SOPHOS

Windows 8: Redmond's Safest Operating System Ever?

By Chet Wisniewski, Senior Security Advisor, Sophos, 2012

A SophosLabs technical paper - October 2012

With its Windows 8 operating system Microsoft has introduced sweeping changes to the desktop environment. While much of the discussion around Redmond's new operating system has been around the naming convention of its Modern UI interface and its touch-friendly tiles, it's equally helpful to examine Windows 8 from a security standpoint.

Technology Features

Secure Boot

The first feature owners of a new Windows 8 PC will benefit from is known as Secure Boot. All new PCs that are certified for Windows 8 must utilize the UEFI (Unified Extensible Firmware Interface) standard, rather than a traditional BIOS. UEFI must be configured to only launch boot loaders that are signed by trusted authorities. Vendors shipping Windows 8 certified machines will trust Microsoft's signature, but are not prohibited from including others or allowing end-users to import their own.

This change will go a long way towards ending traditional boot sector malware. Going back to the 1980s MBR-based viruses and other malware have been able to hide simply due to the fact they are able to load before the operating system. Whatever your opinion on how this may restrict operating system choice, ultimately, it's a win for security.

Immediately after Microsoft's boot loader is launched it will validate the signature of the Windows kernel and continue to the next new optional boot component, ELAM.

ELAM (Early Load Anti Malware) is designed to enable security vendors to validate non-Windows components loaded during startup. In addition to the Windows kernel verifying that all boot driver signatures are valid, a bare-bones anti-malware engine may also be used to check drivers before they are loaded.

Exactly how effective the feature will be against today's sophisticated threats remains to be seen, but it's a step in the right direction, and could prove useful in rootkit cleanup (e.g. in preventing malicious components from being loaded).

The last new boot component is known as Measured Boot and requires the PC to have a Trusted Platform Module (TPM) which is also enabled. All components loaded during the boot process will record measurements, such as how long they took to initialize, to the TPM.

After the boot is complete the results can be sent to a trusted external entity to verify that only wanted code was executed and that it behaved in an expected manner. Few computers today ship with TPMs and this seems like it could be highly error-prone. It remains to be seen whether the benefit will outweigh the overhead, and additional cost.

Microsoft has also beefed up some of the more traditional exploit mitigation technologies introduced in Windows Vista and 7. Address space layout randomization (ASLR), data execution prevention (DEP) and heap randomization have all been updated to strengthen their protection against buffer overflow and other stack-based attacks. For something nearly invisible to users, this should help to harden Windows against attacks.

User-Facing Features

So far all of the features we've evaluated have been "behind the scenes" work that shouldn't impact day-to-day users of Microsoft's latest OS. We will now explore how this new approach interacts with those users.

SmartScreen

SmartScreen, a technology Microsoft introduced in Internet Explorer 9, has now been expanded to cover all executables downloaded onto Windows 8 systems. SmartScreen is designed to take a checksum of an EXE and compare it to Microsoft's cloud database of known good and bad application checksums.

If the result is unknown, Microsoft will warn the user before execution that this program could be malicious and is of unknown provenance. Microsoft insists this feature protected millions of IE 9 users from harm, but I remain unconvinced.

In testing it reminded me of a constant false alarm that triggered scary messages frequently enough on innocent files that I learned to ignore the warnings and, occasionally, put myself in harm's way.

Consumers will be happy to hear that Microsoft is now including basic anti-virus protection courtesy of its Windows Defender tool. While most businesses require more comprehensive protection, not to mention centralized control, reporting and updating, home users will likely appreciate the basics being thrown in for no extra charge.

Microsoft's free home anti-virus product, Security Essentials, hasn't fared all that well in recent independent testing, but it should be good enough for most home users, and would likely stop freshly installed copies of Windows from being instantly compromised.

DirectAccess

DirectAccess was a nifty new VPN solution when first added to Windows 7, with one problem. It required IPv6 to operate, resulting in almost zero adoption. Windows 8 is taking another crack at it, but this time with IPv4 support.

