Pod Slurping

Kevin J. Slonka
Rhuel T. Adams

What's pod slurping?

- Pod slurping is the act of using a portable data storage device such as an iPod digital audio player to illicitly download large quantities of confidential data by directly plugging it into a computer where the data is held.
- As these storage devices become smaller and their storage capacity becomes greater, they are becoming an increasing security risk to companies and government agencies.
- Usually access is gained while the computer is unattended.

What's the vulnerability?

- Hosts are often left unattended
- Hosts allow USB storage devices to be connected
- Autorun is rarely disabled
- Users are stupid

How do you mitigate the risk?

- Control physical access
- Disable USB in the BIOS
  - Disables keyboards, mice, and other useful devices
- 3rd party utilities to disable use of USB storage devices
  - Vista-based hosts can do this natively
- Implement policies on hosts to disable autorun
- Training, training, training!
  - You can't fix stupid

Technical mitigation

- Group Policy
  - Disable autoplay
    - Gpedit.msc > Local Computer Policy > Computer Configuration > Administrative Templates > System > Turn Off Autoplay
      - Enabled
      - All Drives

Technical mitigation

- Registry
  - Enable write protecting of USB storage devices
    - HKLM\System\CurrentControlSet\Control\StorageDevicePolicies\WriteProtect=1 (0=disabled)
  - Disable loading of USB storage driver
    - HKLM\System\CurrentControlSet\Services\UsbStor\Start=4 (3=enabled)
      - Rename C:\Windows\Inf\UsbStor.{inf,pnf} to .bak

How do you exploit the vulnerability?

- Three approaches
  - The social engineering approach
  - The fully automated approach
  - The "it plays video games, seriously" approach

The social engineering approach

- Take the USB stick that, when plugged in, will pop a window with pictures from your vacation
- "Hey Bill, here, check out my vacation pictures."
- Bill will be amused by your pictures, not realizing the blinking light on the USB stick is actually all of his personal data being written to it.

The fully automated approach

- While a co-worker steps away, plug the automated USB stick into the back of his computer (where it's well hidden)
- Walk away
- Come back and remove the USB stick
- This can even be done in the presence of the victim if you have easy access to a well hidden USB port

Creating the automated USB drive

- U3 USB Drive
  - U3 drives are partitioned "CDROM" and "Removable Disk”
  - Not feasible to write to ISO9660 (CDROM) File System with standard system utilities
  - A 3rd party app is needed to write to ISO9660
- U3 Customizer
  - Provides a script to generate a custom .iso and "burn" it to the ISO9660 Partition of the U3 drive
  - Allows custom software to be run on the victim computer with no knowledge by the user

The "it plays video games, seriously" approach

- Most corporations do not allow the use of personal, writable storage devices such as USB sticks
- Most facility security officers don't realize that gaming devices, such as the Sony PSP, are writable storage devices

Demo

References

- "Hack U3 USB Smart Drive to Become Ultimate Hack Tool." http://www.raymond.cc/blog/archives/2007/11/23/hack-u3-usb-smart-drive-to-become-ultimate-hack-tool/ (accessed March 18, 2009).
- "How to: Simple "Podslurping" Example With a USB Flash Drive." http://www.usbhacks.com/2006/10/29/how-to-simple-podslurping-example-with-a-usb-flash-drive/ (accessed March 18, 2009).
- "USB Hacksaw." http://wiki.hak5.org/wiki/USB_Hacksaw (accessed March 20, 2009).
- "Disable USB Flash Drives." http://www.intelliadmin.com/blog/2007/01/disable-usb-flash-drives.html (accessed March 19, 2009).
- "Download." http://gonzor228.com/download (accessed March 20, 2009).
- "Test your defenses against malicious USB flash drives." http://blogs.computerworld.com/node/12946/print (accessed March 19, 2009).
- "Hacking U3 Smart USB Drives." http://www.mcgrewsecurity.com/pub/hackingu3/ (accessed March 22, 2009).
- "Pod slurping." http://www.sharp-ideas.net/pod_slurping.php (accessed March 17, 2009).
- "Pod slurping." http://en.wikipedia.org/wiki/Pod_slurping (accessed March 24, 2009).
- "Disable Writing to USB Disks with GPO." http://www.petri.co.il/disable_writing_to_usb_disks_in_xp_sp2_with_gpo.htm (accessed March 19, 2009).