You are the Trojan!

David Maynor

X-Force Advanced R&D

INTERNET | SECURITY | SYSTEMS®

The rise to power of security tools and researchers.

INTERNET | SECURITY | SYSTEMS®

Rise to power…

- **Rise to power of the modern security tools**
  - Security in general is reaching a state of maturity
  - Deployment has increased
  - Understanding of the operation and theory of the tools has increased greatly

Rise to power…

- **IDS->IPS**
  - Detection vs. prevention
    - IDS
      - Limited to basic prevention at mitigation
        - Access device reconfiguration
        - TCP RST
      - Mostly a passive technology
    - IPS
      - Inline tool
      - Prevention
        - Stop attacks in real time
        - Better attack recognition
  - Contributes to a tighter border security

INTERNET | SECURITY | SYSTEMS®

Rise to power…

- **Vulnerability Scanner->Automated Pentesting tools**
  - Marketing materials
  - Deployment configuration for exploits may not be a threat
  - No admin access required
    - No patch checks
  - Identification of truly vulnerable systems

Rise to power…

- **Source Auditing->Binary auditing**
  - Simple bug classes are gone
  - Protocols and formats become increasing complex
    - Binary only drivers
  - Easier to spot bugs
    - Signed comparison
    - Unintended results of operations
  - Tools are becoming more available
    - IDA
    - OllyDBG
    - SoftIce

Rise to power…

- **Vulnerability announcement->PoC available**
  - PoC availability has normally been measured in months
  - UPNP was measured in days.
  - Patch diffing technology increasing
  - Soon PoC time will be measured in hours.

Rise to power…

- **Rise to power of the security researcher**
  - Tools and techniques
    - grep is all but gone
    - Auditing techniques have increased
  - Maturity
    - Actual methodologies have emerged
  - Knowledge
    - Txt files to shellcoders handbook

Rise to power…

- **Proprietary does not mean impossible**
  - Tools are becoming more available
    - Ida supports several processor types
    - Embedded visual studio
    - Ring 0 debuggers
  - Reverse Engineering techniques have improved
    - Researchers know several types of asm
    - Architectures of different chips is more commonly available

Where have all the Vectors gone?

Vectors, we hardly knew thee

"Oh hey! I just love these things! ... Crunchy on the outside and a chewy center!"

Vectors, we hardly knew thee

- **“Internet wide” attacks are going to the way side**
  - Blaster and Slammer were huge wake up calls
  - Results
  - Corporations perimeter defenses?
  - Sophistication of security tools and researchers leads to quick malware protection being created.

Vectors, we hardly knew thee

- **The designer era**
  - ZOTOB and variants proved wide scale internet scanning is less effective than targeted attacks.
  - Finical gain
  - “Recruitment drive” or “pledge week”
  - Even more effective is malware designed to target one specific business.
    - Banks
    - Credit Card Companies
  - If malware is not widespread enough it is hard for security companies to create protection

Vectors, we hardly knew thee

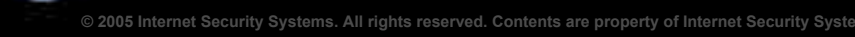
- **If the perimeter has been tightened, how do these attacks keep getting inside?**
  - Advanced evasion techniques?
  - Super secret 0day?
  - The user!
    - Mobile users
    - VPN users
    - Security is often sacrificed for speed or usability
    - Compliance?

What is an attacker to do?

GIVE UP!

(Raise your hand if you think this is likely)

(Point and laugh at people with their hand raised)



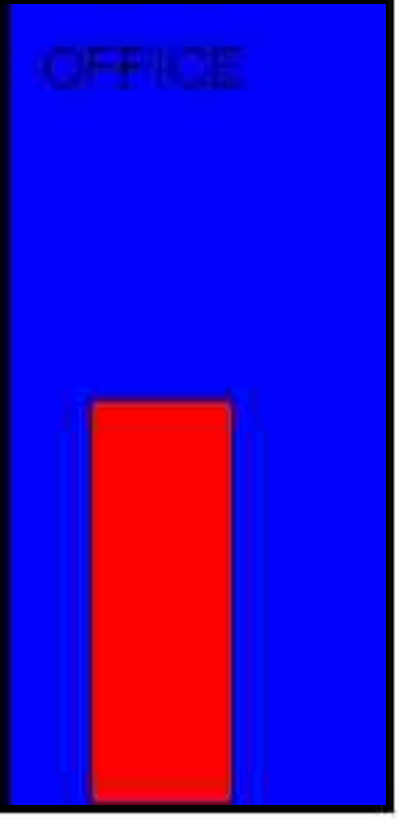
The resourceful attacker

- **Sometimes old school is best**
  - Sneaker-net may be the best way to bypass security
  - What is sneaker-net?

