Lokální útoky s Teensy

Pavel Bašta • pavel.basta@nic.cz • 22.05.2014

Stažení software a příprava

- Vývojové prostředí Arduino s předinstalovaným doplňkem teensyduino a CZ layoutem klávesnice
- Pro Windows
- https://secure.nic.cz/files/pbasta/arduino-1.0.1_windows.zip
- https://secure.nic.cz/files/pbasta/nc111nt.zip
  - nc111nt.zip
  - arduino-1.0.1_windows.zip - použijte oblíbený nástroj pro rozbalování zip souborů

Stažení software a příprava

- Pro Linux
- https://www.pjrc.com/teensy/49-teensy.rules
  - sudo cp 49-teensy.rules /etc/udev/rules.d/
- https://secure.nic.cz/files/pbasta/arduino-1.0.5_linux_32bit.tar
  - arduino-1.0.5_linux_32bit.tar - tar xf arduino-1.0.5_linux.tar
- openjdk-7-jre ?

Programování

- Arduino programming language
  - http://arduino.cc/en/Reference/HomePage
- C
- BASCOM-AVR
- LabVIEW
- Python
  - Python-on-a-Chip
- Txtzyme
- AttoBASIC

Nastavení

- Provedeme kontrolu
- Tools:
  - Board
  - USB Type
  - Keyboard Layout

První test

```
void setup() {        //funkci setup musi obsahovat kazdy program pro
teensy, jeji obsah se provadi pouze jednou

  pinMode(6, OUTPUT); //ve vychozim stavu jsou vsechny piny v
modu INPUT,musime tedy ledPinprepnout do modu OUTPUT
}

void loop() {         //funkci loop musi obsahovat kazdy program pro
teensy, je to nekonecna smycka
  digitalWrite(6, HIGH);   //zapnutí LED
  delay(1000);
  digitalWrite(6, LOW);    //vypnutí LED
  delay(1000);
}
```

Použití jako HID zařízení

- Jednoduchá varianta
- Keyboard.print("Hello World ");

Hello World

```
void setup()
{
delay(5000);
Keyboard.print("Hello World");
}
void loop()
{
}
```

Individuální zadávání kláves

- Keyboard.print má své limity
  - ctrl~c
  - Home, PrintScreen, kurzorové šipky
- Keyboard.set_modifier(MODIFIERKEY_GUI);
- Keyboard.set_modifier(MODIFIERKEY_CTRL | MODIFIERKEY_ALT);
- Keyboard.set_modifier (0);

Individuální zadávání kláves

- Možnost přenést až 6 kláves najednou
  - Keyboard.set_key1(KEY_A);
  - Keyboard.set_key2(KEY_B);
  - Keyboard.set_key3(KEY_C);
  - Keyboard.set_key4(KEY_D);
  - Keyboard.set_key5(KEY_E);
  - Keyboard.set_key6(KEY_F);
- Keyboard.send_now();

Individuální zadávání kláves

- Keyboard.set_modifier(0);
- Keyboard.set_key1(0);

Name	Function
MODIFIERKEY_CTRL	Control Key
MODIFIERKEY_SHIFT	Shift Key
MODIFIERKEY_ALT	Alt Key
MODIFIERKEY_GUI	Windows (PC) or Clover (Mac)

Individuální zadávání kláves

Normal Keys			
KEY_A	KEY_B	KEY_C	KEY_D
KEY_E	KEY_F	KEY_G	KEY_H
KEY_I	KEY_J	KEY_K	KEY_L
KEY_M	KEY_N	KEY_O	KEY_P
KEY_Q	KEY_R	KEY_S	KEY_T
KEY_U	KEY_V	KEY_W	KEY_X
KEY_Y	KEY_Z	KEY_1	KEY_2
KEY_3	KEY_4	KEY_5	KEY_6
KEY_7	KEY_8	KEY_9	KEY_0
KEY_ENTER	KEY_ESC	KEY_BACKSPACE	KEY_TAB
KEY_SPACE	KEY_MINUS	KEY_EQUAL	KEY_LEFT_BRACE
KEY_RIGHT_BRACE	KEY_BACKSLASH	KEY_NUMBER	KEY_SEMICOLON
KEY_QUOTE	KEY_TILDE	KEY_COMMA	KEY_PERIOD
KEY_SLASH	KEY_CAPS_LOCK	KEY_F1	KEY_F2
KEY_F3	KEY_F4	KEY_F5	KEY_F6
KEY_F7	KEY_F8	KEY_F9	KEY_F10
KEY_F11	KEY_F12	KEY_PRINTSCREEN	KEY_SCROLL_LOCK
KEY_PAUSE	KEY_INSERT	KEY_HOME	KEY_PAGE_UP
KEY_DELETE	KEY_END	KEY_PAGE_DOWN	KEY_RIGHT
KEY_LEFT	KEY_DOWN	KEY_UP	KEY_NUM_LOCK
KEYPAD_SLASH	KEYPAD_ASTERIX	KEYPAD_MINUS	KEYPAD_PLUS
KEYPAD_ENTER	KEYPAD_1	KEYPAD_2	KEYPAD_3
KEYPAD_4	KEYPAD_5	KEYPAD_6	KEYPAD_7
KEYPAD_8	KEYPAD_9	KEYPAD_0	KEYPAD_PERIOD

Vypnutí firewallu ve windows

Otevření síťového připojení z PC s Linuxem

To není vše

- Kautilya
  - Generuje útočné kódy pro Teensy
  - Napsáno v Ruby
  - Kódy pro hlavní platformy Linux, Windows a OS X
- Obrana
  - Zákaz instalace nových zařízení ve skupinových politikách windows
  - Pomocí UDEV povolit v linuxu pouze známá zařízení

Kde se dozvědět více?

- AZB
  - http://www.csirt.cz/news/security/
- Školení a akademii CZ.NIC
  - Výrazné slevy pro studenty
  - Svobodná aplikační bezpečnost I. a II.
  - Elektronický podpis a problematika infrastruktury veřejných klíčů (PKI)
  - DNSSEC – zabezpečení DNS
  - Bezpečnost prakticky

Děkuji za pozornost

Pavel Bašta • email@nic.cz