

What's New For Security In Windows 7 and Server 2008-R2

Jason Fossen

SEC505: Securing Windows

<http://blogs.sans.org/windows-security>

sans.org

What's New?

"New" Relative To What?

- **90% of companies skipped over Vista.**
 - Congratulations if you decided to skip over Vista!
- **Roughly 50%-75% of Windows Servers are still running 2000 or 2003.**
- **So this talk aims to find a balance between "New versus XP" and "New versus Vista".**

Windows 7 First Impressions: Faster and Less Annoying

- **Windows 7 is really Windows Vista-R2:**
 - But being an R2 release is good! (It means *tested*.)
 - Runs faster than Vista (and sometimes even XP).
 - Boots and resumes from sleep/hibernation quickly.
 - Is less annoying than Vista (fewer UAC prompts).
 - Has fewer device driver problems.
 - It's what Vista was *supposed to be*...
- **Server 2008-R2 inherits these benefits:**
 - Plus lots of other server enhancements too.

What Is User Account Control? More Than Annoying Dialog Boxes

- **Standard User Process (the default):**
 - Medium or Low MIC label.
 - SAT stripped of dangerous privileges.
- **Administrative User Process:**
 - High or System MIC label.
 - Standard SAT for an Administrators group member.
- **How to launch programs with administrative powers:**
 - Right-click > Run As Administrator, Shortcuts, hard-coded.
- **UAC can be turned off or managed via Group Policy:**
 - Admin Approval Modes: Prompting Options
 - Standard User Approval Modes: Fail or Prompt for Credentials

User Account Control Changes

- **Fewer changes require prompting:**
 - No prompt for using Windows Update, installing Microsoft-signed drivers, adding bluetooth devices, reset NICs or otherwise fixing networking problems.
 - Fewer prompts for file operations.
 - Fewer prompts for ActiveX control changes in IE.
 - More Group Policy control over UAC details.
- **Control Panel applet (Action Center).**

BitLocker Overview

- **Benefits:**

- Verification of boot-up integrity.
- 128- or 256-bit AES sector-level encryption.
- Transparent to the user.
- TPM chip integration (optional).
- Emergency recovery options (including AD backup).

- **Requirements:**

- Windows 7 Ultimate or Enterprise (not Professional)
- Windows Vista Ultimate or Enterprise (not Business)
- Windows Server 2008 or later.
- Two drive volumes: boot-up and OS
 - Boot-up volume cannot be encrypted.

BitLocker TPM Options

- **With TPM:**

- TPM + PIN + USB
- TPM + USB Drive
- TPM + PIN
- TPM Only
 - Least secure of the TPM-required options, but 100% transparent to the user during boot-up.

- **With No TPM:**

- For older computers that don't have TPMs.
- One option only:
 - USB flash drive inserted at boot-up with key.
 - Provides no boot-up integrity protection to detect malware.

New In Windows 7: "BitLocker To Go"

- **BitLocker for Removable Drives:**
 - Requires Win7-Ent-Ult/2008-R2 or better to create, but other versions have read-write or read-only:
 - All Windows 7 and later versions can read-write.
 - Built-in reader for Windows XP/Vista/2003 to copy files.
 - Drive can be NTFS, FAT, FAT32 or ExFAT.
 - Drive unlocked by passphrase or smart card:
 - Use auto-unlock on your favorite systems.
 - Group Policy control over all aspects of USB drives.
 - Same recovery features as regular BitLocker.

Group Policy Control Of BitLocker and Removable Drives

- **Almost every aspect of BitLocker and removable drive interaction can be regulated through Group Policy.**
- **BitLocker To Go is not intended to be used in isolation, but with other GPO policies:**
 - Deny write access to plaintext drives.
 - Set passphrase policy for BitLocker drives.
 - Configure recovery options.
 - Allow only IEEE 1667 storage devices.

BitLocker Recovery Certificates

- **EFS can have a recovery certificate pushed out through Group Policy, and now BitLocker has this too!**
- **Trusted administrator will always be able to decrypt EFS and BitLocker:**
 - Recovery private key can be stored locally on the administrator's computer, in a smart card, or both.

BitLocker-Encrypted VHD Drives

- **Mount VHD files as drives:**
 - Computer Management > Disk Management.
 - DISKPART.EXE (run "help create vdisk").
 - **Encrypt with BitLocker!**
- **Boot from a local VHD file without a host OS, VM software, or a hypervisor!**
 - No special BIOS requirements, only the Windows boot loader files must be present first.
 - BCDEDIT.EXE registers VHD file as bootable.
 - Get WAIK from Microsoft for mass deployment.