SNEAKER-NET

INTERNET | SECURITY | SYSTEMS®

SNEAKER-NET



INTERNET | SECURITY | SYSTEMS®

The resourceful attacker

- **How useful is this?**
  - During the Blaster infection GaTech blocked the affected ports at the border routers and cleaned the infected machines over the weekend.
  - Monday more infections appeared, why?
    - Laptops from home.
  - ZOTOB came into companies over VPN links and piggy backed on laptops that were brought in.
- **What is a modern day sneaker-net?**
  - Use the weakest link in security, the user.
  - OS hardening is making attacking the machines remote less likely to be successful.

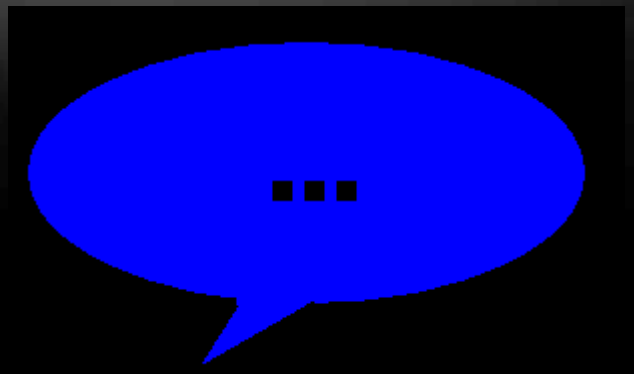
The resourceful attacker

- **What is still really vulnerable?**
  - Peripherals
  - Everything is getting them
  - The design of the common PC architecture allows for explicit trust of the components.
- **Think about you machine…**
  - My laptop has
    - 2 usb ports
    - 1 cardbus port
    - Graphics/network adapters

The resourceful attacker

- **Components are getting more complex**
  - You no longer have a single computer, you have a collection of several single purpose computers.
  - Current video cards have more processing power and storage space than my first PC.
  - Can these components be used to do you evil bidding?

