USB the Root of All Evil

Tim Pierson
President, Data-Sentry.com

The Pentagon conceded that a USB flash drive carried an attack program inside a classified U.S. military network.

Could your company be next?

Who is this Guy?

Tim Pierson AS, BS, MS

Professional PenTester, Instructor and Consultant for over 26 years.

EcCouncil – Instructor of the year recipient 2009 from a large pool of nominees.

Contributing author to the book-
VMware vSphere™ and Virtual Infrastructure Security: Securing ESX and the Virtual Environment
ISBN-10: 0137158009 Pearson Publishing

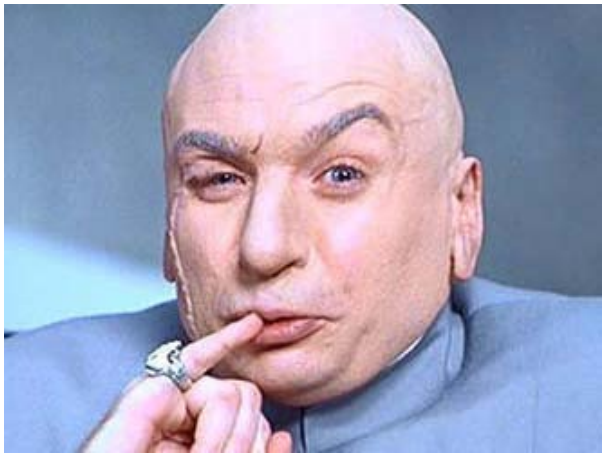
- **Very Intrigued with the Virtual Environment.**

How you know if you're a Geek?

- If you wife says….
  - Why do we have to reboot our TV?
  - None of my friends have to reboot their TV?
    - You might be a Geek.
- If you keep fixing things even though others don't think they are broken. Then break it, and your wife misses her favorite show…
    - You might be a Geek.
- TalkShoe.com
    - Popular Podcast Site.

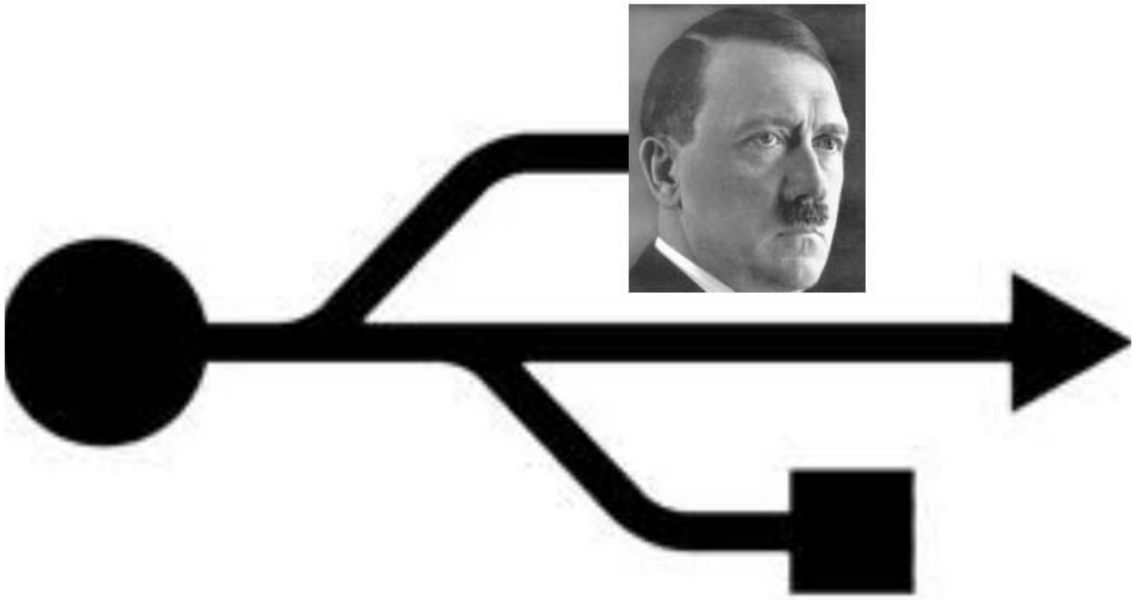
Overview

- I will show you something new
- “Direct from the BatCave secret evil minds….”



