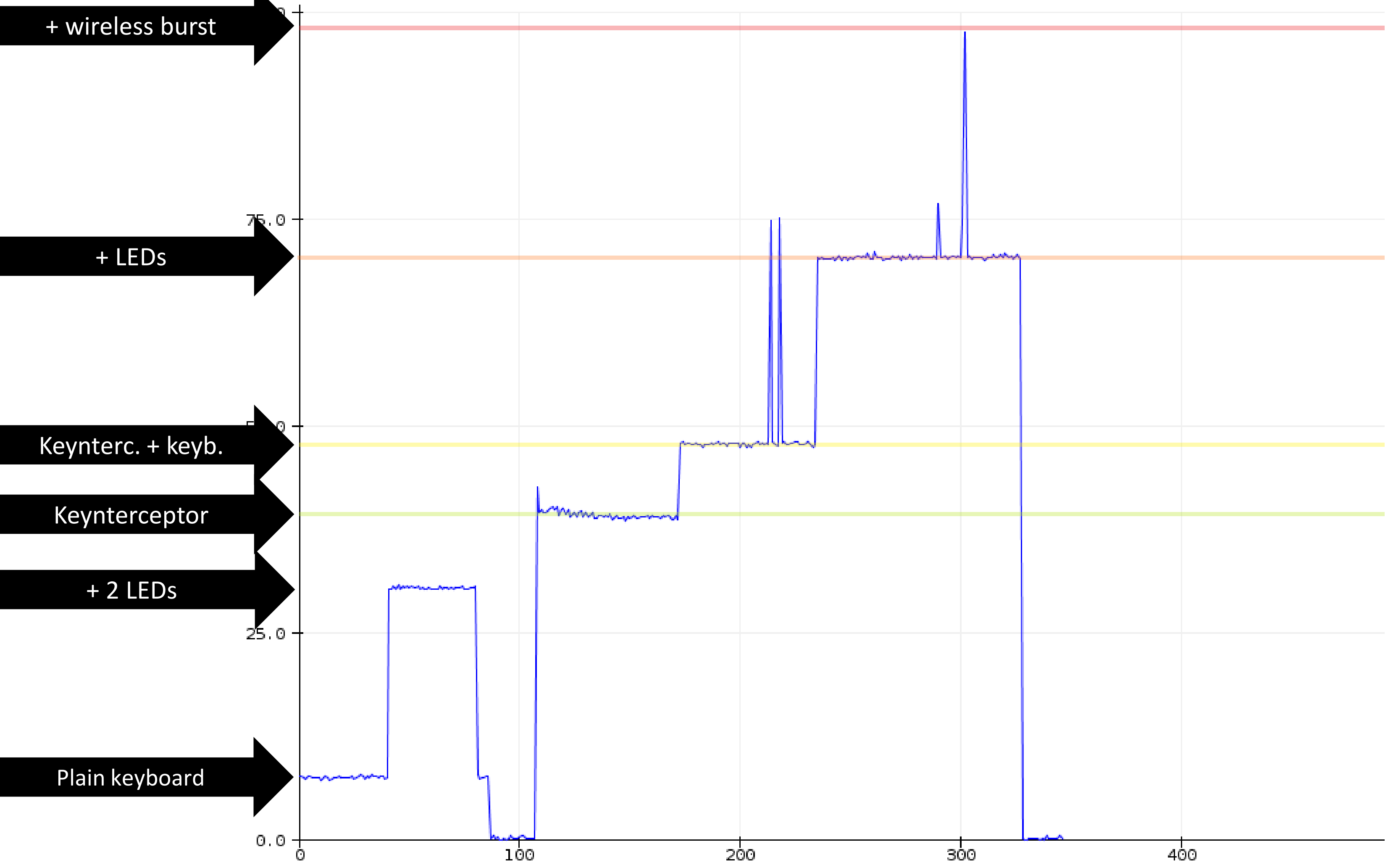
Uploaden voltooid.

```
Teensy did not respond to a USB-based request to automatically reboot.

Please press the PROGRAM MODE BUTTON on your Teensy to upload your sketch.
```

