USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs

Yang Su
University of Adelaide

joint work with

Daniel Genkin
UPenn and UMD

Damith Ranasinghe
University of Adelaide

Yuval Yarom
University of Adelaide and Data61





UNIVERSITY OF MARYLAND



THE UNIVERSITY of ADELAIDE

Universal Serial Bus (USB)





Version	Year	Speed
USB 1.0	1996	1.5 Mbit/s
USB 1.1	1998	12 Mbit/s
USB 2.0	2000	480 Mbit/s
USB 3.0	2008	5 Gbit/s
USB 3.1	2013	10 Gbit/s

Universal Serial Bus (USB)





Version	Year	Speed
USB 1.0	1996	1.5 Mbit/s
USB 1.1	1998	12 Mbit/s
USB 2.0	2000	480 Mbit/s
USB 3.0	2008	5 Gbit/s
USB 3.1	2013	10 Gbit/s

Today

Most Human Input Devices (HID) are still using USB 1.x





USB Security Features



USB does have some basic routing mechanism, so not all devices see all the traffic

USB Topology

- Downstream data is broadcasted
- Upstream data is unicasted



USB Root Hub

USB Hub



How can we mount off path attack on USB devices?

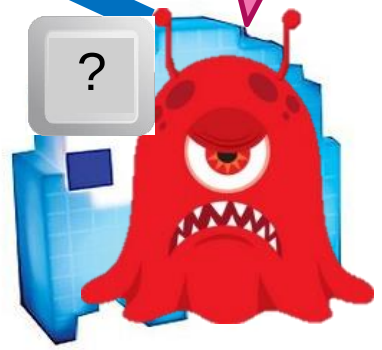












Our Results

- Demonstrate off path attacks on USB devices
  - Human input devices
  - USB storage



- Utilizing crosstalk leakage between adjacent USB ports
  - Analog effects between adjacent USB ports on the same hub
  - Recover signals present on the other port



- Works on internal and external USB hubs
  - 30 out of 34 internal hubs
  - 17 out of 20 external hubs

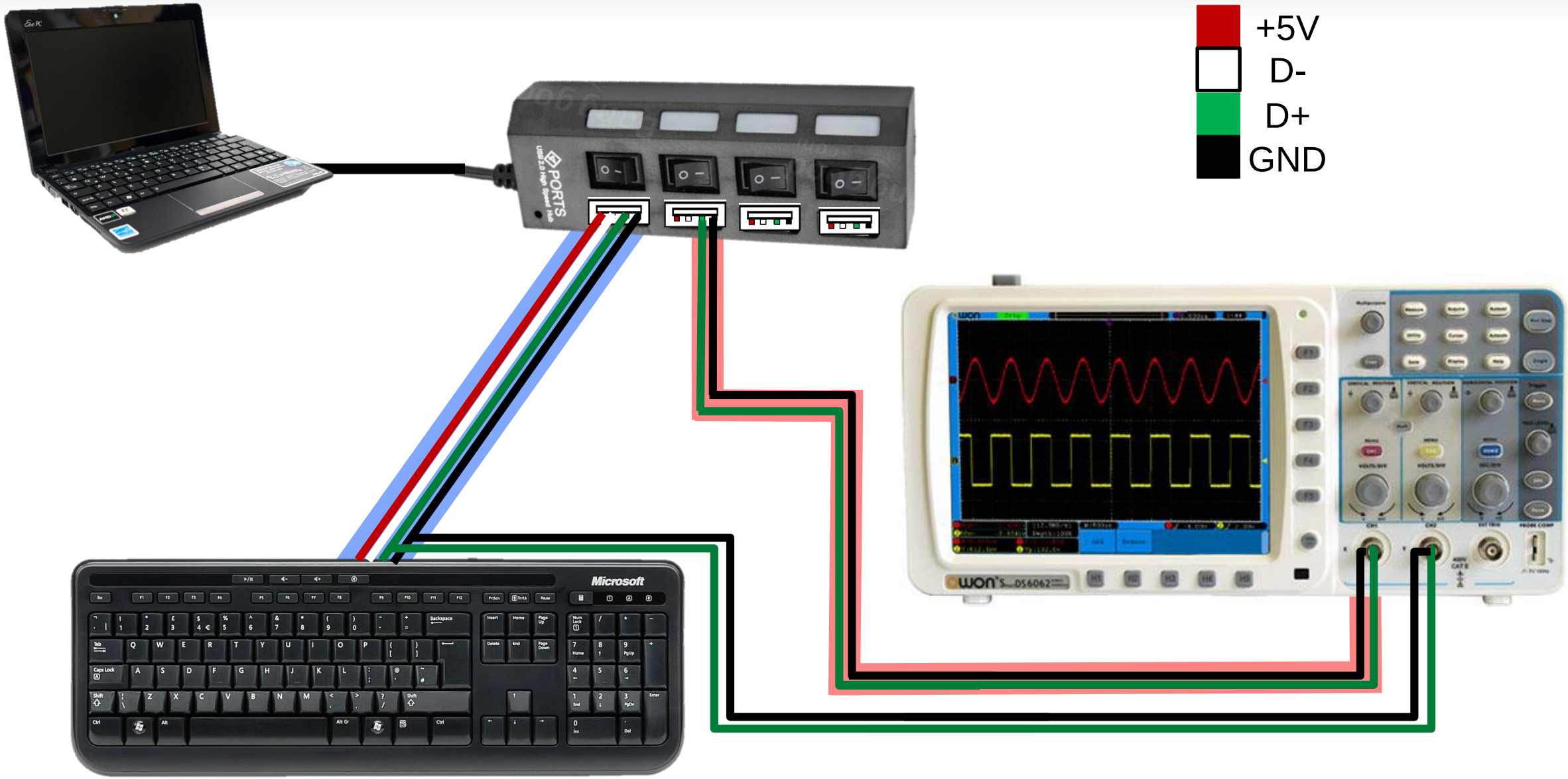




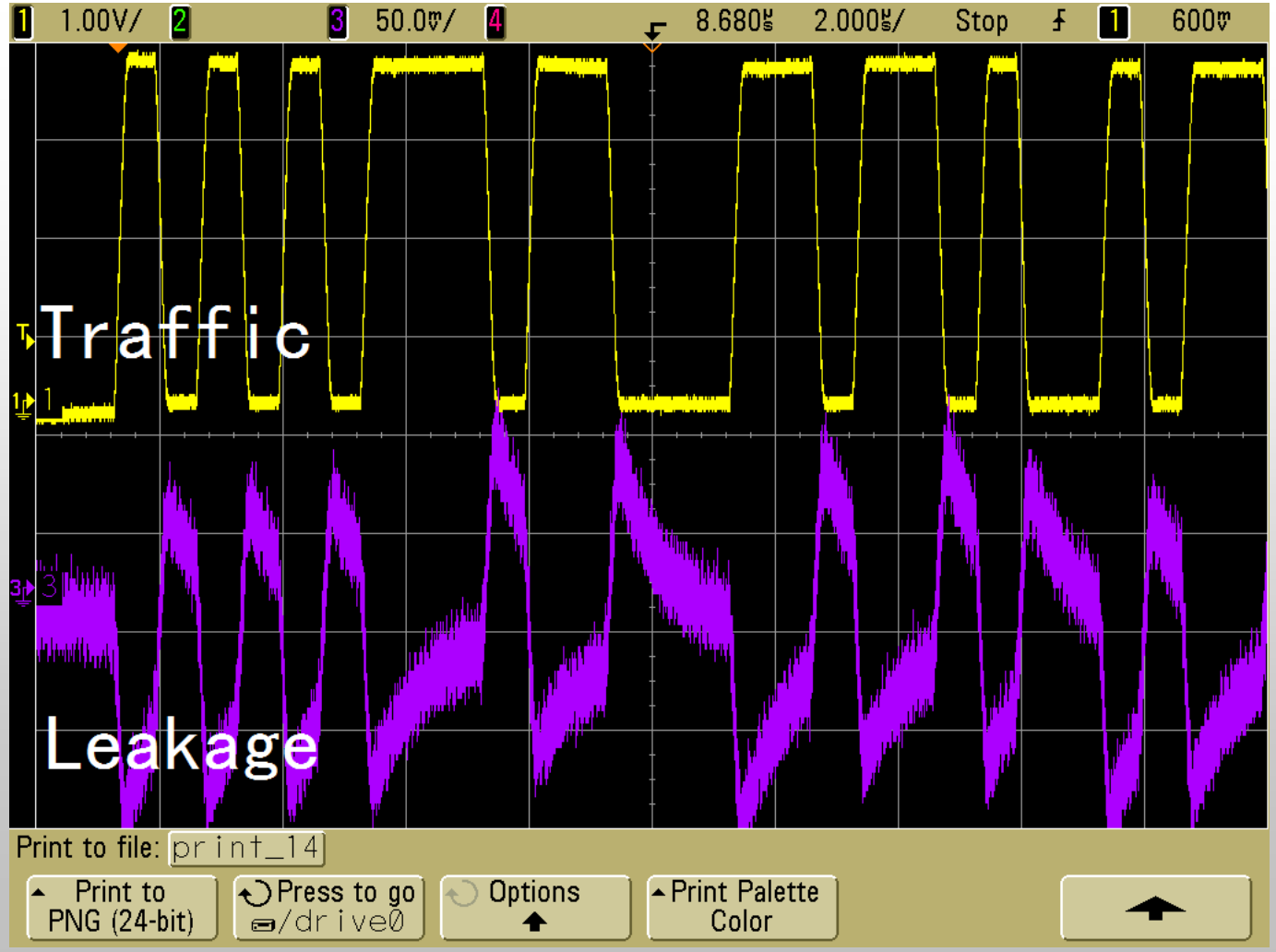
- Leakage is present on both power and data lines
  - Bypassing typical hardware countermeasures such as USB power only cables



