Your Key to Security

CHANGES IN FORENSICS WITH WINDOWS VISTA

Daniel J. Cotton, Associate of (ISC)²
Nebraska University Consortium on Information Assurance
College of IS&T, Peter Kiewit Institute
University of Nebraska at Omaha

Windows Vista: Security Features

- **Windows Firewall**
- **buffer overrun protection**
- **data encryption**
- **User Access Control (UAC)**
- Windows Defender
- Internet Explorer
- parental controls
- data redirection
- additional security on 64-bit computers
- restrictions on removable drives

Windows Vista: Windows Firewall

- More functionality than the original Windows Firewall
- New features include:
  - filter incoming and outgoing traffic
  - Microsoft Management Control (MMC) snap-in for GUI configuration
  - firewall filtering
  - IPSec

Windows Vista: Windows Firewall

- Protection settings integrated
- More customization available
- Exceptions can be configured for:
  - Active Directory directory service accounts and groups
  - source and destination IP addresses
  - IP protocol number
  - source and destination TCP and UDP ports
  - all or multiple TCP or UDP ports
  - specific types of interfaces
  - ICMP (IPv4 and IPv6) traffic by type and code
  - services

Windows Vista: Address Space Layout Randomization (ASLR)

- Buffer overflow still one of the largest problems with programs.
  - ☹ We have known about this for years ☹
- Windows Vista could be the best piece of software ever written
  - don't quote me on that
- the problem is the amount of code that runs on top of it that is not that well written and contains numerous buffer overflows

Windows Vista: Address Space Layout Randomization (ASLR)

- ASLR is part of Microsoft's adoption of Secure Development Lifecycle
- Tries to prevent buffer overflows from giving access to trusted aspects of the operating system
- Doesn't consistently load the operating system into the same piece of memory, so an exploit that works at one point in time may not work another.
- Protecting themselves

Windows Vista: Bit Locker

- Only offered with Enterprise and Ultimate versions
- Data protection by encrypting the hard drive
- Makes use of the TPM at boot up
- Can be used in one of three modes.
  - Transparent Operation
  - User Authentication
  - USB Key Mode

Windows Vista: Bit Locker

- Transparent Operation Mode
  - most transparent to user
  - offers least amount of protection
  - uses TPM to verify operating system
  - uses TPM key to do all of the encryption/decryption silently in the background

Windows Vista: Bit Locker

- User Authentication Mode
  - requires user to either enter a pin or a USB device with a startup key in order to boot the operating system
- USB key mode
  - requires a user to either enter a USB device with a startup key
  - does not require a TPM

Windows Vista: Bit Locker

- By Default:
  - Uses Advanced Encryption Standard (AES) using a 128 bit key
    - can also use a 256 bit key
  - uses the "Elephant Diffuser"
    - optional

Windows Vista: Bit Locker

- Has been speculated that Microsoft has aided governments by putting in a backdoor to this software so that they can get into it if they want to.
- Neils Ferguson released a statement on his Microsoft blog saying that this would happen "Over (his) dead body"

Windows Vista: User Access Control (UAC)

- Pops up extra windows when a program is being run to initiate user interaction.
- Purpose is to help protect against malicious programs being run.
- The background color on these windows does differ.
- Knowing these colors will help a user know what kind of a program is being run.

Windows Vista: User Access Control (UAC)

- A red background with a red shield
  - a program from a blocked publisher or it is blocked by a group policy
- A yellow-orange background with a red shield
  - an application, signed or unsigned , that is not yet trusted by the local computer
- A blue-green background
  - a program that is an administrative application that is part of Windows Vista
- A gray background
  - a program that is Authenticode signed and trusted by the local computer

Windows Vista: Smaller Changes

- Much of this information was given in a presentation by Lance Mueller of Guidance Software at the 2007 Computer and Enterprise Investigations Conference.