The concept of an always-on VPN is a good one and could likely go a long way towards protecting corporate users who frequently get online at unsecured WiFi hotspots at airports, hotels and coffee shops.

Windows To Go

Another security effort aimed at mobile users in enterprise environments is Windows To Go. This feature allows an enterprise licensed Windows 8 user to take their entire desktop with them on a USB memory stick.

It appears that Windows To Go is intended to go head to head with virtual desktop initiatives (e.g. booting from your PC from any PC that supports USB booting). Access to hard disks and other potentially dangerous peripherals is disabled when in To Go mode, but all of your files, preferences and programs are there for your convenience.

I could certainly see this being a safer option for companies who want employees to be able to connect from home PCs without opening up VPN access to untrusted home computers.

Modern User Interface

Last, but not least, is the much discussed Modern Interface and associated security features. Modern is based on the App Store concept that Apple pioneered with iOS. All applications (with one caveat) must be installed directly from Microsoft and must meet Microsoft's privacy and safety standards.

Walled gardens sound good, but the devil is in the details especially when you compare Apple's approach with that of Google. Google Play has evolved into a safer world, but it has been plagued with many more issues that seem to result from Google trying to exercise less control and offer a more open playing field.

Enterprise environments will have the option to load their own trusted certificate onto devices that will allow side-loading of applications. This is similar to iOS and is far more controlled than the tick-box approach that allows for a wild West of unknown applications being loaded on Android.

When applications are viewed in Microsoft's store a granular list of requested permissions is available, similar to what is seen on Android devices.

This list, however, is only available if you select the Details tab. There is no prompting to raise awareness of this privacy feature. This may be a good thing as asking users to make decisions too frequently leads to the "always saying yes" problem that plagues SmartScreen, but it would be beneficial if the permissions appeared on the default installation screen rather than hidden behind a tab.

IE 10

Windows 8 introduces a new dual personality version of Internet Explorer 10. While IE is largely unchanged in "Desktop" mode, it operates in a far more limited mode when used as a Modern UI application.

The Modern UI IE eschews support for plugins, with the rare exception of a whitelist that allows Adobe Flash (which is native to IE 10) to execute on a Microsoft managed list of sites. With that comes the inability to patch when Adobe announces their availability as users will need to wait for a Microsoft update rollup. Enterprises that require Java or other proprietary plugins will find, in most cases, they will need to use Desktop mode, erasing most of the advantages offered by the Modern UI.

Another problem with the Modern UI version of IE is that it hides the location bar when surfing. While hiding the location bar may make the user experience more seamless, eliminating the visual indicators they depend on to determine if a site is encrypted (e.g. padlocked, verifying the address of the site they believe they're on), could make it harder for users to protect themselves from online harm such as phishing.

All applications that use the Modern UI are required to operate within a sandbox. This limits the attack surface and largely prevents applications from interfering with or attacking other applications on the system.

Microsoft is limiting access to Application Programming Interfaces (APIs) to only those explicitly declared in an application's manifest file. This will prevent applications with vulnerabilities from being exploited to steal confidential information or access system resources their authors never intended.

An extension of this concept is what Microsoft refers to as contracts. Applications are allowed to declare they are a source or destination of information for other Modern apps. For example the Twitter app might declare an inbound contract for social messaging. This would allow a photo app to send a picture to the Twitter app for sharing purposes.

Apple does not allow applications to reach outside of their sandboxes, nor to interact with other applications. Microsoft is certainly increasing the attack surface by allowing applications to talk to one another, albeit through a restrictive interface. It remains to be seen whether this is a tactical advantage or a security mistake.

The Safest Windows Ever

In summary, Windows 8 isn't blazing any innovative trails into a perfectly secure future; still, it offers improvements that can and will lead to a safer Windows experience. I don't see anything (other than the new IE interface) that truly concerns me.

The big question that remains is this: will enterprises with their investment in training and legacy hardware embrace an entirely new user interface so soon on the heels of Windows 7 deployments? I don't think the incremental improvements in security will sway this decision, but there is no doubt that this is the safest Windows operating system ever.

United Kingdom and Worldwide Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

3497.dsna.10.12

SOPHOS