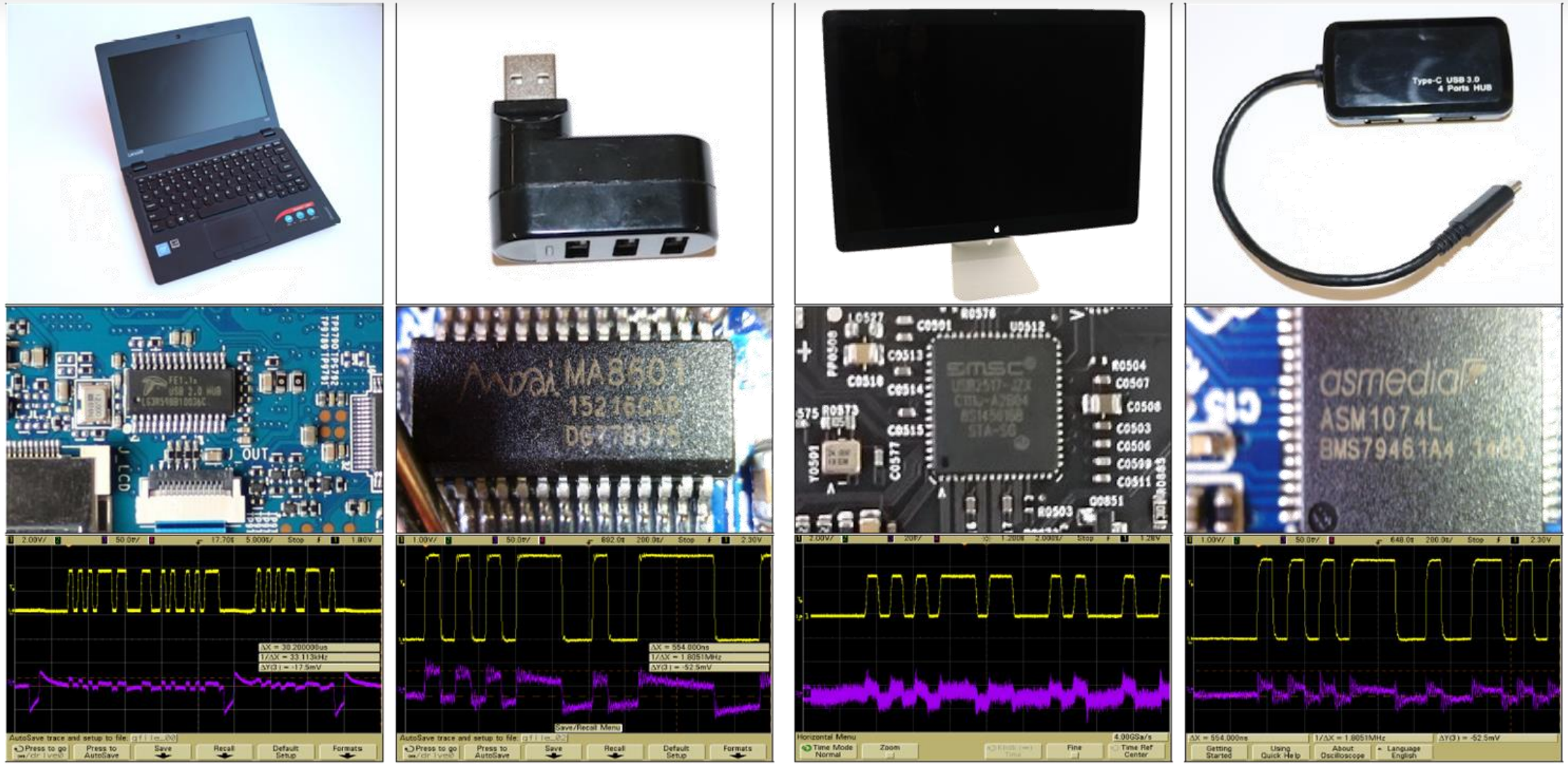
Observing Crosstalk Leakage



Demo: Observing Crosstalk Leakage



Observing Crosstalk Leakage



(a) Terminus Tech FE1.1s (inside a Lenovo 100s laptop)

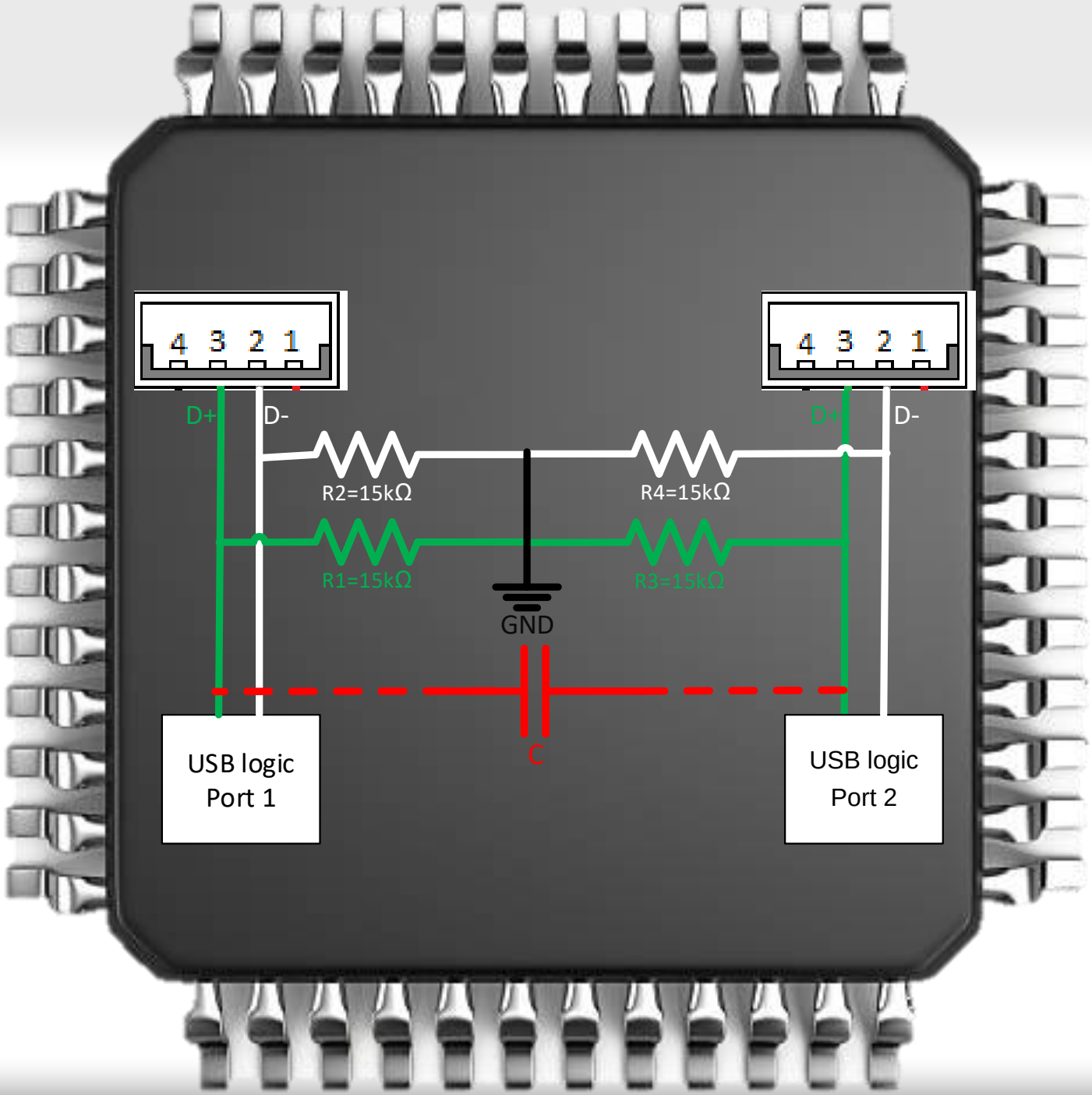
(b) Prolific MA8601

(c) SMSC USB2517-JZX (inside an Apple Display)