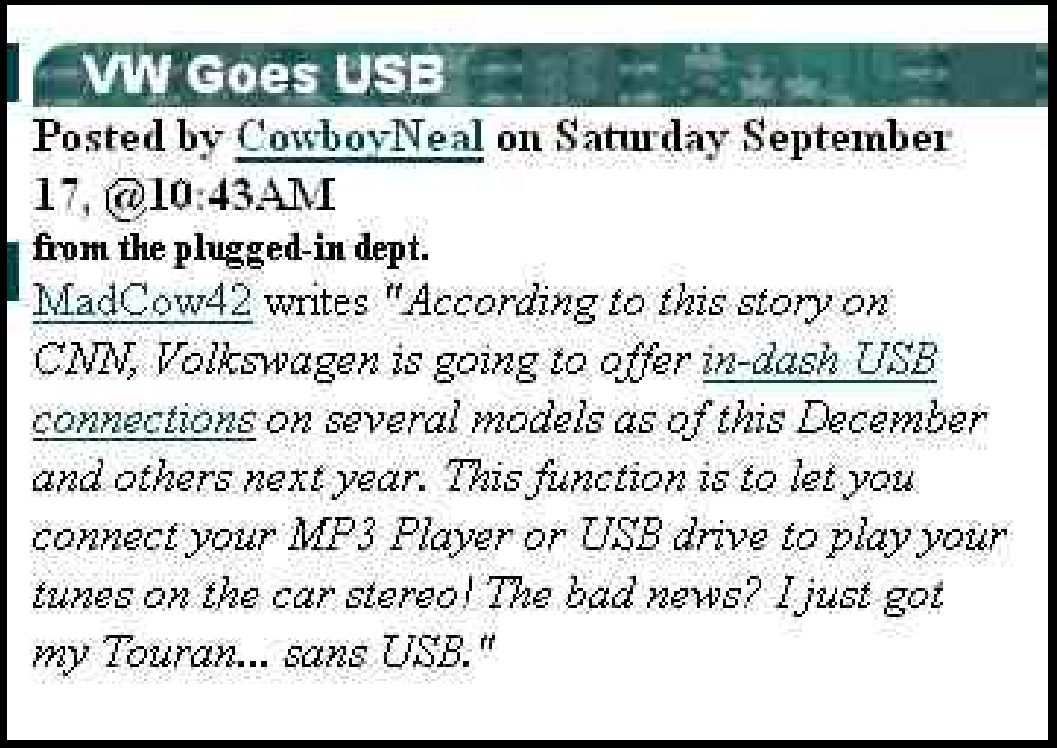
True Story…



INTERNET | SECURITY | SYSTEMS®

The resourceful attacker

- **Looking at the components.**
  - Everything is getting more “integrated”



VW Goes USB

Posted by CowboyNeal on Saturday September 17, @10:43AM

from the plugged-in dept.

MadCow42 writes *"According to this story on CNN, Volkswagen is going to offer in-dash USB connections on several models as of this December and others next year. This function is to let you connect your MP3 Player or USB drive to play your tunes on the car stereo! The bad news? I just got my Touran... sans USB."*

INTERNET | SECURITY | SYSTEMS®

The resourceful attacker

INTERNET | SECURITY | SYSTEMS®

The resourceful attacker

INTERNET | SECURITY | SYSTEMS®

The resourceful attacker

INTERNET | SECURITY | SYSTEMS®

The resourceful attacker

The resourceful attacker

INTERNET | SECURITY | SYSTEMS®

The resourceful attacker

- **Gadgets**
  - Thinks about what gadgets you have?
  - I personally have:
    - Laptop
    - Blackberry
    - Psp
    - Ipod
    - Usb key chain

It really does mean Direct Memory Access.

Bus Mastering

- DMA is a type of “BUS Mastering.”
- Bus Mastering is when a device can use the system bus to communicate with other devices without needing the CPU.
- Full bus mastering requires the device to have its on controller.