USB

- *I am here to prove to you that….*
- **USB = EVIL**



Problem as I see it…

- **The SCADA Threat**

- I recently attended a INSA* event where various security related issues were discussed.
- The main speaker was **Admiral Mike McConnell**, the former head of the NSA and former DNI, and he said something which I greatly fear is true, particularly regarding major infrastructure.
- *"The USA will do nothing to stop cyber attacks until a large attack against the country is successful – and at that point the government will step in and do the wrong thing"*

  - **Intelligence and National Security Alliance**
    - INSA is the premier not-for-profit, nonpartisan, private sector professional organization providing a structure and interactive forum

Cost of StuxNet

- Most have speculated that the development of Stuxnet may have cost several million dollars, somewhere in the upper seven-digits.
- The next cyber weapon will be considerably cheaper, since much of the attack vector and the specifics of how to use automation equipment will simply be copied.
- So let’s assume the next Stuxnet costs below one million dollar and is for sale on the black market (it’s just a question of time).

Cost of StuxNet

- It is then that some not-so well equipped nation states and well-funded terrorists will grab their checkbooks.
- Let the street price drop to the five-digit region and organized crime is in. Sabotage with the motivation of extortion will get a commonplace scenario.
- At this time targets are no longer limited to critical infrastructure but will especially cover the private sector —
  - a TARGET-RICH AREA where it cannot be assumed that organizations will install countermeasures large scale in a reasonable amount of time.

The Danger….

- We are probably familiar with the dangers of plugging in a USB?
- It is doubtful that someone at this conference will pick up a USB and plug it in their unprotected computer. At least we hope not.

- We all have Naturally we have set our computer to

  No Autorun!

- Whew… At least that won't happen to me now..

- If you fall into this Camp, Buckle Up!

Now … On with the Show…

- How can we take what we have learned from Stuxnet and stop this?
- Naturally we “should” be caught by these mechanisms that are in place …
- Right?
- Guess Again…

DEMO

- USE of USB to act as a Keyboard and whatever the programmer has decided to do can be easily keyboarded to you machine as soon as you put in the USB stick.
- While I am showing you a Safe Distribution it can easily be made into a Nefarious or even Lethal version.

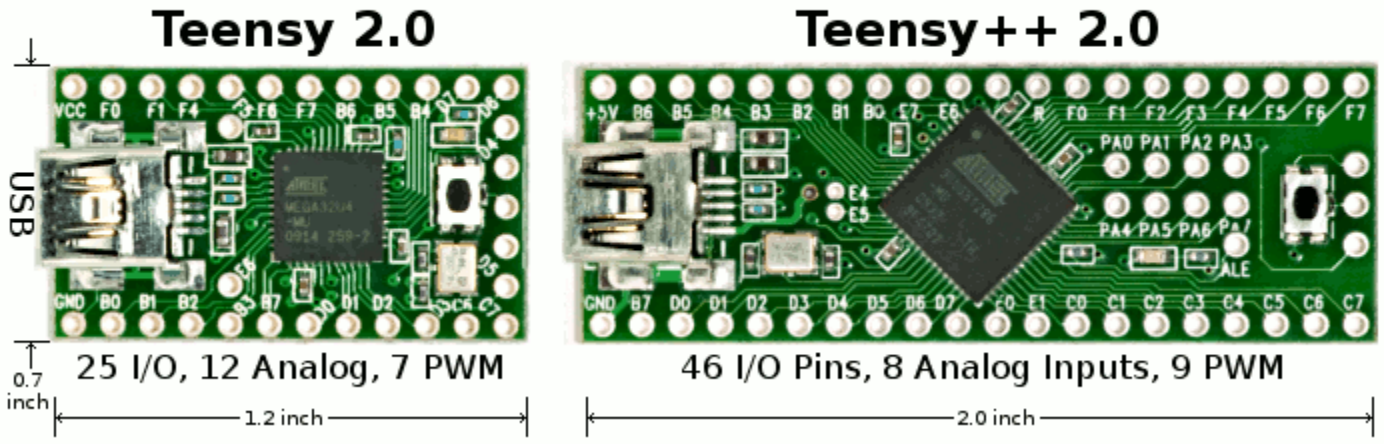
Have you Heard of HID? Human Interface Device

- USB Keyboard
- USB Mouse
- USB GameController

- Any device can be a USB HID class device as long as a designer meets the USB HID class logical Specification
- Wireless Devices opens up an entire Pandora's Box.