(d) ASMedia Technology ASM1074L

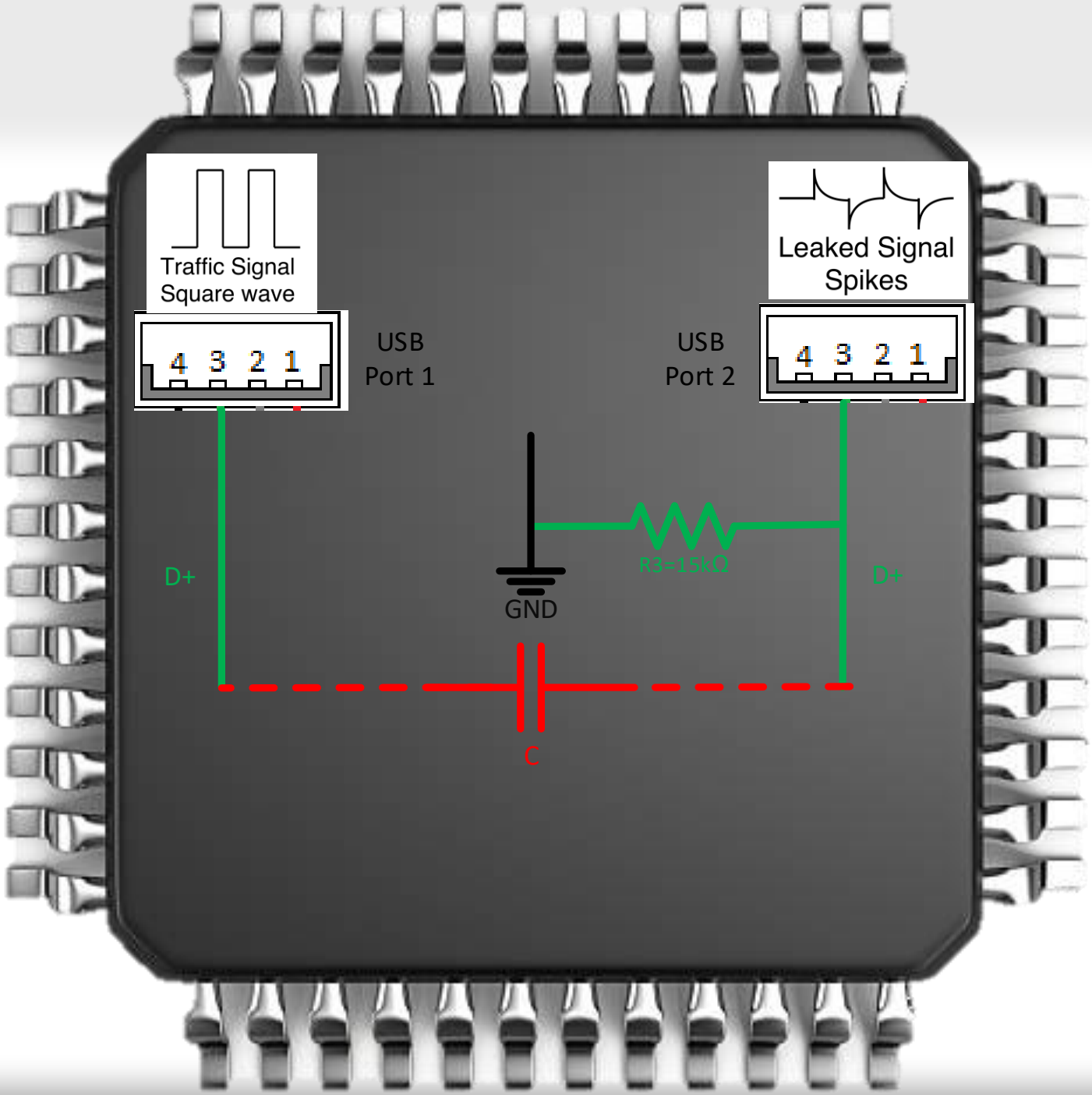
Leakage Mechanism

- USB hubs typically consist of one main chip
- Two USB logic blocks should be isolated from each other
- Due to manufacturing imperfections parasitic capacitance is present between different USB ports on the same chip



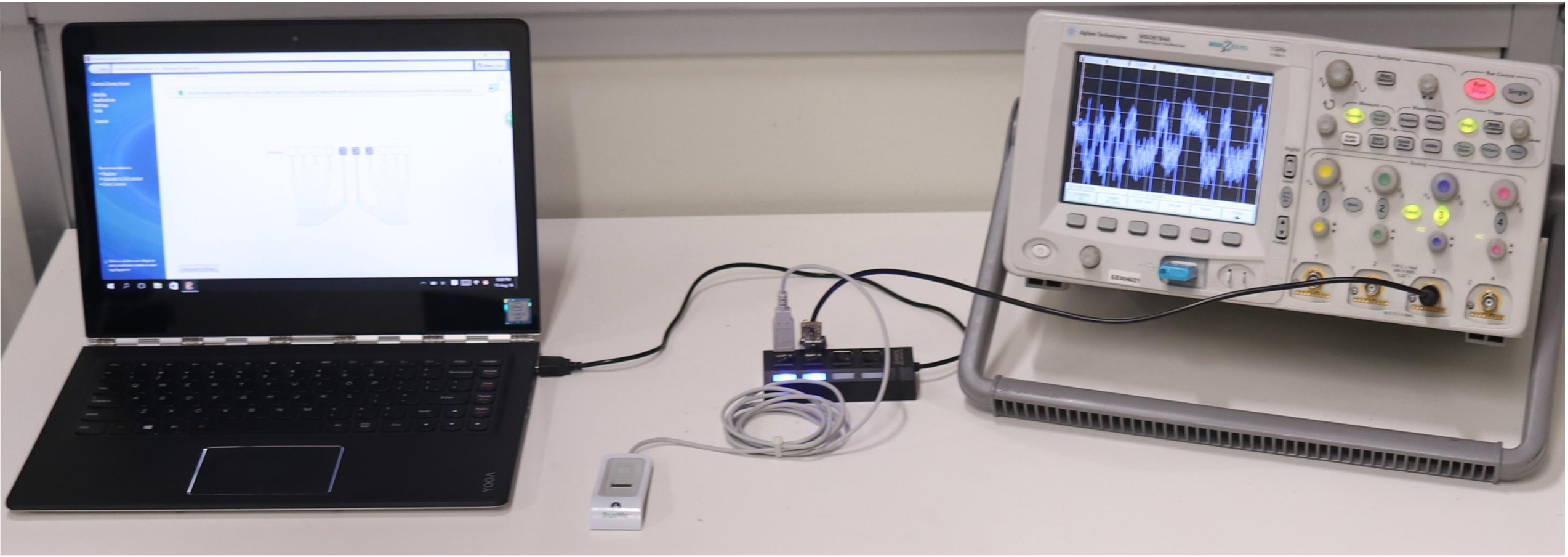
Leakage Mechanism

- USB hubs typically consist of one main chip
- Two USB logic blocks should be isolated from each other
- Due to manufacturing imperfections parasitic capacitance is present between different USB ports on the same chip
- Fluctuations on one port can be visible from other ports



Attacking other devices

USB Fingerprint reader



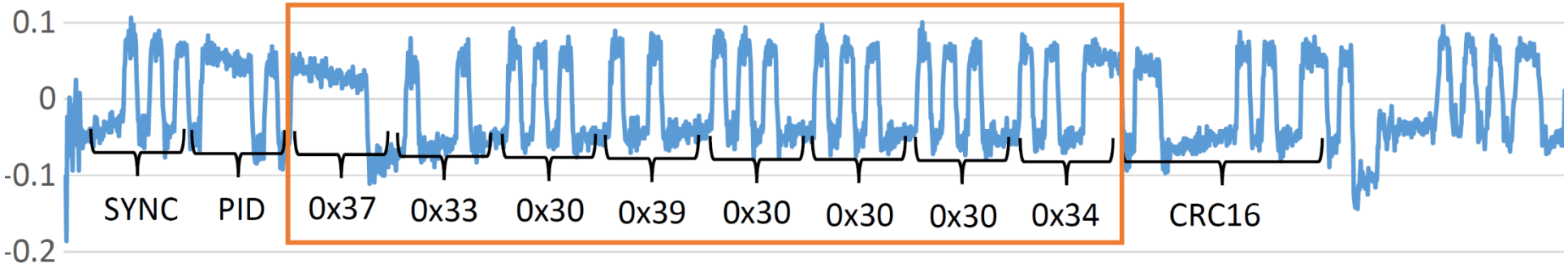
Attacking HID devices

Magnetic card reader



Attacking HID devices

Magnetic card reader



Offset	Hex [005A]	Ascii
00000000	37 33 30 39	7309
0000000F	30 30 30 34	0004
0000001E		
0000002D		
0000003C		
0000004B		
0000005A		
00000069		
00000078	37 33 30 39 30 30 30 34	73090004