Windows Vista: Smaller Changes

- Showed in a graphic that the Volume Boot Record has moved
- Journaling
  - when a file is accessed, the operating system makes a note of the event via the file system transactional journaling
    - instead of updating the file access time
  - this journaling is enabled by default, but can be turned off via the registry
  - USN Journal is an NTFS logging mechanism used to log file system transactions
    - disabled by default in Windows 2000, XP, and 2003
  - Saved via alternate data streams into a metadata file

Windows Vista: Smaller Changes

- Directory Structure
  - C:\Documents and Settings → C:\Users
  - C:\Users\All Users → C:\ProgramData
    - using a symbolic link
  - C:\Users\Default Users → C:\Users\Default
    - via a junction point
  - Junction points now used in every user's folder

Windows Vista: Smaller Changes

- Example
  - Internet History → C:\Users\AppData\Local
    - using three junction points
  - C:\Documents and Settings\All Users → C:\Users\Public
- Deleting Files and Copy Files
  - has been called unbearable
  - Vista checks each file for a protection flag before any transaction
    - including deletion

Windows Vista: Smaller Changes

- Virtual Folders
  - If a user without the appropriate permissions tries to create a folder or write to a file in a protected part of the system, they are redirected to another location
    - no error indication
    - stored at C:\Users\<user>\AppData\Local\VirtualStore\

Windows Vista: Smaller Changes

- Registry Structure
  - several new values
  - NTUSER.DAT file is still located at the user's root folder although now it's at C:\Users\<user>
  - uses a virtual registry
    - used to prevent users without administrative access from writing to parts of the registry
    - if a user installs a program that tries to write to a protected registry value, it will be redirected to a virtual registry value contained in that user's NTUSER.DAT file

Windows Vista: Smaller Changes

- Recycle Bin
  - contents and name have changed
    - now $Recyle.bin
    - when a file is deleted two files are created with the same random looking name, preceded with either a $R or $I
      - the file starting with the $R contains the data of the deleted file
      - the file starting with $I contains the path to the original file, the date, and the time that the file was deleted

Windows Vista: Smaller Changes

- Event Logs
  - now saved in a XML format with an extension of "EVTX"
  - located at C:\Windows\System32\winevt\Logs\
  - now 30 different event logs that events are saved to
  - tools that collect these need to be updated to retrieve these new event logs

FDCC

- Office of Management and Budget (OMB) mandated core configuration for operating systems in government agencies.
- Named the Federal Desktop Core Configuration.
- Windows Vista is the first operating system being used with this baseline, although an Air Force standard has been pulled in to be used as the baseline for Windows XP.
- Currently only out for Windows XP, Windows Vista, and some programs that come with operating systems.
  - they are looking to expand it however

FDCC

- Multi-agency initiative:
  - National Institute of Standards and Technology (NIST)
  - Office of the Secretary of Defense (OSD)
  - Department of Homeland Security (DHS)
  - National Security Agency (NSA)
  - Defense Information Systems Agency (DISA)

FDCC

- Tests conducted focused on the command line tools.
- The tool list is not meant to be complete. It is meant to be a general test of the freely available tools used by a forensic examiner.
- The tools, when run on Vista, were tested with both on a normally run command line as well as a command line run as an administrator.
- Major differences found are the registry values.
  - The FDCC versions had registry values that were completely removed as opposed to being merely disabled in some cases.
- The impact of FDCC with respect to Windows XP and Vista is minimal.
- The FDCC may hinder incident detection and incident response, but it will only affect it marginally.

Native to XP	Native to Vista	Non-Native
arp	arp	AFind
at	at	Autorunsc
doskey	doskey	BinDiff
gpresult	gpresult	diruse
hostname	hostname	FileStat
ipconfig	ipconfig	fport
mem	mem	getsid
nbstat	nbstat	handle
net	net	hfind
netstat	netstat	listdlls
openfiles	openfiles	LogonSessions
route	route	macmatch
schtasks	schtasks	ntfsinfo
systeminfo	systeminfo	ntlast
tasklist	tasklist	openports
wmic	wmic	procinterrogate
find	find	psexec
findstr	findstr	psfile
reg	reg	psgetsid
netsh	whoami	psinfo
		pslist
		psloggedon
		psloglist
		psservice
		pstat
		psuptime
		regdmp
		sfind
		streams
		strings
		timezone
		tlist
		uptime
		whoami

