Take 5 for Safety

USB Enabled Devices and Malware
Picture of the Week

Collider-Accelerator Department
4-3-12

BROOKHAVEN NATIONAL LABORATORY

a passion for discovery

Office of Science

USB Enabled Devices and Malware

- Majority of malware attacks are triggered by USB enabled devices and insufficient security knowledge
- Viruses jump right onto USB devices when you plug them in, including cameras, thumb/flash drives, cell phones, and MP3 players, and they will also infect the computers that you plug them into, even if you didn't voluntarily load any files from them
- All USB enabled devices should be prohibited from any device running in the operations mode. For example, do not charge a cell phone through a USB port since it may carry malware from one computer to another

Examples of USB Enabled Devices

- Two billion in 2009 and four billion USB enabled devices by 2013
  - Cell phone chargers
  - Portable battery chargers
  - USB drives
  - USB mass storage devices
  - Printers
  - Game hardware
  - Flat panel TVs
  - Digital cameras
  - USB powered air conditioned shirt
  - Mini fridge, humidifier, cup warmer, pencil sharpener, fans…

C-AD Rules to Protect Operations

- OPM 1.30.1: USB removable media must NOT be inserted into any device that is running in operations mode without approval that the media is clean of any malware, and this action must be due to extenuating circumstances or emergency remediation only
- OPM 1.30.1: USB removable media may be used on development computers, office workstations, laptops, and home computers provided they are equipped with a current version of the BNL provided anti-virus software that is updated and actively running the Real Time Scan feature
- Note: ‘USB media’ is being changed to ‘USB devices’ in the OPM

Picture of the Week: The Glory Days of Windows 95

- Plenty of time to enjoy a cup of coffee and then some