Card number and cardholder's name

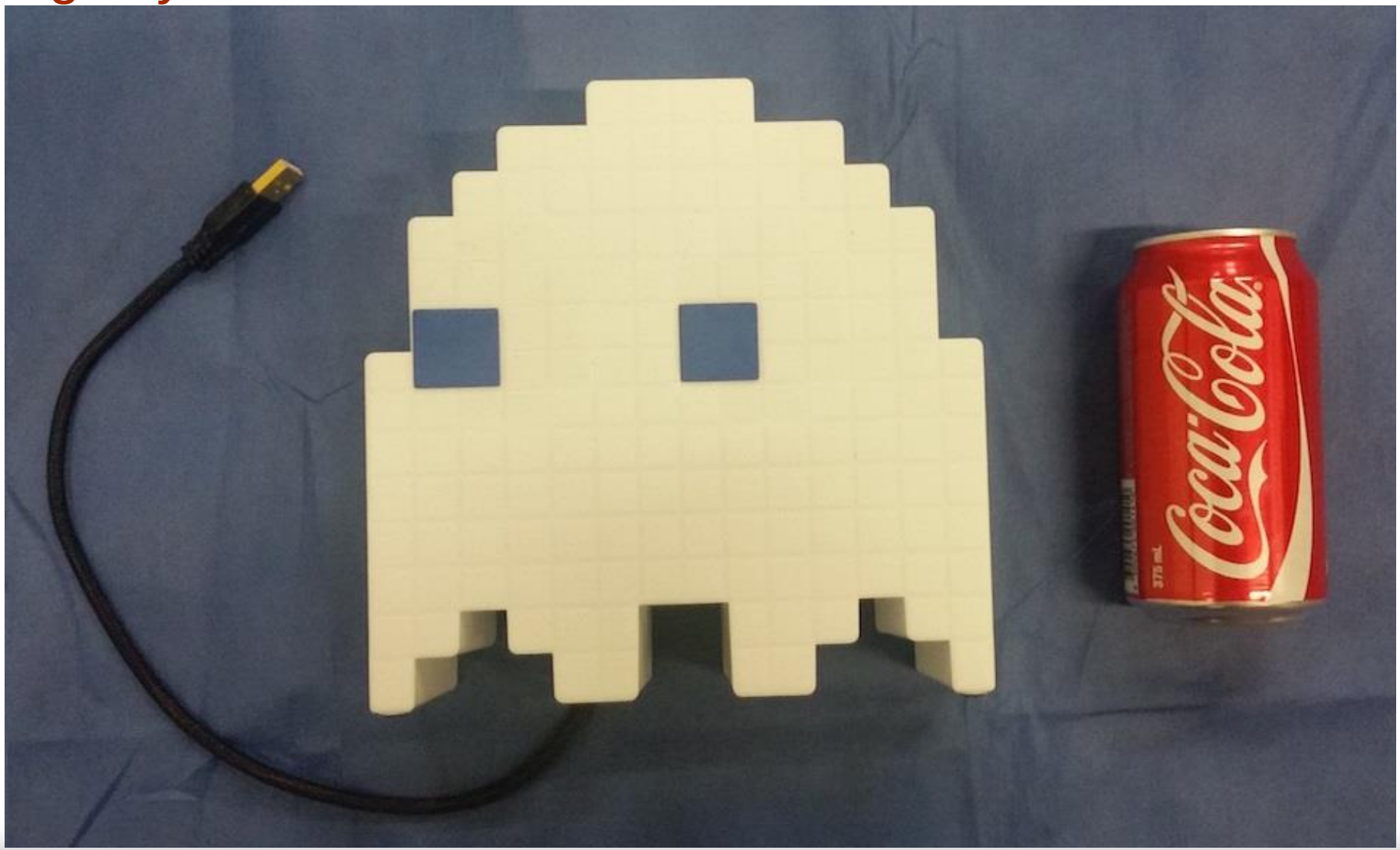
Expiration data, Service code, Discretionary data