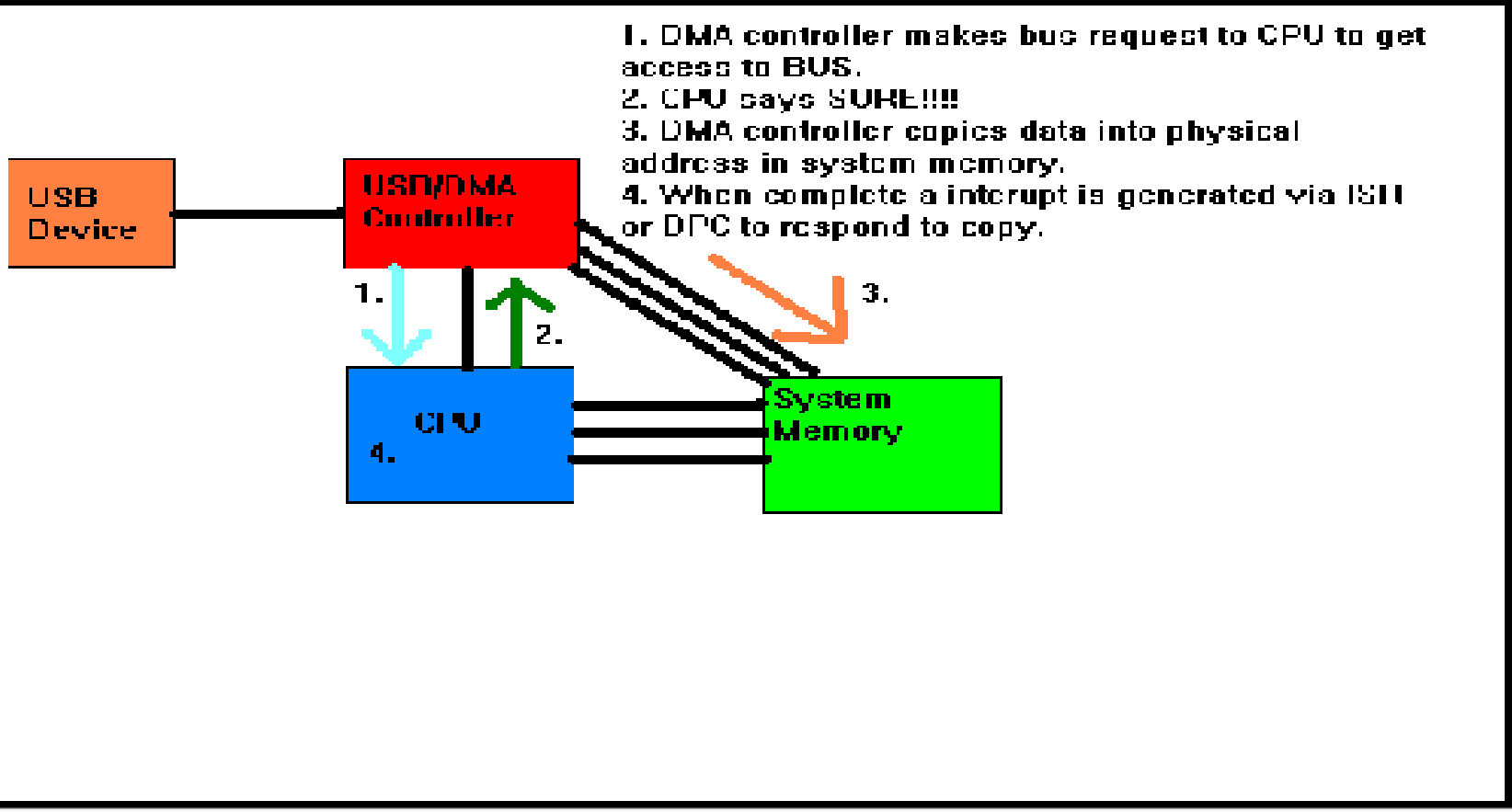
INTERNET | SECURITY | SYSTEMS®

DMA

- **DMA == Direct Memory Access**
  - Allows for independent reads/writes
  - Designed to free the CPU from massive interrupt loads
  - The key to high performance data transfers for things like USB and Firewire.
  - Zero-Copy Implementation.
- **What uses DMA?**
  - It is used by most everything in a modern PC architecture
  - Think of it as the internal communication protocol for the computer.