Local vs. Remote Execution

- Tested using the PsTools suite.
  - allow you to run tools remotely and locally
- If tools were preloaded on to the machine, then you could use a tool like PsExec to execute the tool remotely.
  - a possibly smaller impact on the machine being tested
- When tested, none of the PsTools worked on any of the machines.
- It may be possible that settings could be made in order to allow these to run.
  - further investigation is needed as to what settings need to or can be made to allow these tools to run

Tools That Fail Due to Windows Vista

- Only two programs encountered that were non-functional going from Windows XP to Vista.
  - uptime – displays the current uptime for the local or remote system
  - openports – port-to-process mapping utility
- When these programs are run on Vista the operating system tries to solve the problem, but eventually gives up
- When the same programs are run on Vista FDCC, the tools just fail.

Tools that Prompt UAC

- Some of the tools prompted an intervention by the UAC.
  - all of which had a gray colored background
  - shows that some of the tools tested are Authenticode signed
- Was not clear as to how Vista deciphers between the yellow-orange background of a not yet trusted application as opposed to a gray background.
- If this is just a list contained in the operating system of trusted vendors, then how does it prevent someone or something from altering that list.

Unexpected Results

- Autorunsc
  - non-administrative command line
    - asks permission to run via UAC
    - runs in a separate window that closes at completion
  - administrative command line
    - runs in the same window
- reg and schtasks
  - native tools
  - trusted versions copied form the operating system are run from another location, they do not execute
  - when run from the system, they run fine
- PsInfo
  - the installation date fails to resolve

Impact of Administrative vs. Non-Administrative

- Vista does the opposite of XP.
  - any program run, runs as a default user
  - if program needs higher privileges, the user has to "Run as Admininstrator"
    - even if you are an administrator
- When conducting a forensic examination it becomes very important to run tools using an administrative command line.
  - some commands or flags may be considered of an administrative nature and be blocked from executing
- Affects both native and non-native tools.
  - Native
    - netstat –b
  - Non-Native
    - PsFile, PsList, PsUptime, Handle, NTFSInfo

Conclusion

- As originally speculated by Jamie Morris in his article "Notes on Vista Forensics," some of the tools that need changes "may be minor"
  - these tests help to support his hypothesis
- Similarities between Windows Vista and XP aides the forensic examiner, in that they do not need to learn a whole new set of tools, let alone develop a whole new set of tools to conduct their examinations.
- When there are tools that do not work as expected and where they need to be changed, investigators can "adapt their approach accordingly, perhaps moving towards a greater emphasis on live analysis or network-based evidence collection."

Conclusion

- Don’t Panic!!!
  - Vista is relatively similar to XP
- Jaime Morris said – “playing field hasn't changed overnight just because Vista has been released to the public”