Card number



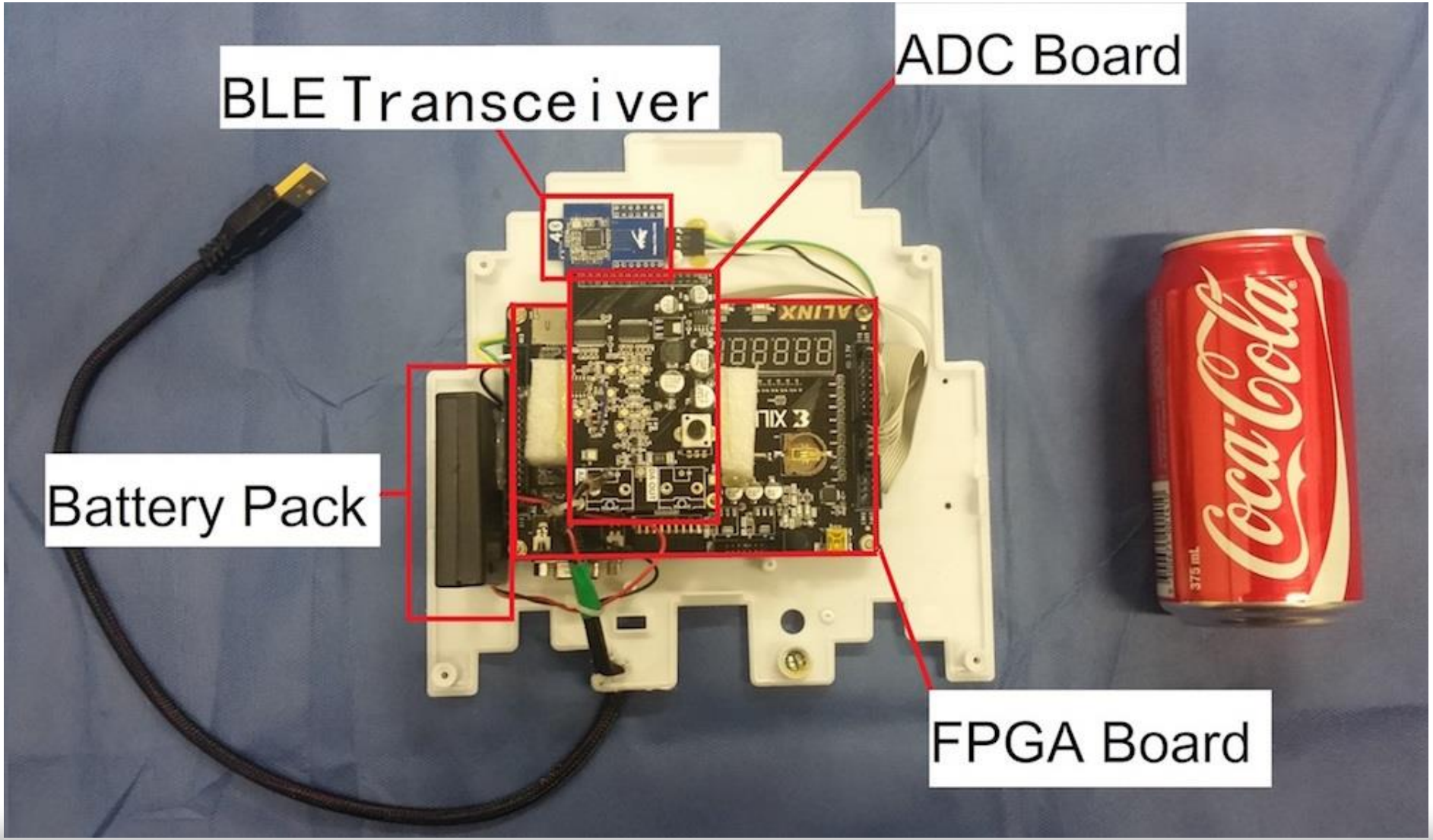
Attacking HID devices

Exfiltrating keystrokes

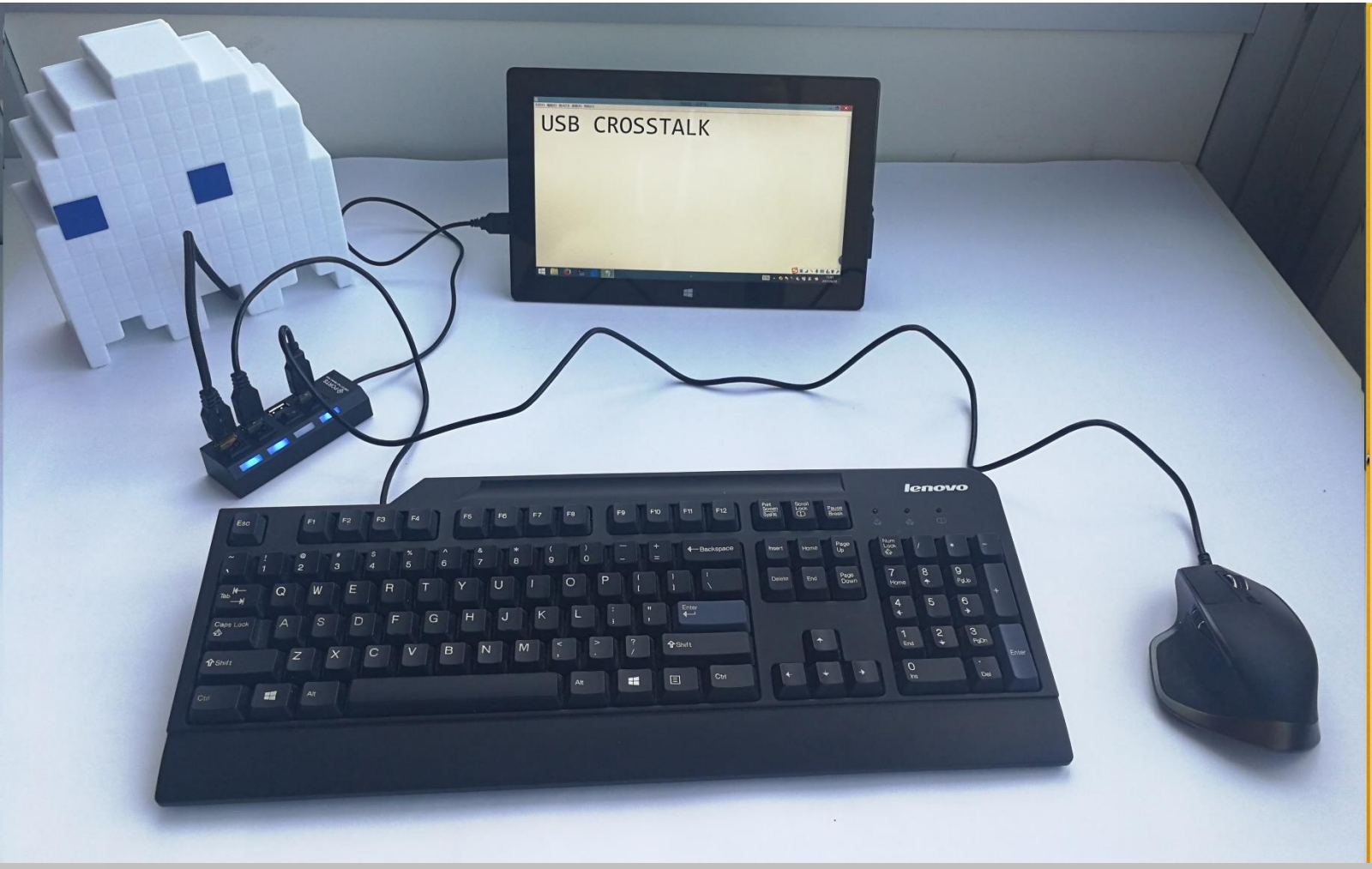


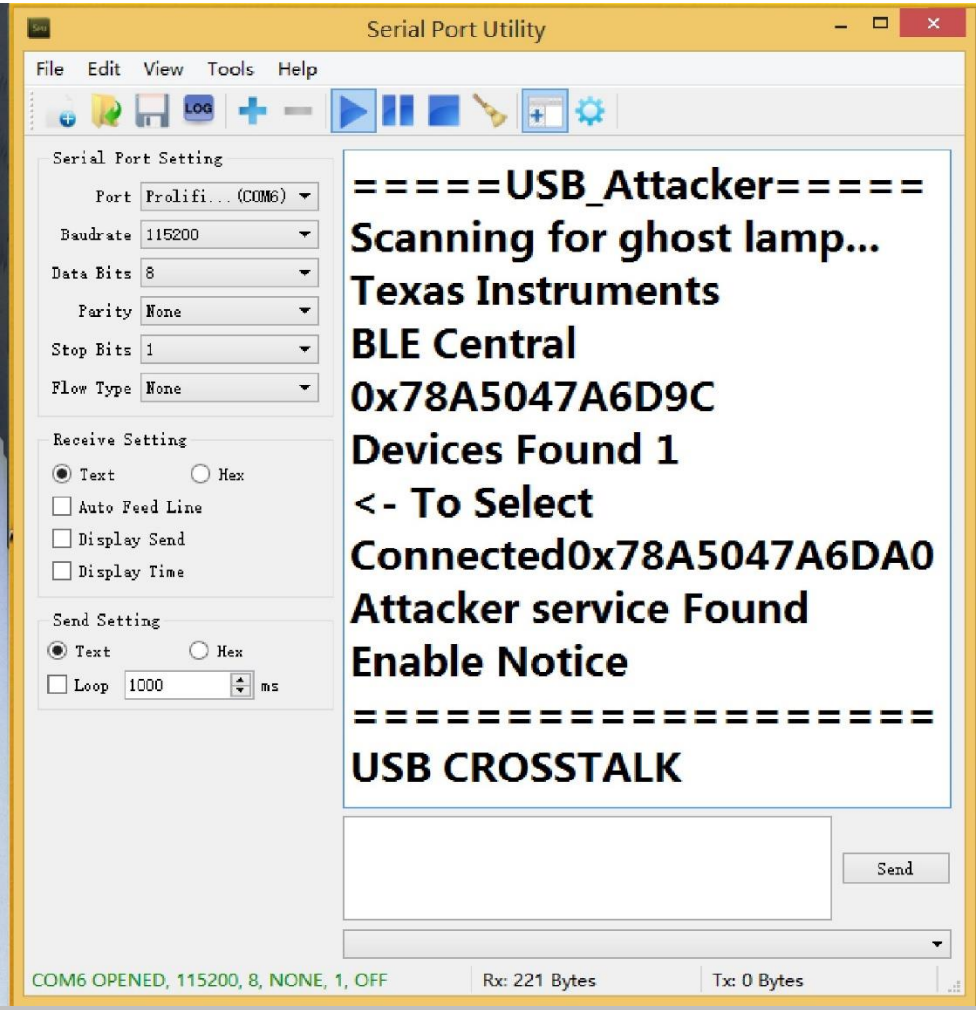
Attacking HID devices

Exfiltrating keystrokes



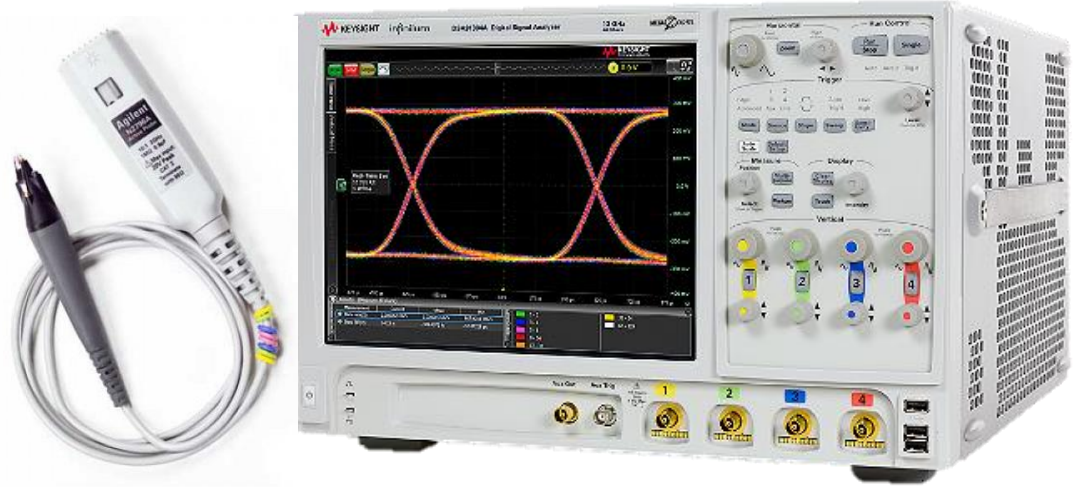