  - USB, PCMCIA(cardbus), Firewire, AGP, disk controllers, network cards, sound cards, …

DMA

- I just got out of my fingerpainting class.



DMA

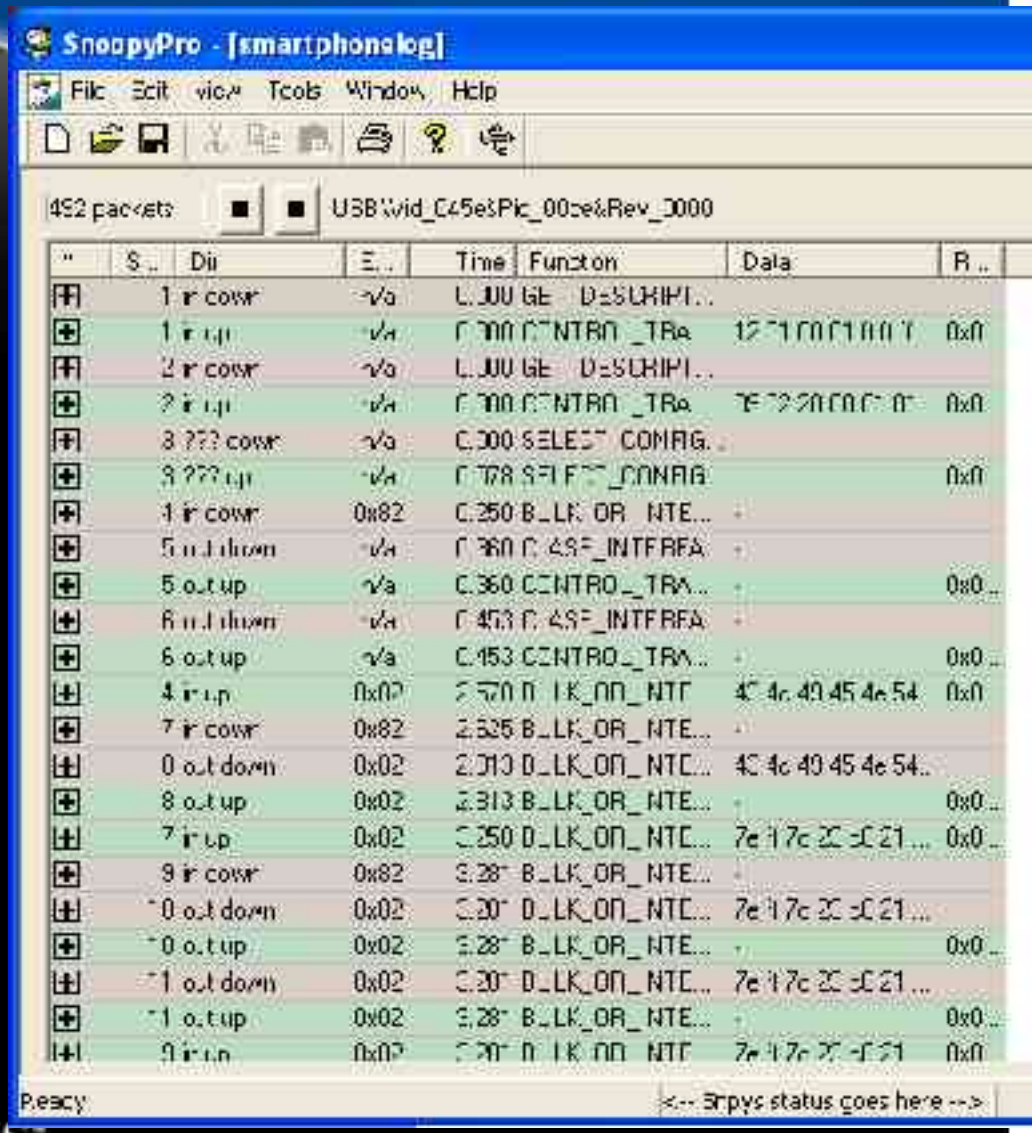
- **Things to keep in mind about DMA**
  - The CPU is oblivious to DMA activity.
    - Don’t think a HIPS will keep you safe.
  - You are dealing with Physical Memory
    - You can implement a virtual memory parser
      - Ask me about this
    - Trivial to cause bad things to happen.
  - Requires a “bus request” to start a transfer.