HID – Human Interface Hardware

Teensy USB Development Board



- USB device class that describes **H**uman **I**nterface **D**evices such as keyboards, mice, game controllers and alphanumeric display devices.

The Hackers Most Common tool these days…

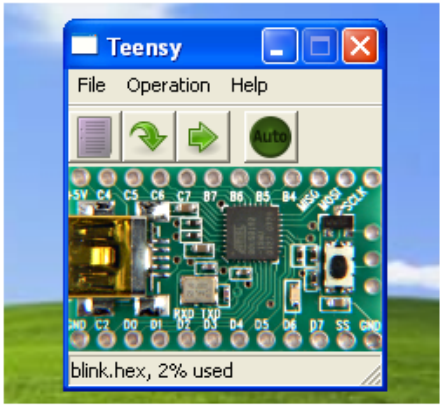
The Swiss Army Knife of a current Day Attacker!

Teensy Loader Program

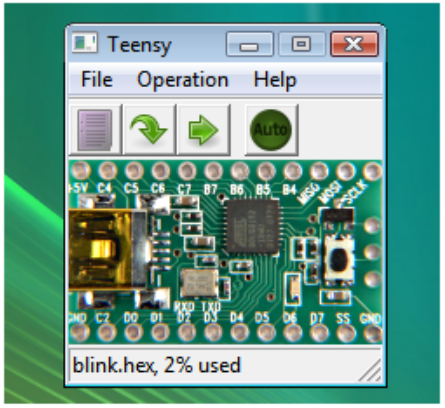
- The Teensy Loader Application
- The Teensy Loader program communicates with your Teensy board when the HalfKay bootloader is running, so you can download new programs and run them.
- Teensy Loader is available for these operating systems:

Macintosh OS X 10.5

Linux (Ubuntu)



Windows XP



Windows 7 & Vista

Source Code - Create Keyboard HID

```
/* Keyboard example for Teensy USB Development Board
 * http://www.pjrc.com/teensy/usb_keyboard.html
 * Copyright (c) 2008 PJRC.COM, LLC
 *

#include <avr/io.h>
#include <avr/pgmspace.h>
#include <avr/interrupt.h>
#include <util/delay.h>
#include "usb_keyboard.h"

#define LED_CONFIG      (DDRD |= (1<<6))
#define LED_ON          (PORTD &= ~(1<<6))
#define LED_OFF         (PORTD |= (1<<6))
#define CPU_PRESCALE(n) (CLKPR = 0x80, CLKPR = (n))

uint8_t number_keys[10]=
    {KEY_0,KEY_1,KEY_2,KEY_3,KEY_4,KEY_5,KEY_6,KEY_7,KEY_8,KEY_9};

uint16_t idle_count=0;

int main(void)
{
    uint8_t b, d, mask, i, reset_idle;
    uint8_t b_prev=0xFF, d_prev=0xFF;

    // set for 16 MHz clock
    CPU_PRESCALE(0);

    // Configure all port B and port D pins as inputs with pullup resistors.
    // See the "Using I/O Pins" page for details.
    // http://www.pjrc.com/teensy/pins.html
    DDRD = 0x00;
    DDRB = 0x00;
    PORTB = 0xFF;
    PORTD = 0xFF;

    // Initialize the USB, and then wait for the host to set configuration.
    // If the Teensy is powered without a PC connected to the USB port,
    // this will wait forever.
    usb_init();
    while (!usb_configured()) /* wait */ ;

    // Wait an extra second for the PC's operating system to load drivers
    // and do whatever it does to actually be ready for input
    _delay_ms(1000);

    // Configure timer 0 to generate a timer overflow interrupt every
    // 256*1024 clock cycles, or approx 61 Hz when using 16 MHz clock
    // This demonstrates how to use interrupts to implement a simple
    // inactivity timeout.
    TCCR0A = 0x00;
    TCCR0B = 0x05;
    TIMSK0 = (1<<TOIE0);

    while (1) {
        // read all port B and port D pins
        b = PINB;
        d = PIND;
        // check if any pins are low, but were high previously
```