Demo: Keystroke Exfiltration

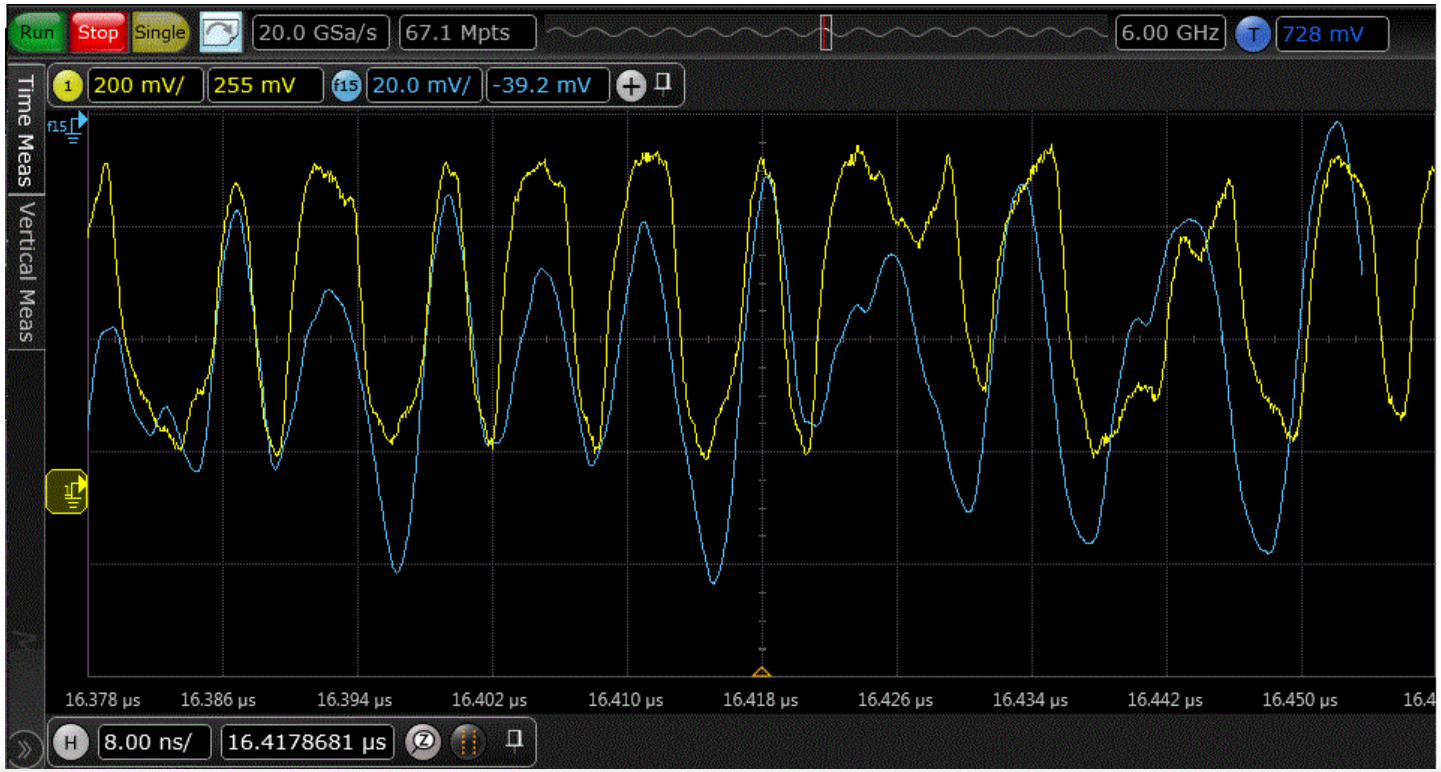




Attacking USB 2.0

- Runs at 480Mbit/sec compared to 1.5 Mbit/sec or USB 1.0
- Uses 0.3V compared to 3.3V for USB 1.0
- Data captured using a 6GHz oscilloscope and active probes

