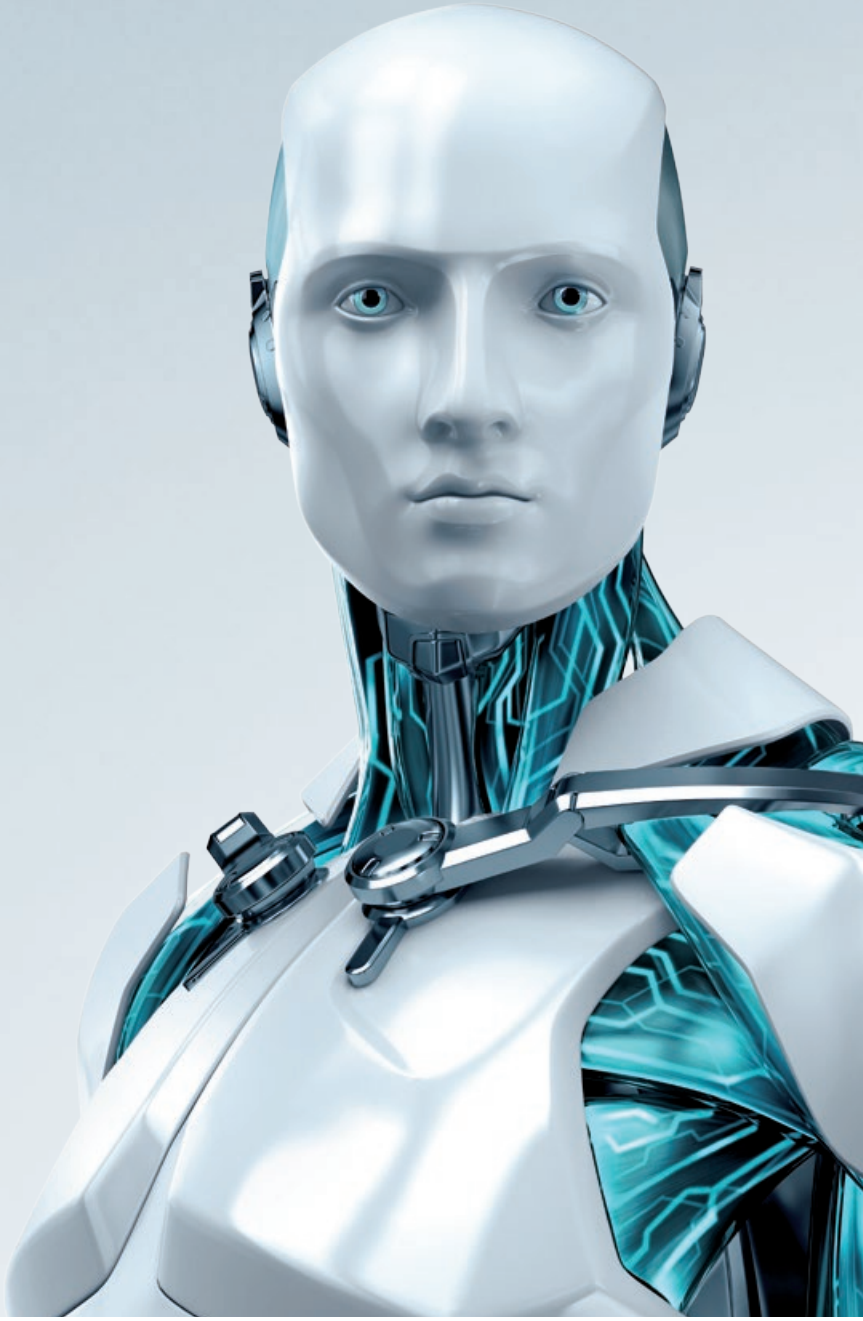
Windows® 8.1 Security

New and Improved



ENJOY SAFER TECHNOLOGY™

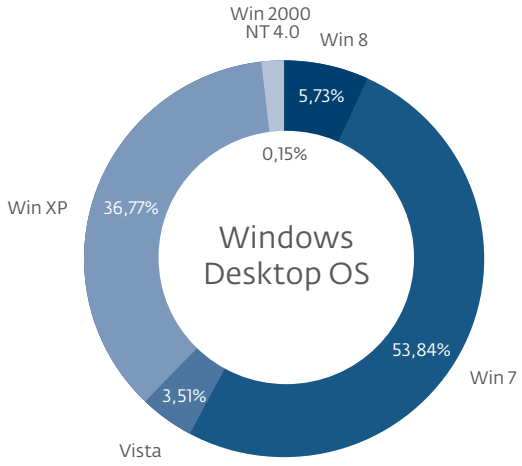
Windows® 8.1 Security – New and Improved