4 Teensy 2.0, Keyboard + Mouse + Joystick, 8 MHz, US English on COM7

Press Button on Teensy to manually enter Program Mode

speed-demo.cpp.hex, 12% use



+ wireless burst

+ LEDs

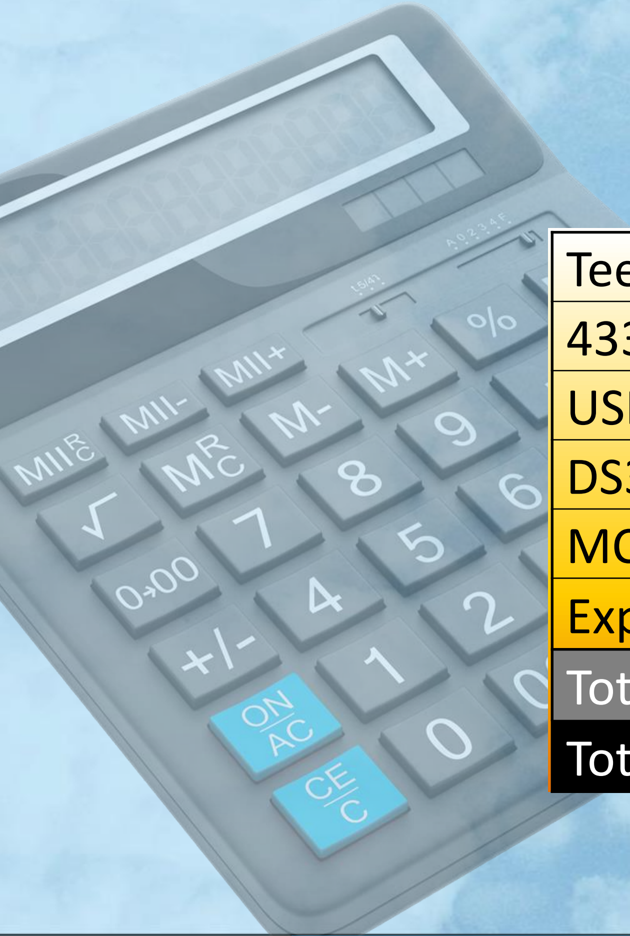
Keynterc. + keyb.

Keynterceptor

+ 2 LEDs

Plain keyboard

BOM / Costs



Teensy 2.0	$ 16,00
433 MHz module	$ 4,00
USB Host module	$ 8,00
DS3231 RTC	$ 4,00
MCP1825S regulator	$ 1,00
Exp. print / LEDs / resistors	$ 2,00
Total in US Dollars:	$ 35,00
Total in Euro's:	€ 30,00