Well lets just Apply for our own HID…
HIDs Application

Vendor ID (VID) Number. The company set forth above hereby applies for a USB Vendor ID Number and agrees to the following: The USB Implementers Forum is the authority which assigns and maintains all USB Vendor ID Numbers. Each Vendor ID Number is assigned to one company for its sole and exclusive use, along with associated Product ID Numbers. They may not be sold, transferred, or used by others, directly or indirectly, except in special circumstances and then only upon prior written approval by USB-IF. Unauthorized use of assigned or unassigned USB Vendor ID Numbers and associated Product ID Numbers are strictly prohibited.

Terms: The membership subscription of the company named above ("Company") becomes effective on the date on which the Forum administrator sends notice of enrollment to Company and is subject to the following terms:

Not discriminate on the basis of gender, race, color, creed, ancestry, place of origin, political beliefs, religion, marital status, disability, age, or sexual orientation;

MAIL PAYMENT ALONG WITH THIS COMPLETED FORM TO:
(Check or Money Order for US Dollars ONLY - No Purchase Orders)

MAKE CHECK PAYABLE TO:
USB IMPLEMENTERS FORUM, INC.
3855 SW 153rd Drive
Beaverton, OR 97006
USA

This will serve as your "INVOICE" as well as agreement of the terms of membership in USB-IF.

So Now what Can we do..?

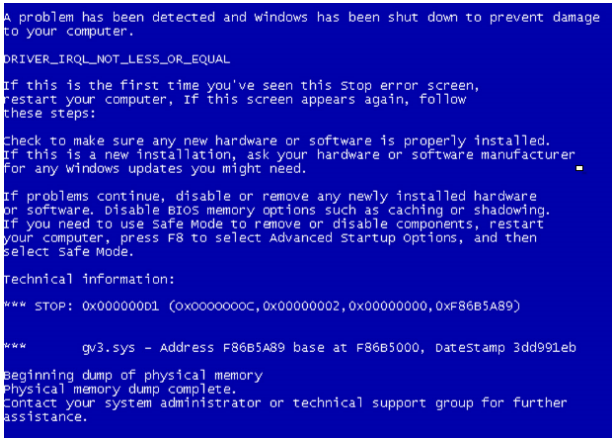
- Basically Anything…
- Malware
- Force a Login
- Click Through UAC
  - Corporate Nightmare.
- If it works on 1 machine.
  - It works on the other 50K machines in the Corporation, because they are mostly deployed by Ghost or similar imaging.

How well are your Drivers Written?

- Who wrote the Drivers in the first place?
- Well lets just see…
- Peach Fuzz…
- Fuzz them!
- In my tests 30 of them "**Hiccupped**"
  - Can you Say… "**Blue Screen?**"

Peach Fuzzing Platform

Definition:
It is how my wife treats me….