USB, DMA's Favorite child

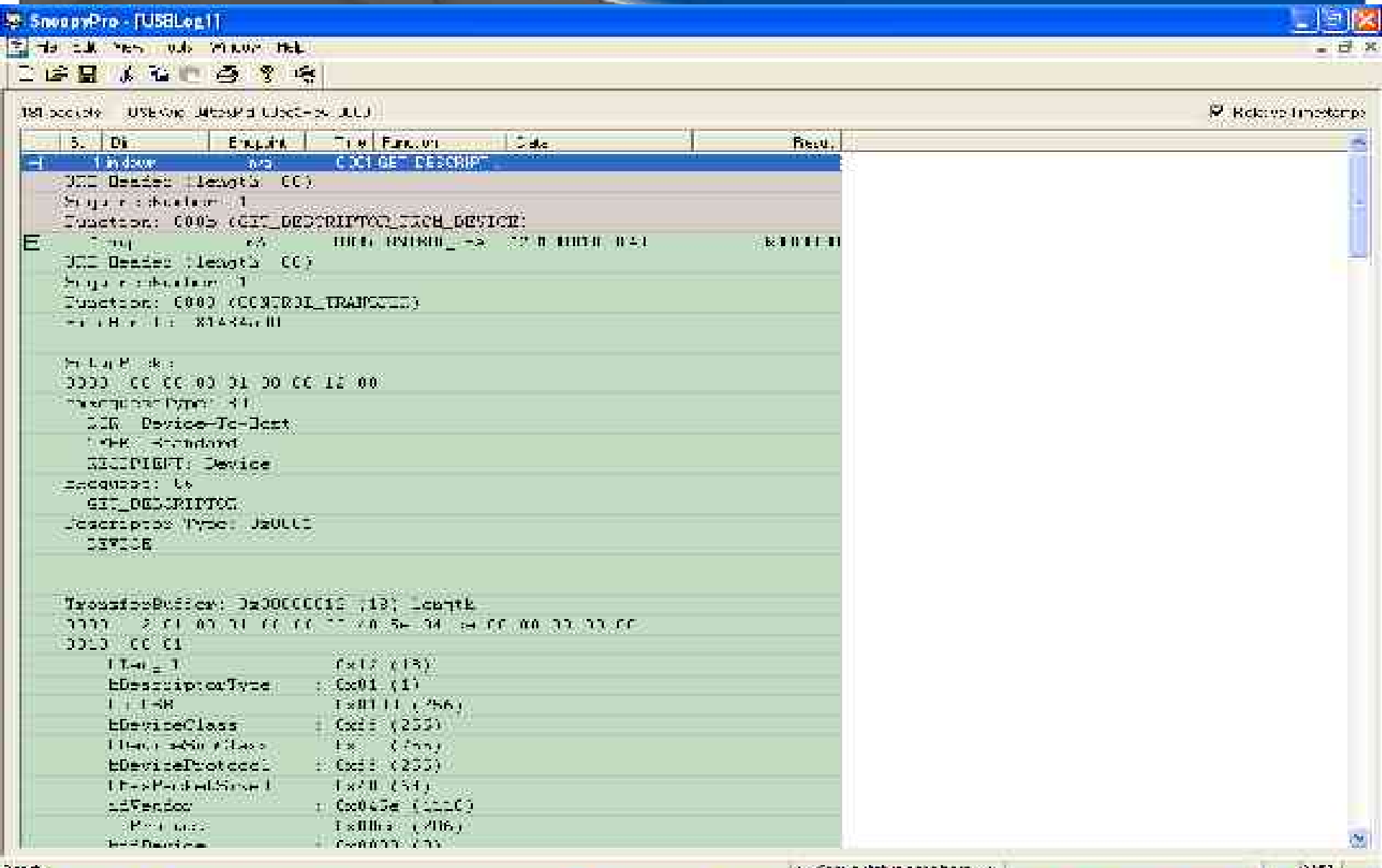
- **USB == Universal Serial Bus**
  - Devices are self identifying
    - Haven't you ever wondered why the name of the device will appear in the ballon when you plug it in?
    - "How did it KNOW!"
  - Self identification allows for specific devices to be handled by certain drivers, or if none are found, more specific drivers.
  - Many different types of devices including input devices, network devices, storage devices, etc…
  - Pack Oriented Protocol
    - Looks a lot like IP