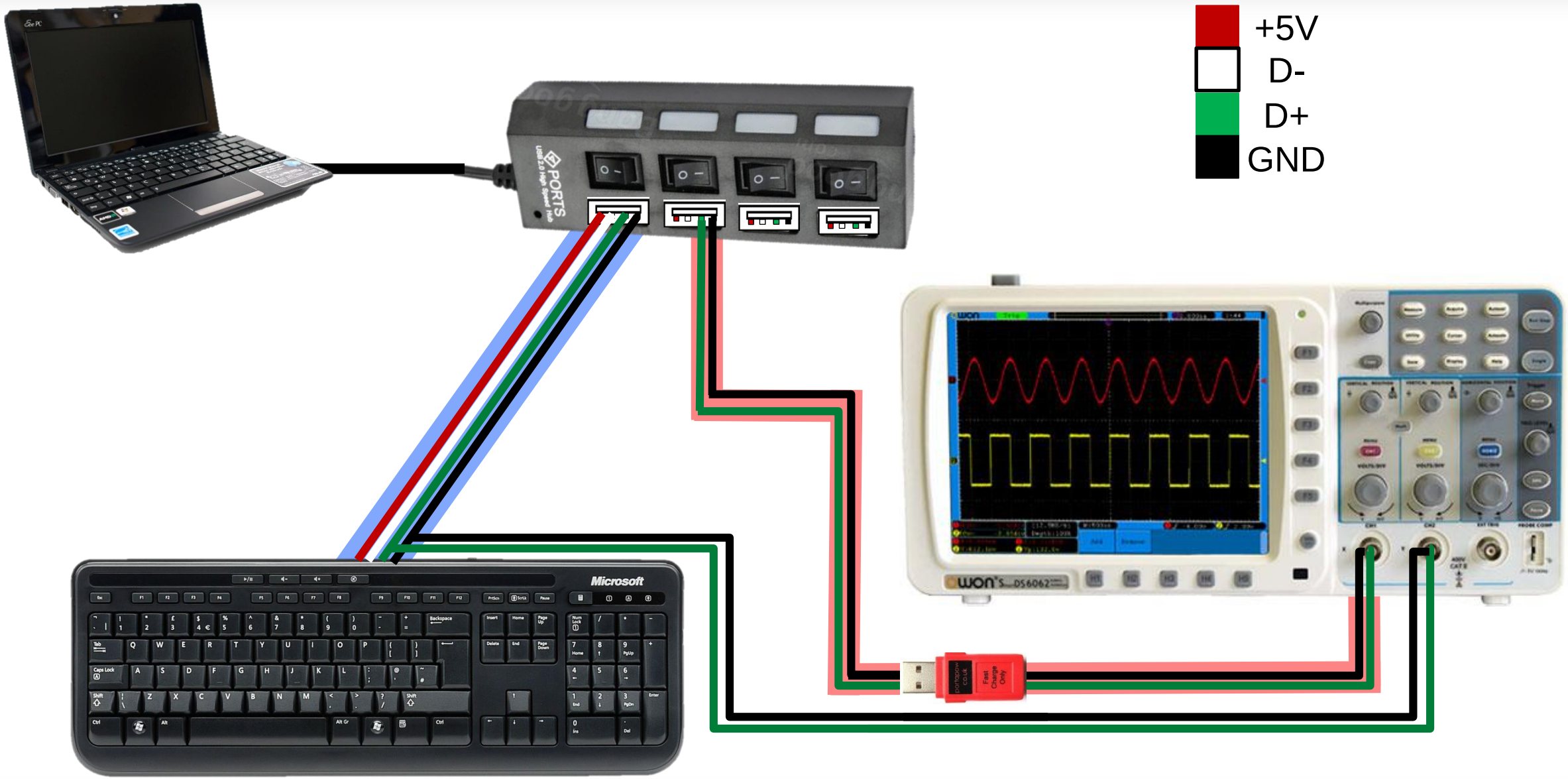




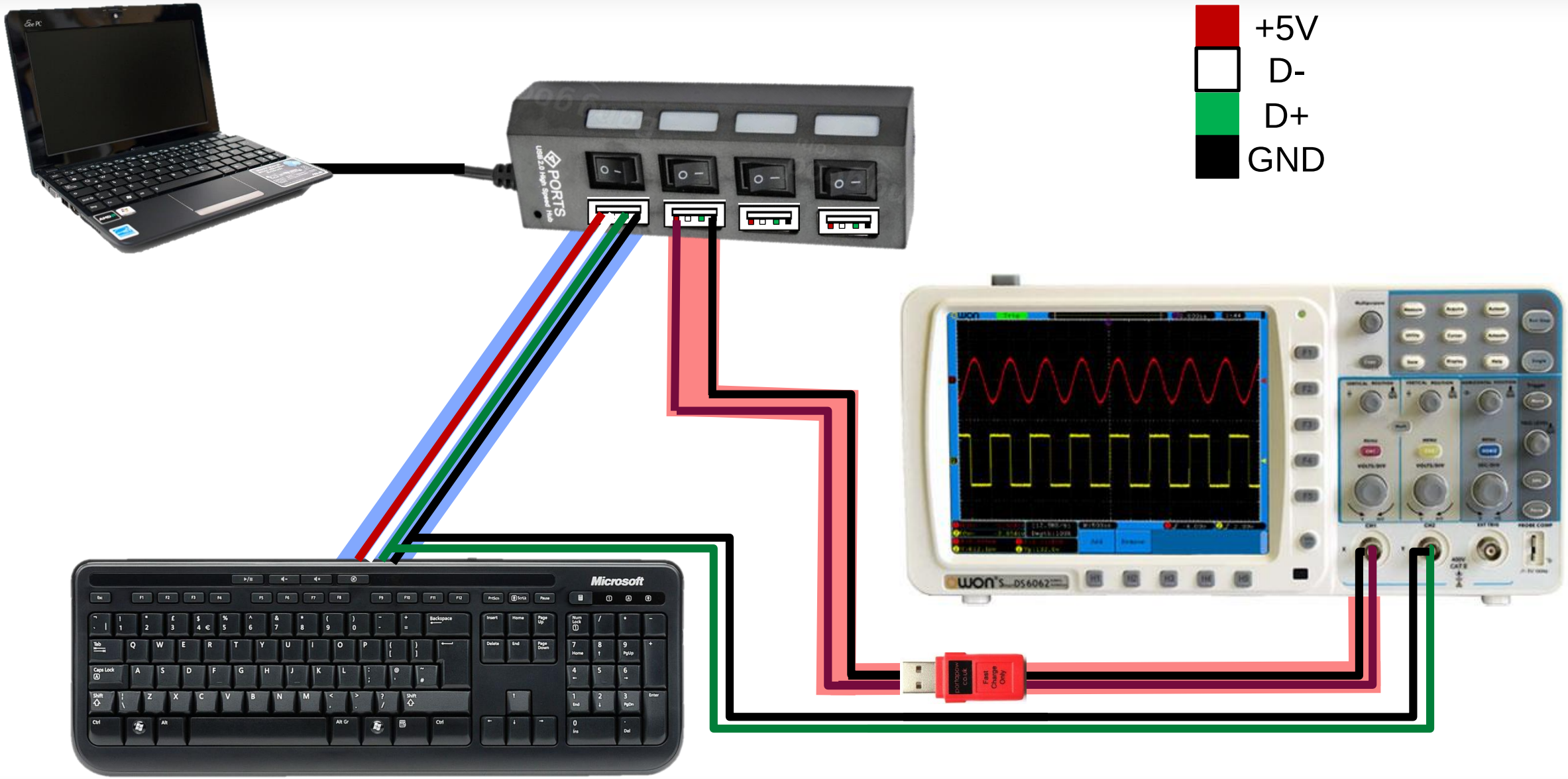
Bypassing power only cables



Observing Crosstalk Leakage

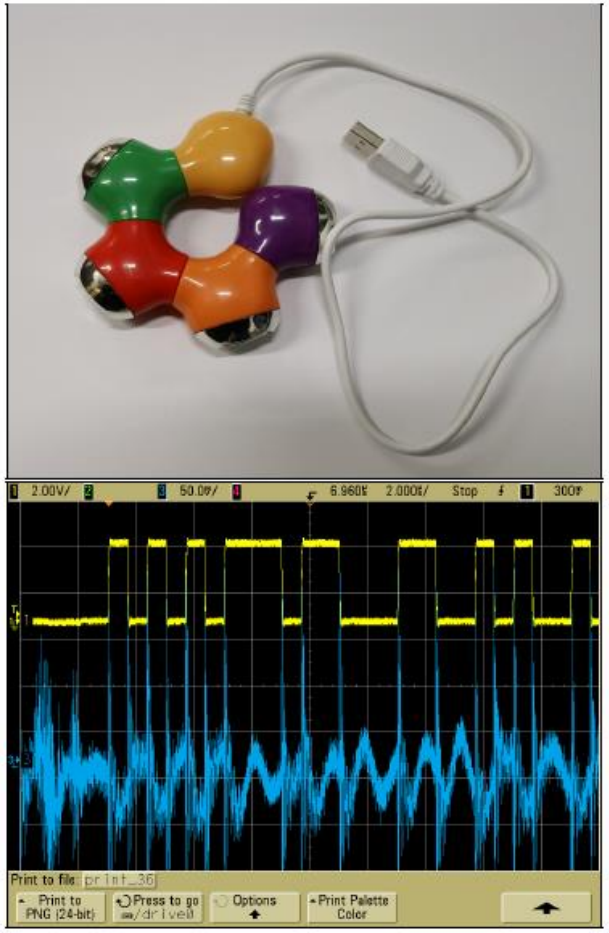


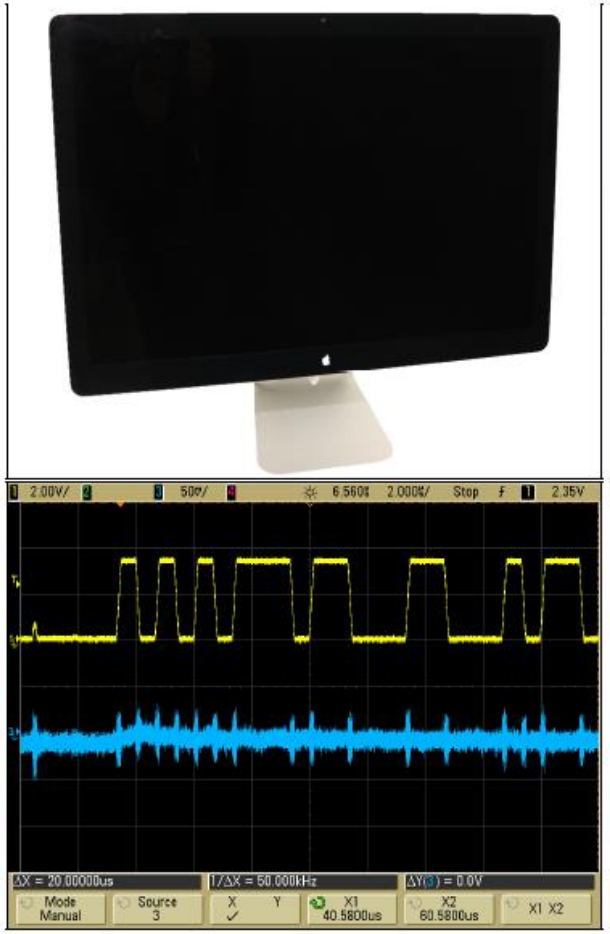
Observing Crosstalk Leakage



Observing Crosstalk Leakage



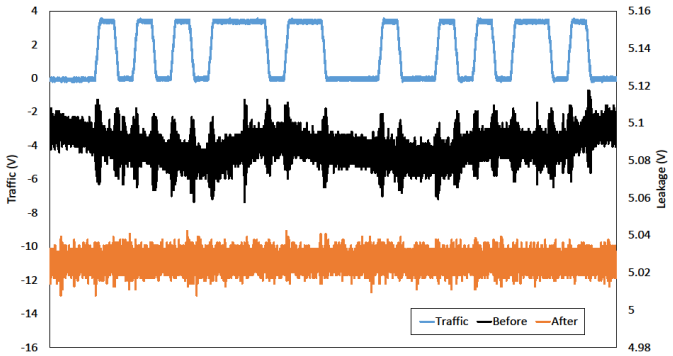


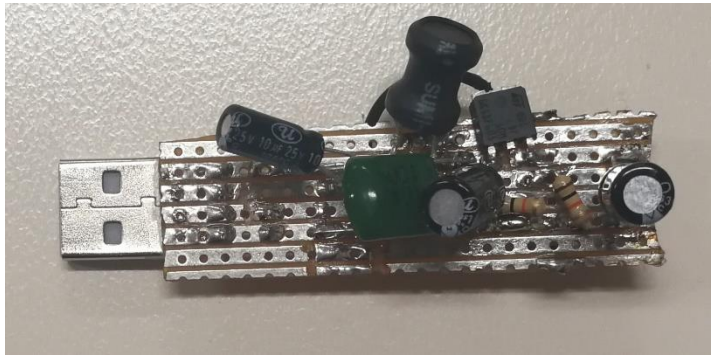




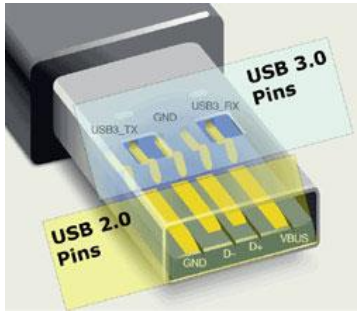
Countermeasures and Future Work

- **Do not plug in what you do not trust**
- Power leakage can be mitigated using voltage regulators while maintaining USB power functionality
- Adding encryption to USB buses