Resources

- *BitLocker Drive Encryption Technology*, [Online], Available: http://www.bitlocker.com [3 Jan 2008].
- Bott, E., Siechert, C., Stinson, C. (2007) *Windows Vista: Inside Out*, 1st Edition, Microsoft Press.
- Davies, J. (2006) *The New Windows Firewall in Windows Vista and Windows Server "Longhorn"*, [Online], Available: http://technet.microsoft.com/en-us/library/bb877967.aspx [3 Jan 2008].
- Evers, J. (2006) *Allchin: Buy Vista for the Security*, [Online], Available: http://www.news.com/Allchin-Buy-Vista-for-the-security/2100-1012_3-6032344.html [3 Jan 2008].
- *FDCC Technical FAQ*. (2007) [Online], Available: http://fdcc.nist.gov/fdcc_faqs_20070731.html [3 Jan 2008].
- *Microsoft Launches Windows Vista and the 2007 Office System to Consumers* (2007) [Online], Available: http://www.microsoft.com/nz/presscentre/articles/2007/jan07_windowsvistalaunch.mspx [3 Jan 2008].
- Morris, J. (2007) *Notes on Vista Forensics, Part Two*, [Online], Available: http://www.securityfocus.com/print/infocus/1890 [3 Jan 2008].
- Mueller, L. (2007) *First Looks: Basic Investigations of Windows Vista*, [Online], Available: www.lance mueller.com/vistaceic2007.ppt [3 Jan 2008].
- *Open Ports* (2008) [Online], Available: http://www.diamondcs.com.au/consoletools/openports.php [3 Jan 2008].
- Russinovich, M. (2007) *PsTools v2.44*, [Online], Available: http://www.microsoft.com/technet/sysinternals/Networking/PsTools.mspx [3 Jan 2008].
- Stone, K. and Keightly, R. (2001) *Can Computer Investigation Survive Windows XP?*, [Online], Available: http://www.encase.com/corporate/downloads/whitepapers/XPwhitepaper.pdf [3 Jan 2008].
- Thurott, P. (2006) *Jim Allchin Talks Windows Vista*, [Online], Available: http://www.winsupersite.com/showcase/winvista_jimallchin.asp [3 Jan 2008].
- *Uptime.exe Tool Allows You to Estimate Server Availability with Windows NT 4.0 SP4 or Higher* Uptime (2007) [Online], Available: http://support.microsoft.com/kb/232243 [3 Jan 2008].

Questions, Comments, Concerns?

Please e-mail any feedback to me at djcotton@gmail.com.

	XP Default Admin	XP FDCC Admin	Vista Default Non-Admin	Vista FDCC Non-Admin	Vista Default Admin	Vista FDCC Admin
arp	P	P	P	P	P	P
at	P	P	P	P	P	P
doskey	P	P	P	P	P	P
gpresult	P	P	P	P	P	P
hostname	P	P	P	P	P	P
ipconfig	P	P	P	P	P	P
mem	P	P	P	P	P	P
nbstat	P	P	P	P	P	P
net	P	P	P	P	P	P
netstat	P	P	P	P	P	P
openfiles	P	P	P	P	P	P
route	P	P	P	P	P	P
schtasks	P	P	P	P	P	P
systeminfo	P	P	P	P	P	P
tasklist	P	P	P	P	P	P
wmic	P	P	P	P	P	P
find	P	P	P	P	P	P
findstr	P	P	P	P	P	P
reg	P	P	P	P	P	P
netsh	P	P	P	P	P	P
route	P	P	P	P	P	P
whoami*	P	P	P	P	P	P
Afind	P	P	P	P	P	P
Autorunsc	P	P	P	P	P	P
Bindiff	P	P	P	P	P	P
diruse	P	P	P	P	P	P

FileStat	P	P	P	P	P	P
fport	P	P	P	P	P	P
getsid	P	P	P	P	P	P
handle	P	P	F	F	P	P
hfind	P	P	P	P	P	P
listdlls	P	P	P	P	P	P
LogonSessions	P	P	P	P	P	P
macmatch	P	P	P	P	P	P
ntfsinfo	P	P	F	F	P	P
ntlast	P	P	P	P	P	P
openports	P	P	F	F	F	F
procinterrogate	P	P	P	P	P	P
psexec	P	P	P	P	P	P
psfile	P	P	F	F	P	P
psgetsid	P	P	P	P	P	P
psinfo	P	P	P	P	P	P
pslist	P	P	F	F	P	P
psloggedon	P	P	P	P	P	P
psloglist	P	P	P	P	P	P
psservice	P	P	P	P	P	P
pstat	P	P	P	P	P	P
psuptime	P	P	F	F	P	P
regdmp	P	P	P	P	P	P
sfind	P	P	P	P	P	P
streams	P	P	P	P	P	P
strings	P	P	P	P	P	P
timezone	P	P	P	P	P	P
tlist	P	P	P	P	P	P
uptime	P	P	F	F	F	F

P = Pass, F = Fail, * = the whoami command run on Windows XP is not built-in, but this tool is included by default on Windows Vista

Note: The PsTools in the chart were run on the local system. These results are not for the remote runs.