BIOS, Boots, and "Badies"
Part II

7th December 2011
Lexington Senior Center
Paul Lewis
paul@ComputerHomeHelp.com

NB In Part 1 the slides referring to Badies were not used due to a time limitation
Part II continues from slide 17

The Route-Plan

- Why this topic
- Explain the terminology
  - BIOS
  - BOOT
  - BOOTING
- The Bits
  - Hard disk drive HDD
  - RAM - Random Access Memory
  - BIOS - Basic Input-Output System
  - CPU - Central Processing Unit
- How the bits work together to Boot the computer
- The "Badie" invades.....
- What to do?

Why?

Because it will help you understand the operation of your computer and be aware of some useful options

- Password "recovery" (bypass) disk
- Boot a Windows 7 computer to access built-in recovery options
- Run a virus-scan on a "dead" computer
- Run a virus-scan that "reaches deeper" into the computer
- Recover files from a "dead" computer

Hard Disk Drive - Storage and Memory

- It's ALL STORAGE
- All a cluster of "boxes"
- Each "box" has a numeric address
- Each "box" contains a "chunk" of information (program or data)

Re-cap on HDD

1. It's like a big sock drawer
2. What's on the hard disk drive (HDD) ->>>
3. Ramble on Sidney.....Windows, antivirus, MS office, browser, Picasa, Google Earth etc
4. AND in a very special compartment the BOOT CODE
   More on this later.....

So What the difference?

- A hard disk drive HDD:
  - Very large storage capacity
  - Non-volatile - data is retained after power removed
  - But relatively slow read and write speeds
  - Sequential access - and data reads in large "chunks" (Think of pages)
- Random Access Memory RAM
  - Smaller storage capacity
  - Volatile - data lost after power removed
  - Very fast read access and write
  - Random access data reads and writes in small "chunks" (Think of words)

HDD vs RAM

- The HDD is appropriate for storing very large quantities of information that does not require VERY fast access
- The RAM is appropriate for "servicing" the microprocessor -
  - because operation of the microprocessor (ie running programs) requires fast random access
- When the computer is OFF all the stuff is kept on the HDD
- When we want to use the computer some stuff has to be copied from the HDD to the RAM

The Library Analogy 1

1. How do you find your book?
    1. Title -> "card catalog" -> book-shelf -> search shelf for book --> find book -> read book ->return book....

2. How do you find your file?
    1. Click an icon
    2. Windows "sees" where you clicked
    3. Sends request to disk driver
    4. Driver sends request to HDD
    5. HDD locates the sectors holding the file
    6. File data gets passed back up the chain

Library Analogy 2

- Company library and Your nearby office
- You move a few critical reports, papers notes, technical standards, specifications, to your office, open each to a particular page and start work
- You can work on them much more efficiently in these conditions
- When you're done, everything goes back the library shelves

Enter THE BIOS!

- The small program stored in the BIOS chip (Basic Input Output System) The chip is like a flash drive. The data is retained even when the power is off.
  The BIOS program starts the process of ransfering some info from:
  - HDD to
  - RAM

- The BIOS-CMOS "combination" (two little chips)
  - Random access memory (fast) for program storage and execution
  - PROM - It's like a flash drive it stores information until you decide to delete it, but it's fast read and write. For storage of changeable system parameters.

- Let's take a peep.....

RAM Contents
Normal Working Conditions

What's in RAM?

- The windows operating system (XP, Vista, windows 7)
- Plus all those little "services"
- Plus drivers for all peripherals
- and

- A selection of your files and programs are transferred from the HDD to the RAM for fast access by the processor

Demo

At this point in the presentation, the presenter should start the computer and enter the BIOS settings program then show how to change settings to make the computer start from different sources:

- CD/DVD Drive
- Hard disk drive
- USB drive

The method and keyboard key required to start this is different on different computers.

What is the BIOS and What Does it Do

The BIOS is a small memory chip that contains a few small programs. For most users these programs do not change for the life of the computer, however it is POSSIBLE to change some settings in the BIOS

1. On power-up
2. Waits for the power supply to report "all supplies good"
3. Performs a scan / test of all components, keyboard, mouse, video, hard disk drive, etc
4. Initiates BIOS code execution on other sub-systems (eg. complex video cards)
5. loads Master boot code from selected boot device
6. Passes control to boot code on the selected hard disk drive
7. Done

Start-Up Sequence

So how do we get from the computer being in the "Off " state to the Normal Operating state?

1. On power-up microprocessor "looks" for BIOS (by design)
2. BIOS code executes - selects boot device
    1. CD-ROM
    2. HDD
    3. Flash drive
    4. Floppy drive?
3. Passes Control to Master boot code on selected device
4. Boot code executes and selects one partion/OS to boot
5. Loader program on selected partition loads operating system
6. Control is transferred to the OS
7. OS loads services, drivers, and start-up programs (and "other"
8. OS requests log in credentials
9. OS displays desktop for selected user

!!! REMEMBER Critical Difference !!!