What does USB look like?

- **USB supports many different endpoints and transfer types.**
  - Endpoints can be thought of as bytestreams.
  - IN means into the controller, OUT is out of the controller.



What does USB look like?



Get to the root issues…

- **What is a root hub?**
  - The primary hub for the USB network
  - Attached to the controller
- **USB is a typical master slave relationship**
- **The host controller will poll the USB network at a periodic frequency to detect if there is data to be transferred.**
  - If data is found the controller will setup the transfer.
    - This is why most people think USB can't be exploited.
- **USB also supplies power for its devices.**

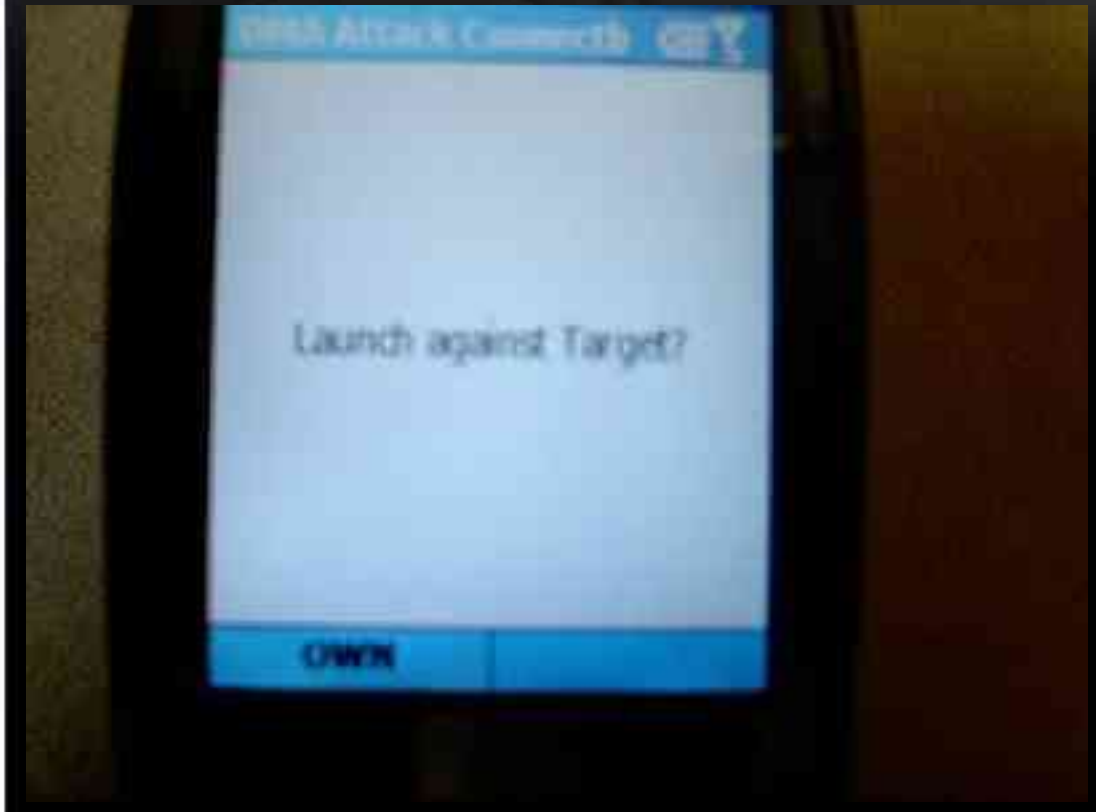
Get to the root issues…

- **OTG**
  - On-The-Go
    - USB had limited usefulness because according to the design specs you needed a host controller to set up data transfers.
    - This means one device could not connect directly to another device.
      - Like a Camera to a printer
      - USB Storage token and a Phone.
    - OTG fixes that by allowing OTG devices to directly communicate with out the need for a host controller.
      - The spec allows for a limited set of host controller functionality to be built in to the devices.
    - Who is in charge?
      - HNP == Host negation protocol

Get to the root issues…

- **Its all about power…**
  - In USB the selection relies on many things the amount current going through a certain resistor.
  - The ability to modify firmware on your attack device is key in being able to masquerade as different types of devices.
- **And the controller…**
  - What is a host controller?
    - Come in 3 varieties
      - EHCI – Enhanced Host Controller Interface
      - OHCI – Open Host Controller Interface
      - UHCI – Universal Host Controller Interface
    - Provide different functionality

Attack



INTERNET | SECURITY | SYSTEMS®

What happened?

- The unhandled exception filter in winlogon was overwritten.
- Shellcode just contains a call to MessageBoxA

Remember the virtual memory parser?

- **It is called sanity**
  - It will be released on source forge as soon as its done
  - Reads information and makes best guesses and where things are
  - Can detect SHE
    - Useful for finding overwrite targets

Other things…

- **This type of attack can be extended to PCMCIA, FireWire, AGP, and so on…**
  - Firewire has already been publicly discussed:
    - Maximillian Dornseif – Owned by an iPod
      - http://www.cansecwest.com/speakers.html
  - Video cards make greats places to hide things
    - You have to do firmware reverse engineering
    - They have more than enough power

What else?

- **The purpose of this talk was to demonstrate how security is no longer just a software only issue.**
- **There is an intresting thing happening where “the power meets the silicon.”**
  - Hardware developers are have to write more code for device drivers and such.
  - Software guys are having to spend more time thinking about hardware to get appropriate performance.
  - This leaves the device driver area a fertile ground for auditing and attacking.
  - There have already been two device driver bugs this year from Mircosoft.
    - Tcpip.sys – exploitable off-by-one dealing with the ip options.
    - Rdpwd.sys – DoS in remote desktop driver.