AppLocker

- **Software Restriction Policies in XP/Vista:**
 - Regulate which processes are permitted to run.
 - So-called "whitelisting" and "blacklisting" of binaries.
- **AppLocker = Updated version of SRP:**
 - More precise certificate and code-signing rules.
 - Assign rules to individual users and groups.
 - An "audit only" mode for testing (writes to event log only).
 - Import/export rule sets as XML files.
- **Requirements:**
 - Only applies to Windows 7/2008-R2 and later, but SRP can still be applied to Windows XP/Vista/2008.
 - Requires at least one Server 2008-R2 domain controller.

PowerShell 2.0

- **PowerShell replaces the old CMD shell:**
 - Available for XP/2003/Vista, built into 2008/7 and later.
- **PowerShell is the future of command-line administration and scripting on Windows!**
- **PowerShell 2.0 has many enhancements:**
 - 100+ new cmdlets (Group Policy, Active Directory, others).
 - Remoting (WS-Management).
 - Background jobs (including remoted jobs).
 - WMI events consumer (synchronous and asynchronous).
 - Graphical editor and debugger.

Managed Service Accounts & Virtual Service Accounts (1 of 2)

- **Automatic password management:**
 - 240 characters, changed every 30 days by default.
- **Automatic SPN management:**
 - Only with 2008-R2 domain functionality level.
- **Requirements:**
 - Windows 7 or Server 2008-R2 service host.
 - At least one 2008-R2 controller to update schema.
 - Cannot share MSAs across multiple machines.
 - **All managed through PowerShell cmdlets.**

Service Hardening (2 of 2)

- **Unique service SIDs:**
 - Per-service DACLs
 - Virtual service accounts
- **Local/Network Service:**
 - Not Local System!
- **No session-0 interaction:**
 - “Shatter” attacks.
- **Per-service IPSec and firewall rules:**
 - netsh.exe and GPO
- **Minimum default privileges:**
 - Example: SeDebugPrivilege
 - MULTI_SZ: RequiredPrivileges
 - sc.exe qprivs
- **Write-restricted SATs:**
 - sc.exe qsidtype
 - Write access must be explicitly granted to the service.
- **DelayedAutoStart**
 - sc.exe qc BITS
- **Non-Success Error Code Stop**
 - sc.exe qfailureflag

Windows Firewall, IPSec & IPv6

- **The Good:**

- **Built-In (Free)**
- **Enabled by Default**
- **Integrated with IPSec**
- **Stateful Filtering:**
 - **Dynamic RPC Ports**
 - **Application/Service-Aware**
 - **IPv4 and IPv6**
 - **Ingress and Egress Filtering**
- **Centralized Management:**
 - **Group Policy & NETSH.EXE**
- **W3C Extended Logging**

- **The Bad:**

- **Only for Vista and later.**
- **Not for 2000/XP/2003.**
- **No IDS features.**
- **No behavioral monitoring.**
- **No centralized logging.**
- **Complex.**
- **Defense In Depth**
 - **Not just for laptops and home users, the firewall should be enabled on all systems, inside and out.**
 - **How is this practical?**

DirectAccess

- **We want 24x7 transparent access to internal servers without client VPN tunnel hassles.**
- **DirectAccess = IPSec + AuthIP + IPv6 + NAP + IPv4-to-IPv6 transition technologies + a wizard-based console to help set it all up.**
- **The DirectAccess server handles the IPv6-over-HTTPS tunneling, the main IPSec tunnel, and the initial authentication.**
- **Client has per-domain DNS settings so that internal servers are correctly resolved (IPv6).**

DNSSEC

- **Sign DNS data to thwart spoofing!**
- **Managed entirely with DNSCMD.EXE.**
- **Incompatible with dynamic updates.**
- **Only the 2008-R2 DNS server validates DNS responses, clients only confirm that a bit flag is set in the response.**
- **Use IPSec to authenticate responses.**

BranchCache

- **HTTP/SMB transparent cache acceleration:**
 - 100% transparent to users, but disabled by default.
 - Managed through Group Policy and/or NETSH.EXE.
 - **Distributed Mode:** peer-to-peer, WS-Discovery (UDP/3702 multi).
 - **Hosted Mode:** central server, queried over HTTPS.
 - Hashed file segments downloaded over HTTP in either mode.
 - File segments encrypted with "custom encryption scheme...".
 - Key can be set or exported with NETSH.EXE.
 - There'll likely be hacking tools to extract the plaintext key.
 - Use "Hosted Mode" with BitLocker on server, not peer-to-peer.
 - Data on shared computers might be at risk:
 - Run "netsh.exe branchcache flush" to clear local file cache.