Use-Cases

a. Control keyboard remotely OTA

b. Autologin with captured creds

c. Inject keystrokes after inactivity with chosen time-frame

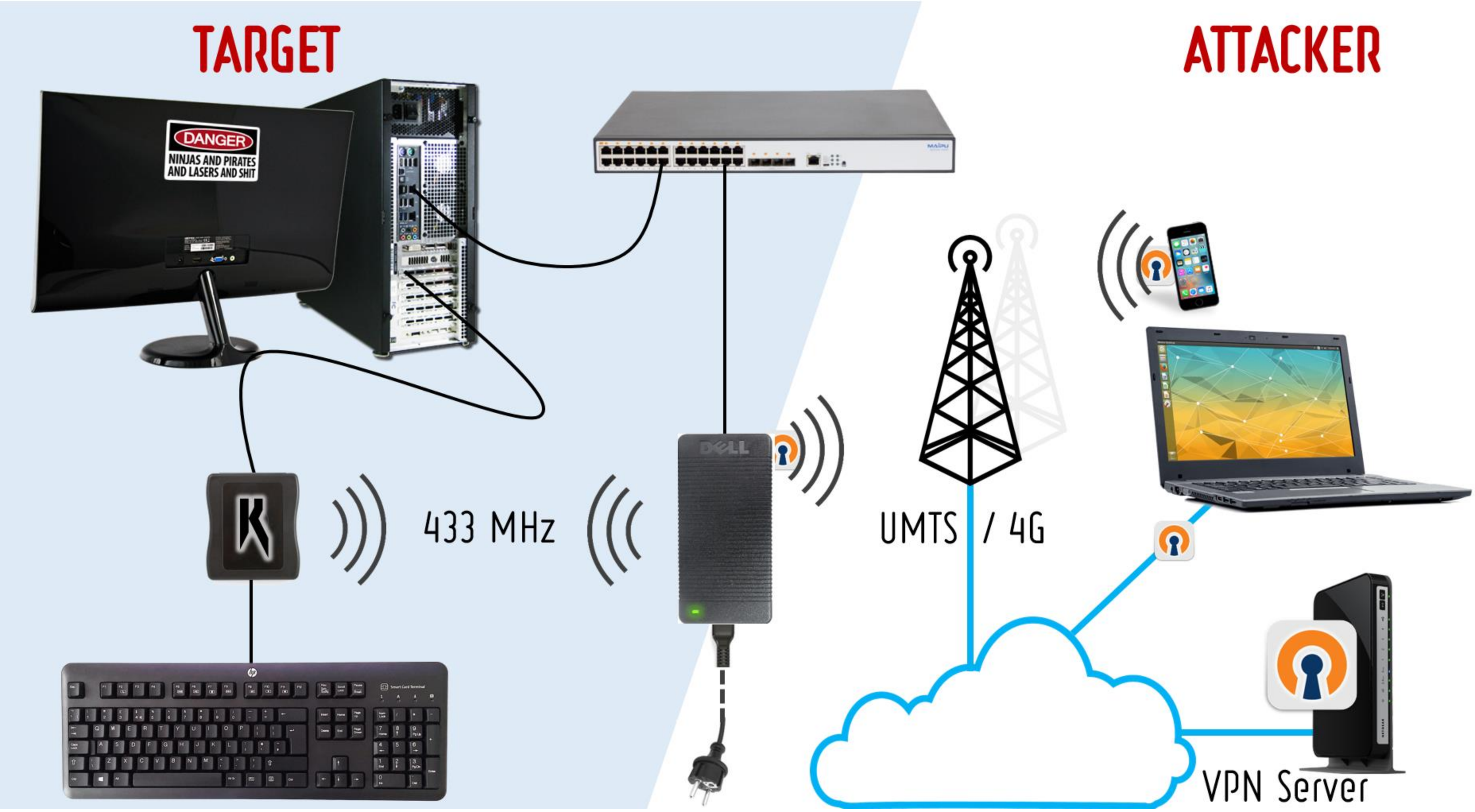
d. Block user input with RF kill-switch (for a take-down)

e. <<*insert scenario here*>>

Add-on for a full attack scenario

Keynterceptor-Companion:

- Nanopi Neo
- 433 MHz
- 4G dongle


TARGET
ATTACKER
DANGER
NINJAS AND PIRATES AND LASERS AND SHIT
433 MHz
UMTS / 4G
VPN Server

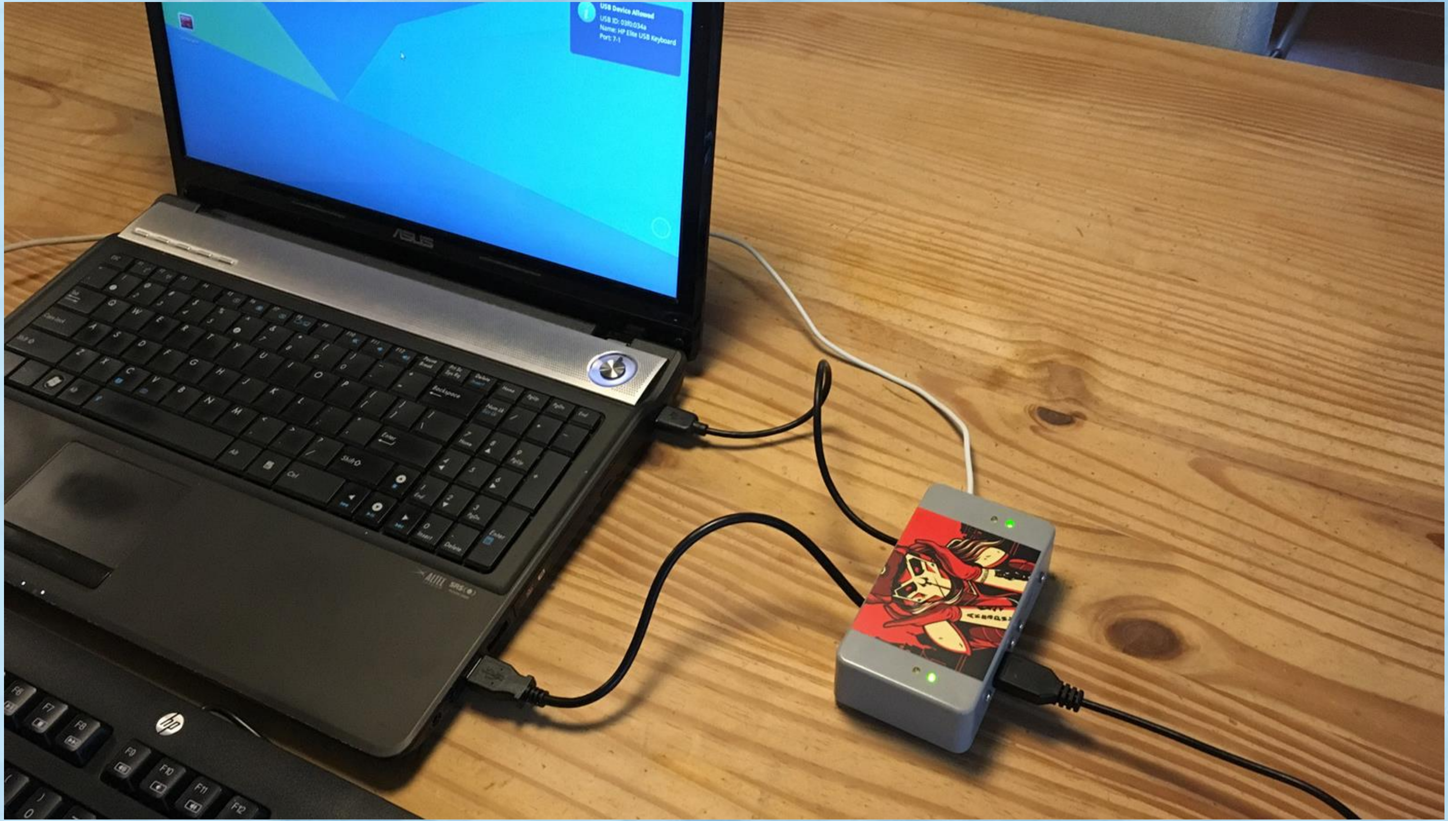
DEMO-Time...

New mitigations?

a. Multi-factor or challenge-response (like captcha's) with every unlocking action ✓

