USB = Universal Security Bug?

András Veres-Szentkirályi
vsza@silentsignal.hu

HACKTIVITY
2012

Problem

- data transfer from a restricted PC environment
- no (usable) network connectivity
- user account with limited privileges
- only
  - video (VGA/DVI/HDMI/DisplayPort) ports and
  - USB HID devices (keyboard, mouse)

  are allowed to be connected
- no audio, RS–232, LPT, SCSI, eSATA, FireWire, etc.

USB – “So much more than a serial port with power”

Fred
2GB
HIGH-SPEED USB 2.0
HACKED!
The OH !*#% Flash Drive
Easily transfer and store files, photos and music with 2GB of high-speed, high-tech hijinks

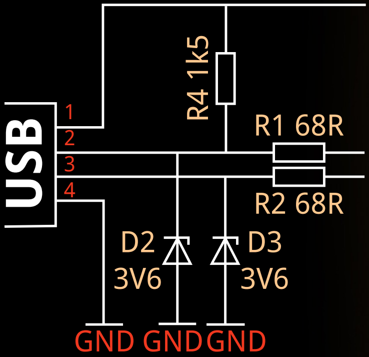
http://media.ccc.de/browse/congress/2010/27c3-4234-en-usb_and_libusb.html

AVR ATmega328

- Think of it as a computer
- It has a CPU clocked at 16 MHz
- It has memory: 2k RAM
- It has storage
  - 32k Flash (code, runtime read-only)
  - 1k EEPROM (data, read-write)
- It has general purpose inputs and outputs (GPIO)

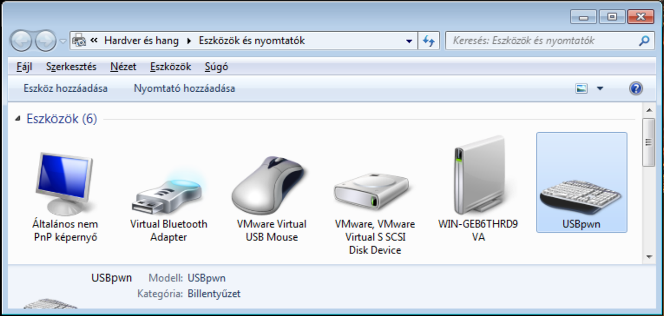
V-USB

- Firmware-only USB (1.1) stack for AVRs
- http://www.obdev.at/products/vusb/



USB HID

- Keyboards, mice, game controllers . . .
- No drivers needed
- Keyboards have input (keys) and output (LEDs) too



« Hardver és hang ▸ Eszközök és nyomtatók
Keresés: Eszközök és nyomtatók
Fájl Szerkesztés Nézet Eszközök Súgó
Eszköz hozzáadása
Nyomtató hozzáadása
Eszközök (6)
Általános nem PnP képernyő
Virtual Bluetooth Adapter
VMware Virtual USB Mouse
VMware, VMware Virtual S SCSI Disk Device
WIN-GEB6THRD9VA
USBpwn

USBpwn Modell: USBpwn
Kategória: Billentyűzet

LED protocol

```
            ___________________________________
   NUM ____/

                                ________________
  CAPS _______________________/

                ______            ______
SCROLL ________/      \__________/      \_____

                  01                11
```

```
set_lock(NUM,  (frame & 0x01) == 0x01);
set_lock(CAPS, (frame & 0x02) == 0x02);
set_lock(SCROLL, 1);
getchar();
toggle_key(SCROLL);
```

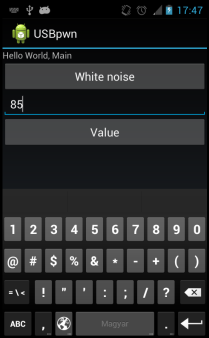
Typing code into vanilla Windows boxes

- Needs editor / environment / runtime
  - Batch files (.bat)
  - debug.com
  - PowerShell
- Needs to be typeable
  - binary
  - hexadecimal
  - base64

Base64 decoding on bare Windows? VBS!

```
Dim oNode, BinaryStream
Const adTypeBinary = 1
Const adSaveCreateOverWrite = 2

Set oNode = CreateObject("Msxml2.DOMDocument.3.0").
    CreateElement("base64")
oNode.dataType = "bin.base64"
oNode.text = "%%DATA%%"

Set BinaryStream = CreateObject("ADODB.Stream")

BinaryStream.Type = adTypeBinary

BinaryStream.Open
BinaryStream.Write oNode.nodeTypedValue
BinaryStream.SaveToFile "foo", adSaveCreateOverWrite
```

Storage and control solutions: smartphone



17:47

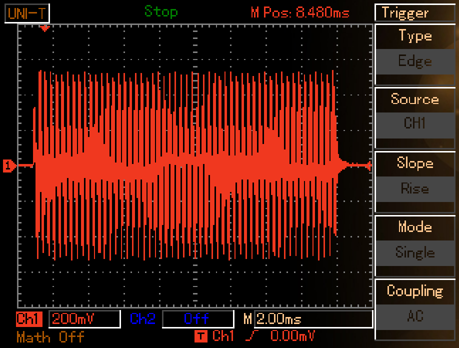
USBpwn

Hello World, Main

White noise

85

Value



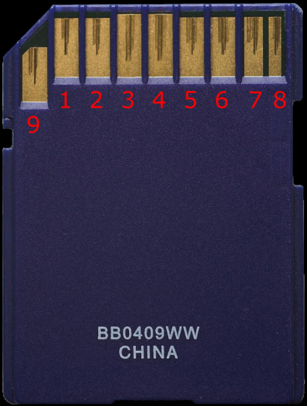
UNI-T Stop M Pos: 8.480ms

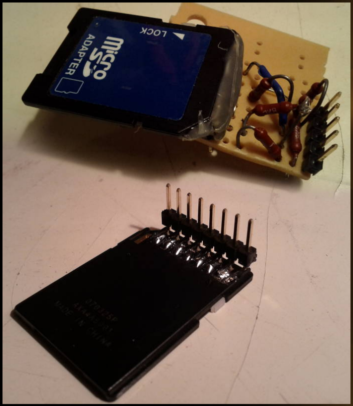
Trigger
Type: Edge
Source: CH1
Slope: Rise
Mode: Single
Coupling: AC

Ch1 200mV Ch2 Off M 2.00ms

Math Off T Ch1 0.00mV

Storage solutions: SD card





Storage workaround: Flash + EEPROM

- approx. 2k of memory is used for code
- 30k input, 1k output
- still enough for 4096 bit private keys
- can be copied to SD card after disconnect

```
type_buf = pgm_read_byte(&dropper[offset]);
eeprom_write_byte((uint8_t *)offset, recv_byte);
type_buf = eeprom_read_byte((uint8_t *)offset);
```

Rough benchmarks

- Typing flash (USB ⇒ host): 13 $\frac{character}{second}$
  - 10 $\frac{byte}{second}$ for base64 parts
- Reading LEDs (host ⇒ USB): 1.24 $\frac{byte}{second}$
- Typing EEPROM hex (USB ⇒ attacker): 4.5 $\frac{byte}{second}$

Room for ~~weaponization~~ improvement

- much smaller form factor is possible
- more and better memory
- encryption
- integrity protection
- same is possible with PS/2 ;)

Source code is free as in both senses

Part	License	URL
Host	MIT	`http://git.io/up-host`
Device	OBDEV	`http://git.io/up-dev`
Base64 VBS	MIT	`http://git.io/b64vbs`

Thanks for your attention!

Facebook

vsza@silentsignal.hu

web

e-mail