XML Event Logs

- **Event Log data stored as XML now:**
 - \Windows\System32\winevt\Logs*.evtx
 - EVTX files are compressed XML.
 - Maximum log file size: 18 million terabytes.
- **Easily attach a task to an event type:**
 - Creates a new task in Task Scheduler.
- **Subscribe to remote event logs:**
 - Somewhat laborious to configure securely.

Group Policy Control Of Audit Policy Subcategories

- **Many new audit categories in Vista/2008/7:**
 - Very precise control over what gets logged to the XML files.
- **In Vista, you had to use AUDITPOL.EXE:**
 - `auditpol.exe /get /category:*`
- **In Windows 7/2008-R2, you can use both Group Policy and AUDITPOL.EXE.**

Restrict NTLM: Completely or Partially

- **NTLM is less secure, slower and less scalable than Kerberos.**
- **Audit-only mode records what *would have been blocked* by disabling NTLM.**
- **Restrict incoming and/or outgoing.**
- **Define exceptions for older systems or systems running older applications:**
 - Exception list can use wildcards.

Active Directory Recycle Bin

- **Restore deleted objects, including all of their properties, links and metadata, for up to 180 days after deletion.**
- **Requires 2008-R2 forest functionality:**
 - Every controller must be Server 2008-R2 or later.
 - Once enabled, can never be disabled again.
- **Enabled and managed with PowerShell:**
 - The scripting is not difficult, and graphical wrappers are available for free, e.g., www.PowerGUI.org.

Internet Explorer 8

- **IE8 SmartScreen Filter = IE7 Phishing Filter:**
 - MS web service of known-bad URLs (phishing and malware).
 - Looks for "phishy pheatures" in web pages.
 - XSS Filter examines browser-server exchanges.
 - Manual and/or automatic checking.
 - Report bad web sites for examination.
- **InPrivate Filter:**
 - Increase privacy against multi-site tracking attempts.
 - InPrivate Browsing maintains no history or cookies at all.
- **New Per-Tab Architecture:**
 - Each tab is a separate IEXPLORE.EXE process.
 - Each tab can have a different Protected Mode state.

Windows XP Mode

- **Similar to VMware Unity:**

- Virtual PC + XP-SP3 VHD + Desktop Integration.
- Applications appear to be running on the host Windows 7 desktop, not in a separate VM window.
- Install applications into the VM, distribute the VM to Windows 7 workstations, then launch applications using the Start Menu in Windows 7 (not in the VM).
- Important for backwards compatibility.
- Requires virtualization support in the CPU though.
- Can use Microsoft MED-V for mass deployments.

Improved Resource Monitor And NETSH.EXE Tools

- **Analyze on a per-process basis:**
 - Listening ports, network connections, file handles, loaded modules, and disk activity statistics.
 - Nice for malware analysis and troubleshooting.
 - Why didn't they just install Process Explorer???
- **NETSH.EXE**
 - Many small enhancements, a great tool! Examples:
 - `netsh.exe wlan set hostednetwork ?`
 - `netsh.exe mbn show interfaces`

Microsoft Security Essentials

- **MSE is free for Windows XP/Vista/7:**
 - Windows Defender installed by default on 7, but it's removed once MSE is installed.
 - AV-Test.org results are pretty good so far, but too early to tell if Microsoft can keep it up (especially if Forefront Client Security sales are bad).
 - You might keep your favorite AV on your Windows 7 host, then save money by only using MSE in XP Mode VMs. Or, use the threat of migrating to MSE to get a better deal from your current AV vendor.

Migrating From IIS 6.0 To IIS 7.5 On Server 2008-R2?

- **New GUI for new XML system.**
- **Highly modular architecture.**
- **SSL-encrypted remote administration.**
- **Precise delegation of authority.**
- **WebDAV authorization rules.**
- **URL Rewrite Module.**
- **FTP Over SSL.**

And More...

- **PKU2U = certificate authentication.**
- **Group SIDs for certificate auth in SAT.**
- **Problem Steps Recorder (psr.exe).**
- **Event Tracing enhancements.**
- **Previous File Versions.**
- **Task Scheduler (schtasks.exe).**

Thank You!