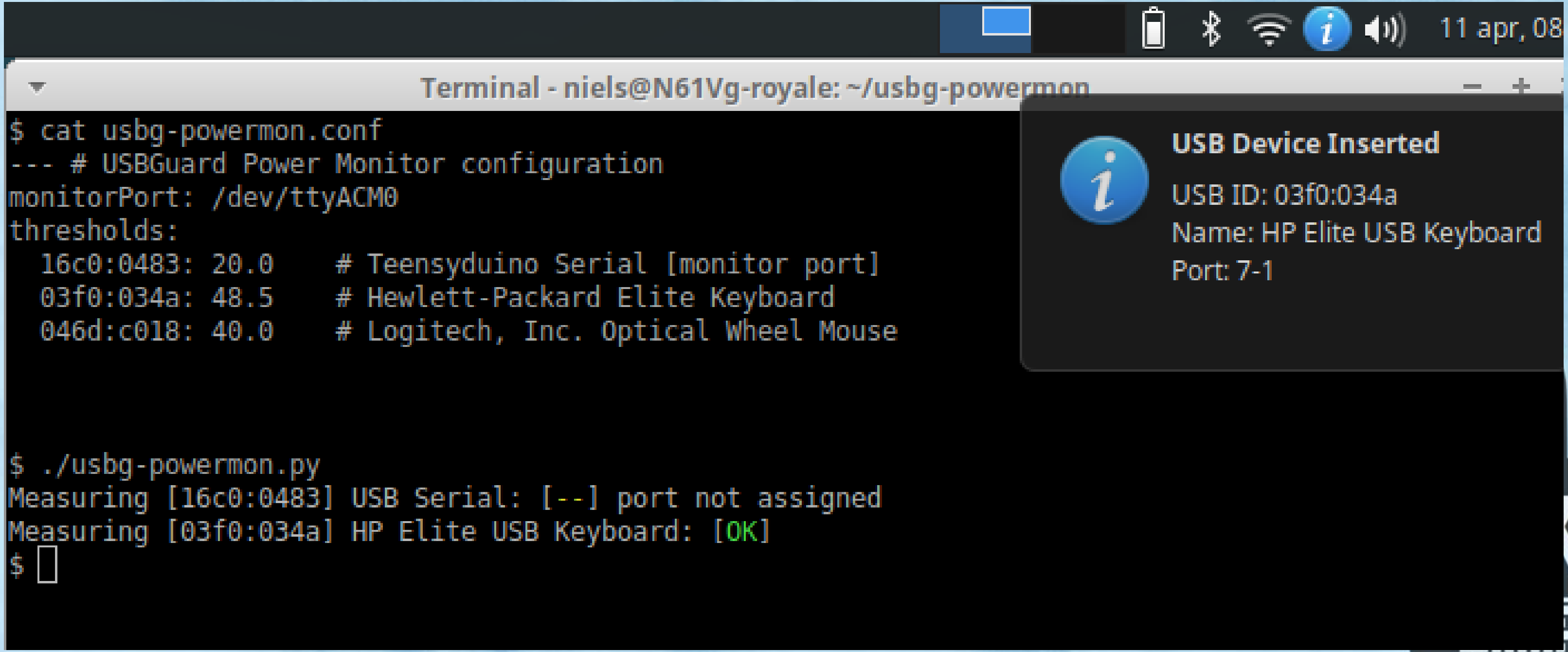
b. Profiling / monitoring power consumption per device *(HW support is problematic)*

USBGuard + power profiling PoC



USB Device Allowed
USB ID: 03f0:034a
Name: HP Elite USB Keyboard
Port: 7-1

USBGuard + power profiling PoC



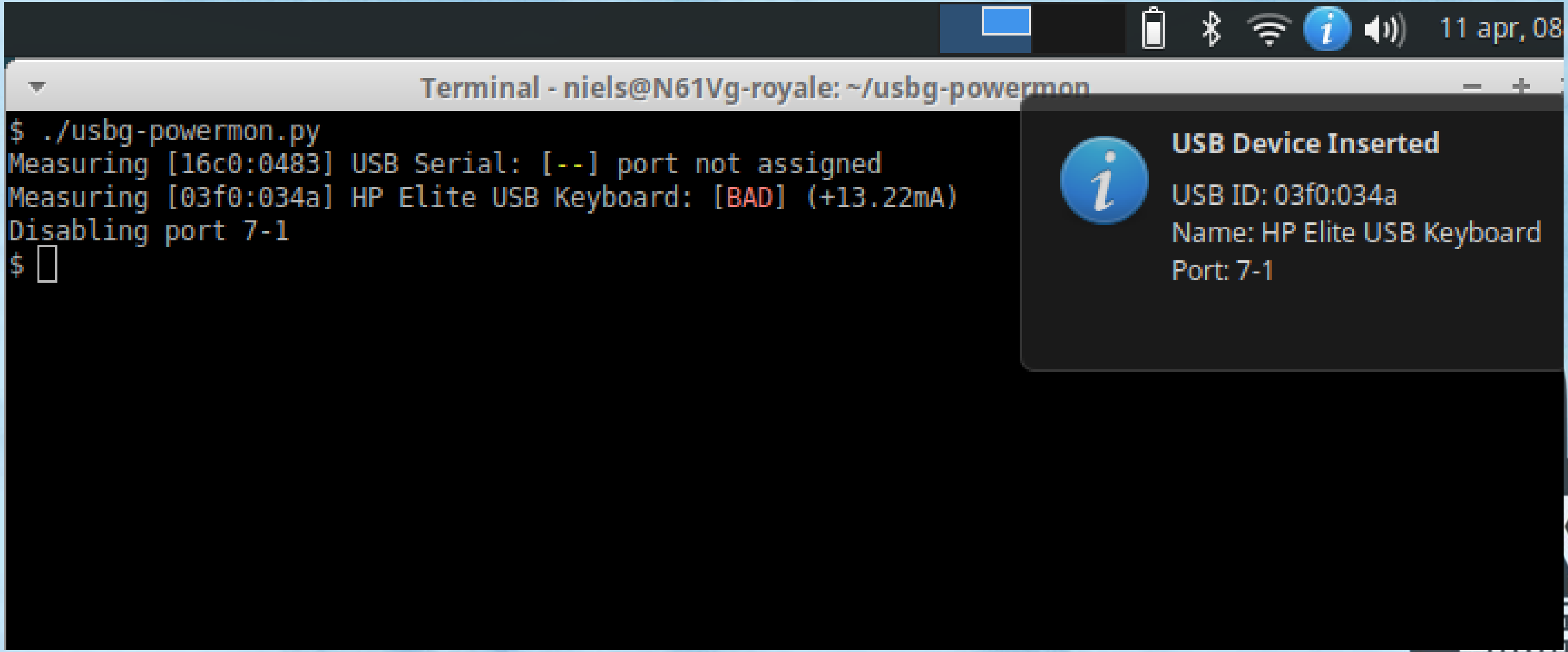
```
$ cat usbg-powermon.conf
--- # USBGuard Power Monitor configuration
monitorPort: /dev/ttyACM0
thresholds:
  16c0:0483: 20.0    # Teensyduino Serial [monitor port]
  03f0:034a: 48.5    # Hewlett-Packard Elite Keyboard
  046d:c018: 40.0    # Logitech, Inc. Optical Wheel Mouse


$ ./usbg-powermon.py
Measuring [16c0:0483] USB Serial: [--] port not assigned
Measuring [03f0:034a] HP Elite USB Keyboard: [OK]
$ 
```