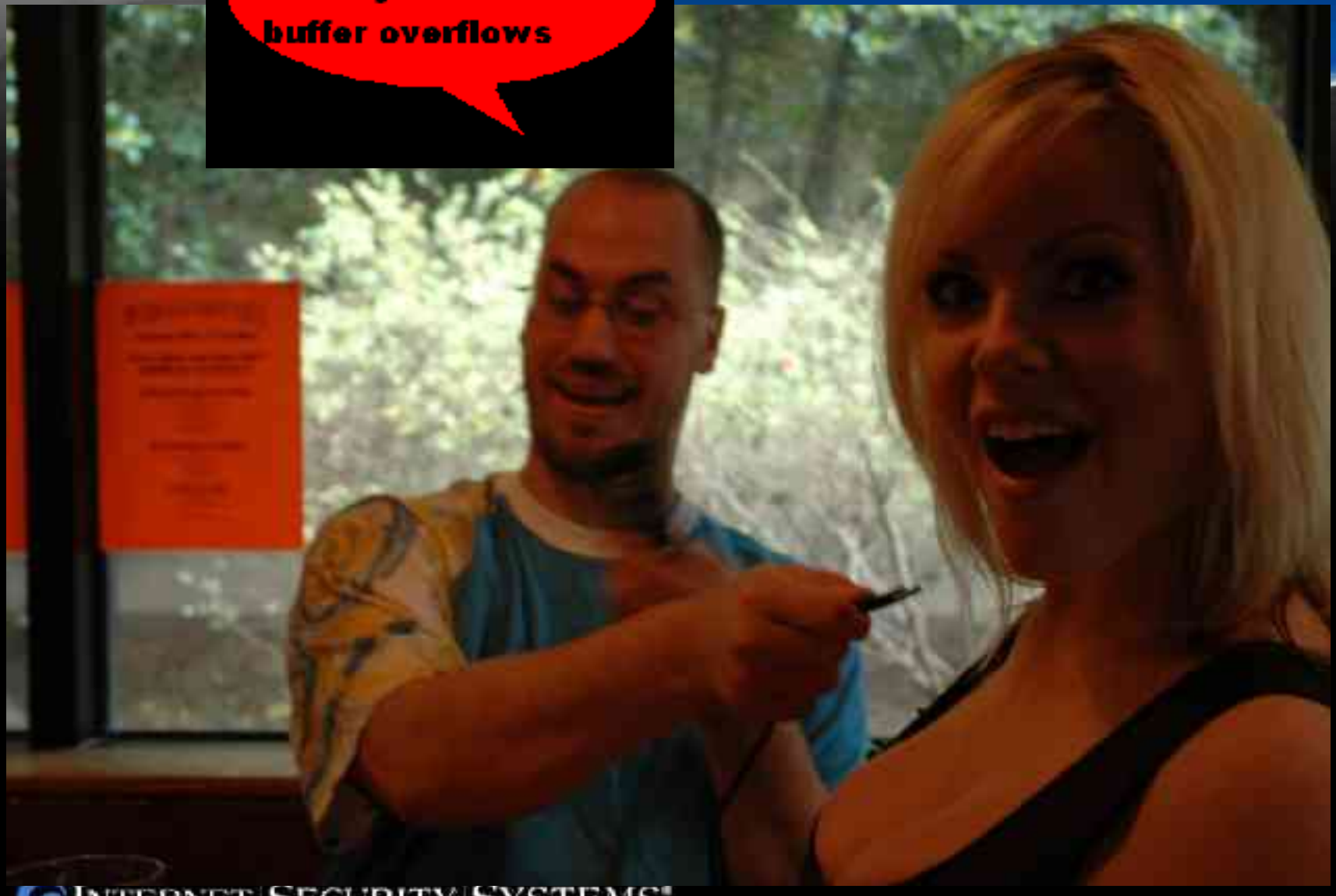
What else?

- **“I think this year or next year exploiting device drivers will be all the rage!” –Maximillian Dornseif (while eating a lot of meat and drinking beer)**
  - For full appreciation it needs to be said in a thick German accent.
- **With that being said I showed 14 examples of bad device driver coding habits at CansecWest.**
  - They were a highlight of unsafe function usage and was meant to demonstrate the code quality of device drivers.
  - After working with the very diligent MSRC it was discovered only two of the bugs could lead to an actual overflow condition, and of those two one was not in a *.sys.

Going forward

- **Fixing and releasing the USB fuzzer.**
  - It is now based on packet creation by scapy
    - http://www.secdev.org/projects/scapy/
- **New generation of smartphone and PocketPC OS, magneto.**
- **Evaluation of wireless drivers.**
  - Holy grail hack would be a remote overflow in the wireless card driver that would allow attacker to take over a machine if its radio is on.
- **Expansion of demo code to include PCMCIA and Firewire.**

at can't be owned over usb?



INTERNET | SECURITY | SYSTEMS®


I love IP fragmentation.
At last Rob, we are not the biggest dorks in the room.

After Rob and I left

INTERNET | SECURITY | SYSTEMS®

Thank You

INTERNET | SECURITY | SYSTEMS®