USB Forensics and Pentesting

Dr. Phil Polstra
PhD, CISSP, CEH

@ppolstra
http://philpolstra.com

Certifications:
http://www.securitytube-training.com

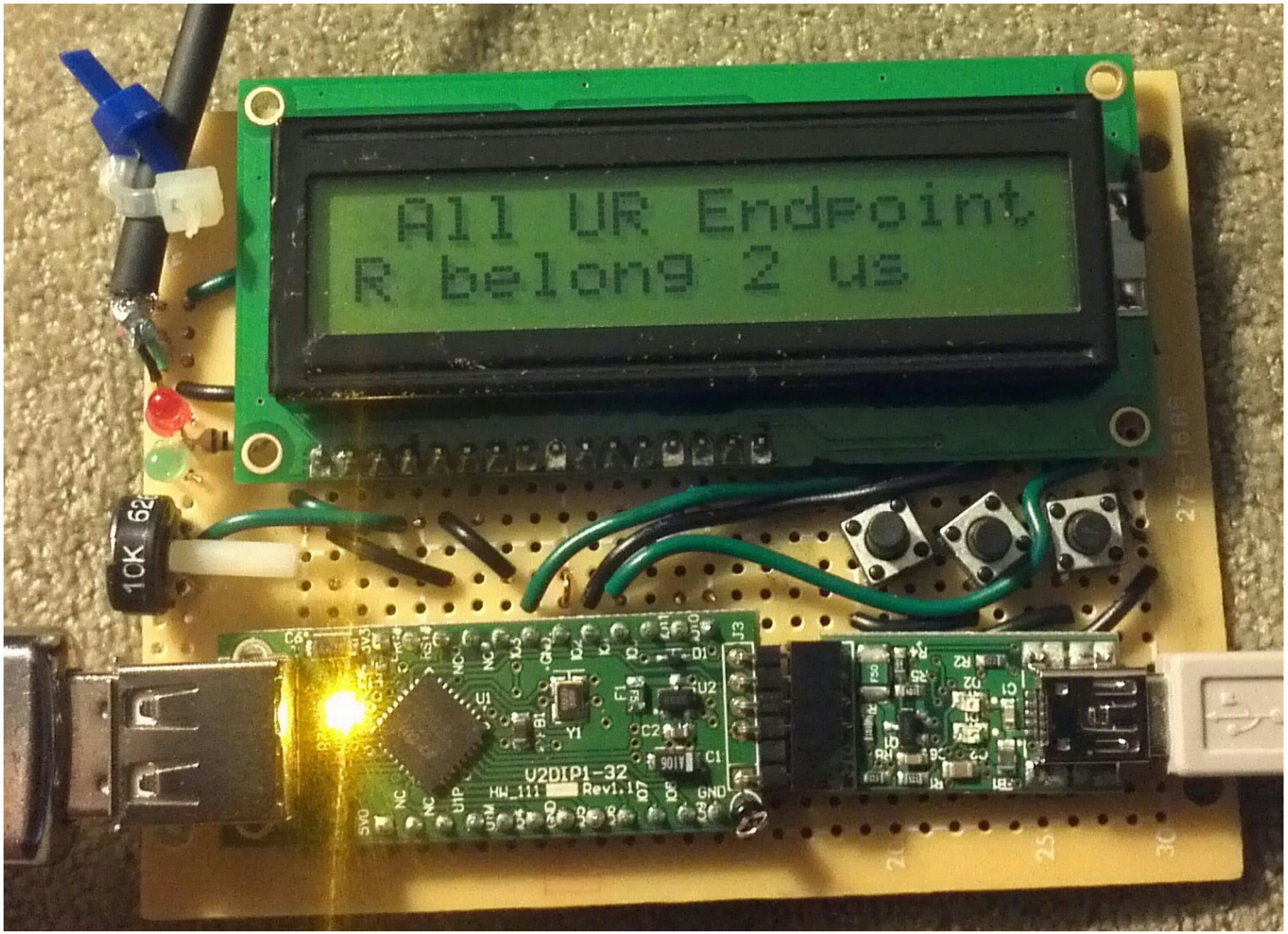
Pentester Academy:
http://www.PentesterAcademy.com

USBMS Impersonation

Why do this?

- Many companies have started to restrict what portable media may be attached to their computers
- Some software is available that does the USB equivalent of MAC filtering – only allows specified VID/PID to be mounted
- The device described allows for injection and exfiltration

Impersonator Hardware



High Level Design

- Builds on USB write blocker
- Write blocking can be toggled on/off
- VID/PID can be changed
  - Manually selected or preprogrammed
  - Automatic mode
    - VID/PID is tried (from list of 500 most common)
    - If host stops talking device is reset and next VID/PID is tried
    - Could also drop to brute force

Impersonator Threads

- Host and slave threads from write blocker
- New timer thread
  - Timer set when VID/PID tried
  - If enumeration isn't successful before timer expires the next VID/PID is tried
- New button thread
  - Checks for button press and updates appropriate variables

Wiring Details V2DIP1-32

- Buttons VID+, VID-, WP on 12, 14, 15, respectively
- LCD D4, D5, D6, D7, RS, E on 23, 24, 25, 26, 29, 30, respectively
- Green/Red LED on 31, 32 with 220 Ohm limiting resistor
- 10k potentiometer for contrast just as with duplicator

Wiring Details Vinco

- Buttons VID+, VID-, WP on 12, 13, 14, respectively
- LCD D4, D5, D6, D7, RS, E on 24, 25, 26, 27, 28, 29, respectively
- Green/Red LED on 31, 32 with 220 Ohm limiting resistor
- 10k potentiometer for contrast just as with duplicator