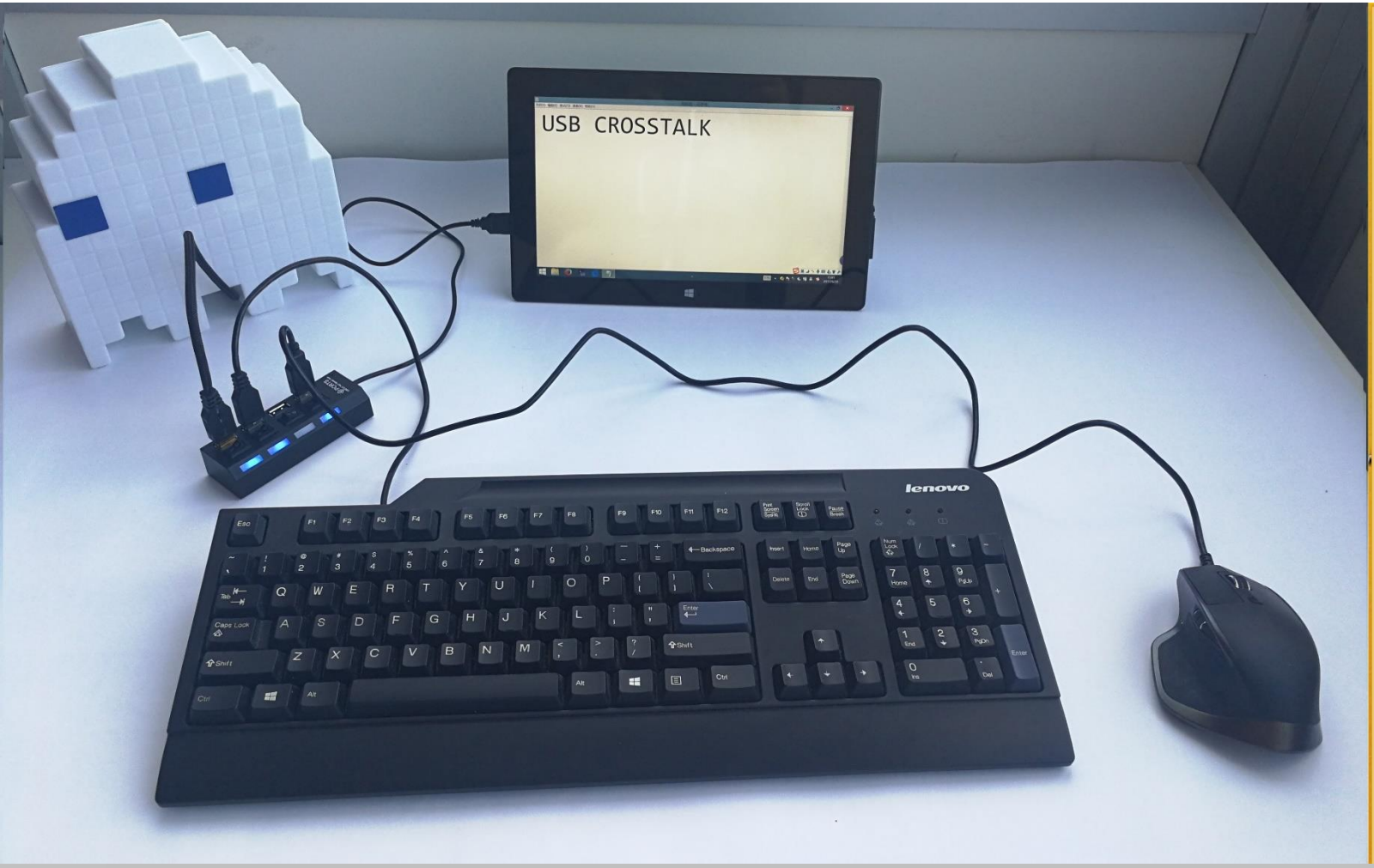
- Attack only works for USB 1.1 and (to some extent) USB 2.0
- Attacks on USB 3.0 and USB C devices remain open
  - Several pairs of data lines, making leakage analysis harder
  - Run at greater speeds, requiring faster equipment to measure
- Other unencrypted buses

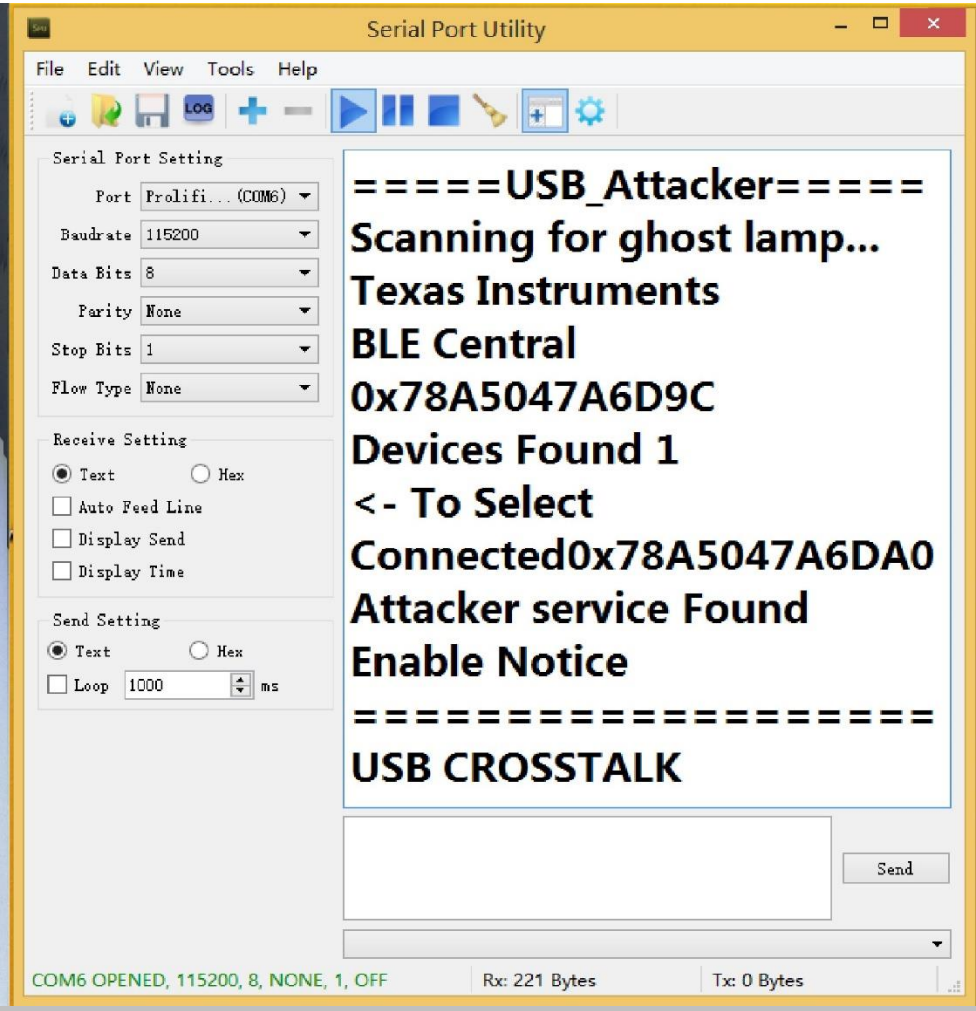




Type-C

Thanks!


USB CROSSTALK
lenovo


Serial Port Utility
File Edit View Tools Help
Serial Port Setting
Port Prolifi...(COM6)
Baudrate 115200
Data Bits 8
Parity None
Stop Bits 1
Flow Type None
Receive Setting
Text Hex
Auto Feed Line
Display Send
Display Time
Send Setting
Text Hex
Loop 1000 ms
=====USB_Attacker=====
Scanning for ghost lamp...
Texas Instruments
BLE Central
0x78A5047A6D9C
Devices Found 1
<- To Select
Connected0x78A5047A6DA0
Attacker service Found
Enable Notice
==========
USB CROSSTALK
Send
COM6 OPENED, 115200, 8, NONE, 1, OFF
Rx: 221 Bytes
Tx: 0 Bytes