# Ne(bezpečné) USB?

## Úvod k workshopu s Teensy

Pavel Bašta • pavel.basta@nic.cz • 23.05.2014

CZ.NIC | SPRÁVCE DOMÉNY CZ

# Útoky prostřednictvím USB

- Autorun
- U3
- Další zneužití USB
- HID USB zařízení

# Autorun

- Flash/CD-ROM/DVD-ROM
  - Dříve oblíbený způsob šíření malware
    - Conficker
    - Worm:W32/Autorun
  - Dnes je funkce autorun pro flash disky ve windows ve výchozím nastavení vypnutá
  - Stále ovšem funguje autorun pro CD-ROM/DVD-ROM

# U3 Flash

- Firmware ohlašuje část flash disku jako CD-ROM
- Dojde ke spuštění obsahu dle autorun.inf
- Switchblade
  - Dump mnoha různých zdrojů hesel
    - Firefox, Mail, WiFi, databáze SAM, atd.
  - Přidání administrátorského účtu
- Hacksaw
  - Novější verze switchblade

# Specialitky

- Stuxnet
  - Zaměřený na útoky proti SCADA
  - Potřeba dostat se do off-line sítě
  - Šířil se především přes USB
  - Zneužití neznámé zranitelnosti
- Evil Made Attack
  - Zavádí se z flash disku
  - Pozmění zavaděč truecryptu
  - Zachytí zadávané heslo

# HID USB zařízení

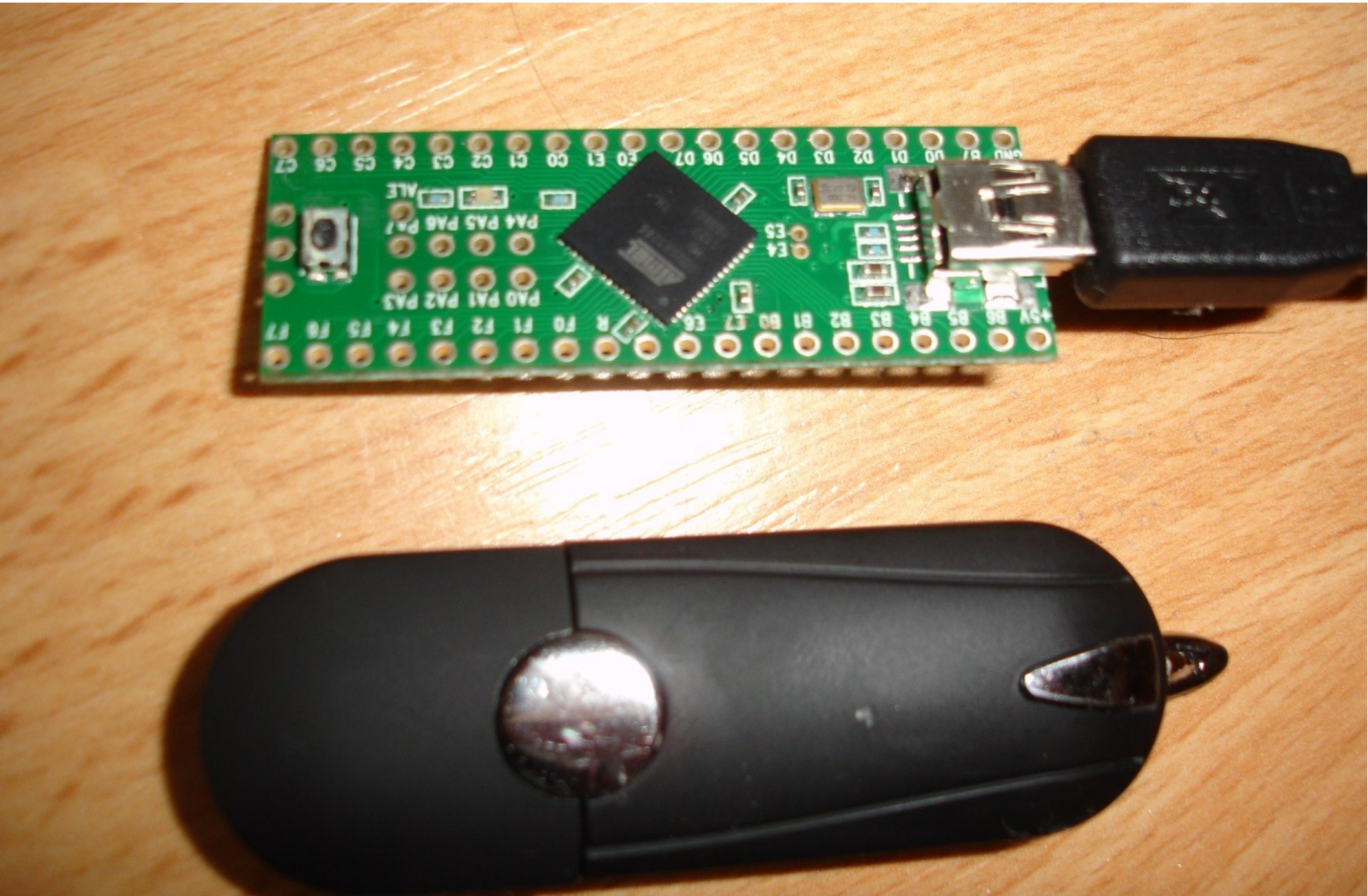
- HID (Human Interface Device)
  - Univerzální protokol pro komunikaci vstupních zařízení (myš, klávesnice, joystick) s PC
  - Není potřeba mít ovladače pro různá  zařízení
  - Host/Device
  - HID descriptor v ROM zařízení
  - Host zpracuje descriptor a pak může komunikovat se zařízením
- Co když připojím zařízení, které se ohlásí jako klávesnice?

# HID USB zařízení

- USB Rubber Ducky
  - http://hakshop.myshopify.com/products/usb-rubber-ducky
  - Open Source firmware
  - Vlastní zjednodušený jazyk, předem připravené útoky
  - Podpora microSD
  - Multiplatformní

# HID USB zařízení

- Teensy
  - Jednočip (AT90USB1286, 8 bit AVR, 16 MHz)
  - $24
  - Je možné si vybrat, jak se bude zařízení prezentovat vůči PC při provádění našeho programu (myš, klávesnice, joystick)
  - Možno programovat útoky pro různé platformy
    - Přidání administrátora
    - Otevření portu
    - Vzdálené připojení k shellu


C7 C6 C5 C4 C3 C2 C1 C0 E1 E0 D7 D6 D5 D4 D3 D2 D1 D0 B7 GND
ALE
PA4 PA5 PA6 PA7
PA0 PA1 PA2 PA3
E5
E4
F7 F6 F5 F4 F3 F2 F1 F0 R E6 E7 B0 B1 B2 B3 B4 B5 B6 +5V

# Workshop

- Příležitost „osahat“ si jednočipové počítače a zároveň si vyzkoušet, jak je může proti Vaší organizaci využít případný útočník
- Připraveno vývojové prostředí pro Linux i Windows
- Máme k zapůjčení 24 zařízení
- Začátek ve 14:30 v salónku

# Workshop příprava

- https://secure.nic.cz/files/pbasta/arduino-1.0.1_windows.zip
- https://secure.nic.cz/files/pbasta/arduino-1.0.5_linux_32bit.tar
  https://secure.nic.cz/files/pbasta/arduino-1.0.5_linux_64bit.tar

# Děkuji za pozornost

**Pavel Bašta • pavel.basta@nic.cz**