- Get used to that if you are going to try that route…

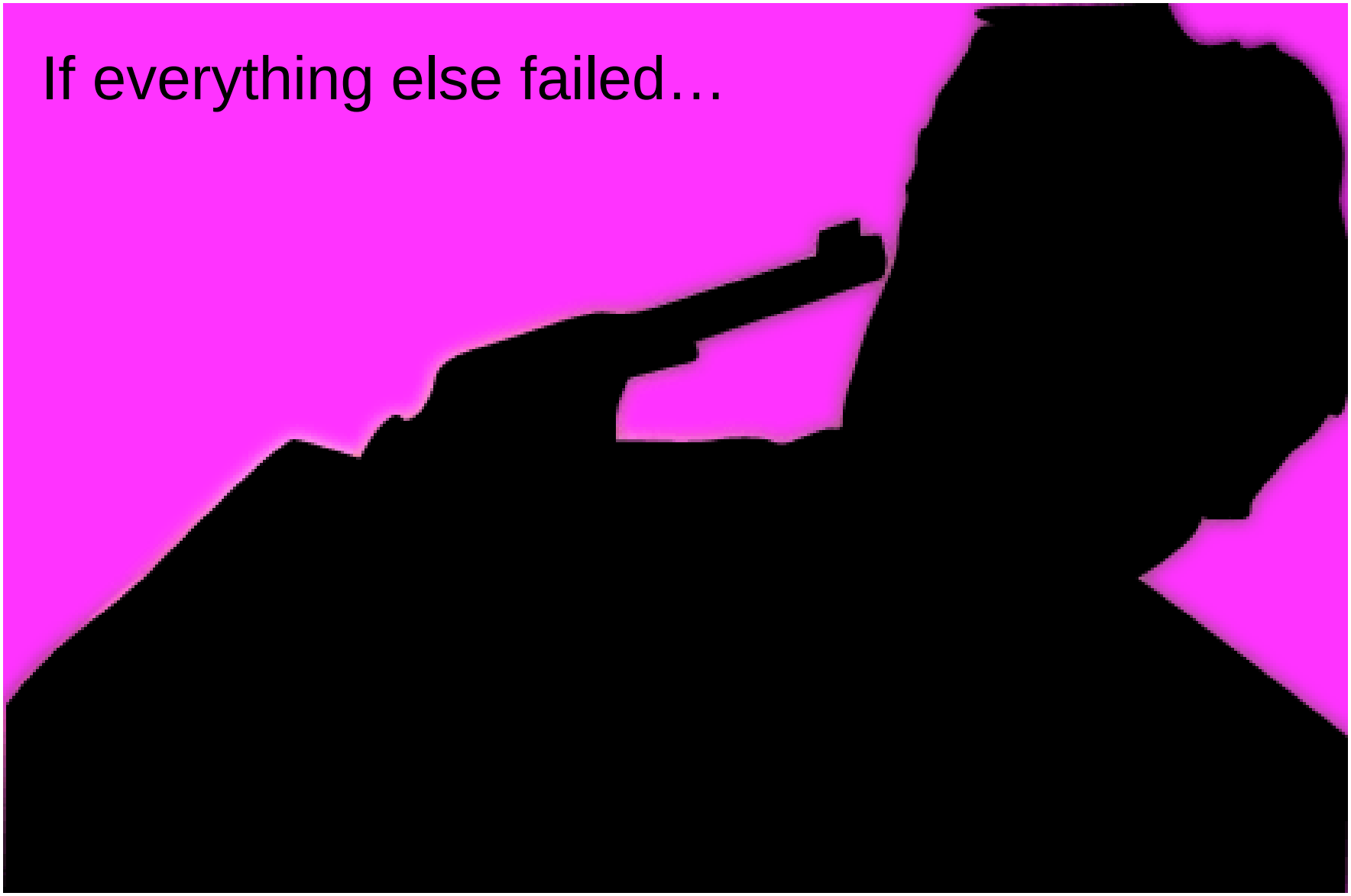
Just a bit of C….
You gotta know how it works to… well Prevent it!

- Use Different Language Tools
  - strcpy(<dest>,<src>) – Poor Choice
  - strncpy(<dest>,<src>,<width>) – Best Choice
- Design and Build Security within Code
- Use Source Code Scanning Tools
- Use Compiler Enhancement Tools
- Know What Is On Your System
- Patch the Operating System and Application
- Java and .Net are more Secure Programming Languages
- Shell code can be as small as
  - 24 bytes in Linux and
  - 300 bytes in Windows

So What do we do?

- This is like watching the evening news…Bad News Tim..
- Just all Bad News….
- So what can we do to fix this?...

If everything else failed…



So What do we do?

- Disable External USB
  - What about Docking Stations?
  - USB Access?
- USB GLUE…

Here is a bright idea from the US Military.

- USB Device Management
- Group Policies
- Watcher Apps… (Never allow the Same USB HIDS)
- O/S monitors/controls HIDs
- USE a VDI solution (XEN is the best in my opinion). Or VMware View, where the idea is the Desktop is secured in the datacenter not in the less secure “Cube Farm” where the user has physical access
- If I can touch it I can break into it. It is not really possible (or practical) for me to protect it there.

Summary…

- USB…
- Just like Nancy Regan Said about Drugs…
- Just don’t do it…