- Files (programs - good and malicious) on the HDD are like books in the library - locked up - can do no harm

- BUT

- Files (programs - good and malicious) in RAM are ACTIVE and can do anything that you, the user, can do on the computer and often MORE
  - make changes to almost any file on the machine
  - spy on your key-strokes
  - spy on your login credentials
  - send and receive messages
  - "phone home" to a malicious website and download more malicious program files

Where do the bad guys live?

- They invade usually via the browser into RAM and then get saved on to the HDD
- Then they will get loaded into RAM whenever the machine is started

The New Breed of Malware

- Sometimes the malware invades and modifies the boot code or the BIOS
- This means that every time the machine is started the malware is re-loaded into RAM and becomes active
- Sometimes this can occur BEFORE the operating system is loaded.
- This can allow the virus files to "cloak" or hide themselves
- This means that it is extremely difficult for antivirus programs to detect the presence of the infection or to remove it.

What to DO?

For example:
If you had two hard disk drives each with it's own operating system

One you use for day-today use

One you use to run diagnostics

So: If your day-to-day system became infected, you could boot the system from your other hard disk drive and run a virus scan from an uninfected system

OR
Boot your computer from a CD-ROM which you know to be virus-free

Microsoft Standalone System Sweeper - Beta

- This is a bootable CD-ROM or USB drive
- Can update the definitions file on line or off-line
- Scans the HDD without booting Windows (or root-kits)
- Microsoft supplies an ISO file for download - 64-bit and 32-bit
- You burn the file to a CD-ROM or save to a USB drive
- The File and instructions are available here:
- https://connect.microsoft.com/systemsweeper/content/content.aspx?ContentID=24894

Windows 7 System Recovery Disk - 1

Manufacturers:
Dell, Acer, HP, Toshiba, Lenovo and probably others...
Do NOT provide a real Windows 7 installation disc with your purchase

If your computer fails to boot to Windows, you have a problem!

The Bootable Windows 7 Recover Disk is the solution

File and instructions are available here:
http://neosmart.net/blog/2009/windows-7-system-repair-discs/

Windows 7 System Recovery Disk - 2

The Windows 7 DVD has

- Complete “recovery center” that provides you with
- Option of recovering your system via automated recovery (searches for problems and attempts to fix them automatically),
- Rolling-back to a system restore point,
- Recovering a full PC backup, or
- Accessing a command-line recovery console for advanced recovery purposes.

To burn an ISO see:
http://neosmart.net/wiki/display/G/Burning+ISO+Images+with+ImgBurn

Webroot finds a BIOS rootkit

Security software company Webroot says a BIOS rootkit has been found in the wild called Mebromi.
The malware is reminiscent of the IceLord proof of concept BIOS rootkit in 2007, was a late 1990s virus that was able to erase the motherboard software. This new rootkit is a different caliber as it is appears to be one of the most persistent malware programs we have heard so far.

http://www.tomshardware.com/news/security-antivirus-malware-bios-rootkit-mebromi,13447.html

Note: The discussion following the article is revealing

Note: I suspect that Windows 7 is not vulnerable to this attack

Windows 7 Recovery CD/DVD

The Windows 7 DVD has a complete “recovery center” that provides you with the option of recovering your system via automated recovery (searches for problems and attempts to fix them automatically), rolling-back to a system restore point, recovering a full PC backup, or accessing a command-line recovery console for advanced recovery purposes.

UEFI - A new version of the BIOS

http://www.pcmag.com/article2/0,2817,2393007,00.asp

If you've been around computers for any serious length of time, chances are you've heard the term "BIOS." The "basic input/output system" has been the standard interface for interacting with a computer's firmware at boot time since, well, since the beginning of home computers. But all that is gradually changing thanks to the Unified Extensible Firmware Interface, aka UEFI.

This new take on firmware interfaces brings the BIOS into the 21st century, and makes possible lots of things the dusty old interface just can't. Here's our rundown of basic facts about UEFI, and why you should care what happens on your computer before the operating system even starts.

Intel and McAfee Reveal DeepSAFE Tech

McAfee's DeepSAFE tech will keep an eye on memory and processor activity in real time, rooting out sneaky malware before they dump their payload.

Zoom

Tuesday during the Intel Developers Forum, newly-acquired and now wholly-owned subsidiary McAfee demonstrated DeepSAFE, a technology that allows McAfee to develop hardware-assisted security products to take advantage of a "deeper" security footprint.

According to the company, the tech resides underneath the computer's operating system to gain better sight on deeply-rooted malware that typically embeds themselves outside the OS to evade current security solutions. McAfee DeepSAFE technology actually provides a direct view of system memory and processor activity that other solutions currently can't access, and will expose the rootkit in real-time as it is trying to hide malware.

http://www.tomshardware.com/news/McAfee-DeepSAFE-malware-rootkit-Paul-Otellini,13436.html

Ed (Paul)
If Intel and McAfee are completely successful in preventing systems from being infected by interception at the processor level, none of the other software-based antivirus software will be necessary!

That's going to irritate the hell out of a LOT of companies currently on the anti-virus band-wagon.

Useful Links

http://www.pcguide.com/ref/mbsys/bios/bootSequence-c.html