USB Device Inserted

USB ID: 03f0:034a
Name: HP Elite USB Keyboard
Port: 7-1

USBGuard + power profiling PoC

USBGuard + power profiling PoC



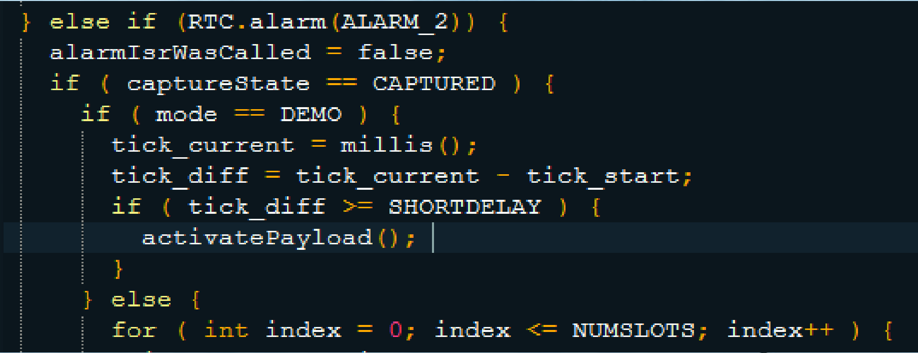
```
$ ./usbg-powermon.py
Measuring [16c0:0483] USB Serial: [--] port not assigned
Measuring [03f0:034a] HP Elite USB Keyboard: [BAD] (+13.22mA)
Disabling port 7-1
$ 
```

USB Device Inserted

USB ID: 03f0:034a
Name: HP Elite USB Keyboard
Port: 7-1

Keynterceptor attack feasible?

- *430 lines of C code*
- *85 lines of Python code*
- *301 lines of Perl code*
- *some development euro's*



```
} else if (RTC.alarm(ALARM_2)) {
  alarmIsrWasCalled = false;
  if ( captureState == CAPTURED ) {
    if ( mode == DEMO ) {
      tick_current = millis();
      tick_diff = tick_current - tick_start;
      if ( tick_diff >= SHORTDELAY ) {
        activatePayload();
      }
    } else {
      for ( int index = 0; index <= NUMSLOTS; index++ ) {
```

Future work?

- Fit it inside real hardware
- Have automatic descriptor cloning
- Encrypt covert OTA communication channel

?