Contents

Introduction

The release of Windows 8.1 may have been more eagerly anticipated for the changes it makes to the Start Screen than for the security improvements it brings, but despite being 'just a point release' there are quite a few *under-the-hood* improvements[1,2,3], to Microsoft's flagship desktop operating system. If you have not done so already, you may wish to review our earlier articles, *Windows 8's Security Features* and *Six Months with Windows 8* to familiarize yourself with what was new in Windows 8.0

Since ESET's last paper on Windows 8[4], nearly half a year ago, it was in use by about 3% of our customers, compared with 49% running Windows 7 and 44% running Windows XP. How has Windows 8 fared since then? the following pie chart shows current Microsoft Windows desktop operating system percentages based on telemetry provided by *ESET Live Grid®* as of mid-November, 2013:



In the past six months, Windows 8 usage has doubled to nearly 6% [note that this covers both Windows 8 and 8.1]. Windows 7 remains the top operating system, having increased to a 54% share. Windows XP continues to hold on to second place, despite a 7% drop in usage to 37%. As Windows XP's end of life approaches in April 2014, we can expect these trends to accelerate.

But for now, let's return our focus to Windows 8.1 and peel off the wrapping off the box to take a look at some of the most important features for both businesses and consumers in this latest iteration of Microsoft's flagship desktop operating system.

Putting a finger (print) on it

One of the biggest changes to Windows 8.1 is its improved support for reading fingerprints[5,6]. While fingerprint readers have been a staple of business laptops for over a decade now, they have never been used to the same extent in the consumer space. This is probably due to the increased device cost in the more price-sensitive consumer market as well as the additional complexity of integrating them into user experience: not just with the operating system, but with third-party software[7] as well, such as web browsers. In Windows 7, Microsoft introduced the Windows Biometric Framework API (applications programming interface) to simplify development of such technologies, but Windows 8.1 has made it much easier for developers to take advantage of fingerprint reading technology.

By handling the scanning of fingerprints to register them within the system, as well as extending their management within the operating system, Microsoft has made it easier for both hardware manufacturers and third-party software developers to develop usage scenarios and applications around fingerprint registration that go beyond simply authenticating a person at login.

Another advantage of using fingerprint readers is that as Windows becomes dominant on more devices such as tablets and smartphones, fingerprint scanning will become an easier way to identify a user, especially when typing a complex password may be made more difficult by lack of access to a traditional keyboard.

It should be noted, though, that for high security applications and environments, a single form of authentication – no matter how secure – should not be used solely to provide access. a scan of a fingerprint could be coupled with entering a password, passphrase or with another access device such as a smartcard or access token in order to authenticate a person.

InstantGoing where no version of Windows has gone before

Another area in which Microsoft has improved upon Windows 8.0 is that of Connected Standby. First introduced in Windows 8, under Windows 8.1 the feature has been renamed to InstantGo[8]. While InstantGo is not a security feature *per se*, it does have important implications for device manageability and integrity, which are security concerns.

So, what exactly is InstantGo? Simply put, InstantGo is a new ultra-low power "sleep" mode built into new PCs, which allows the CPU, storage, network adapter and motherboard to continue to

operate when a computer is asleep, but in a greatly reduced power mode that consumes a fraction of the electricity that more traditional 'doze' states require. PC's have had sleep (S3) and hibernate (S4) states for nearly twenty years using *Advanced Configuration and Power Interface* (ACPI) standard, but in those modes, all programs were suspended.

With InstantGo, the PC will remain connected to the Internet, and Modern Windows Apps will continue to receive updates, even in this new low power state. Windows 8.1 will also have the ability to suspend and pause applications, in order to reduce energy use even further.

As InstantGo is a new technology (or at least a refinement of one about a year old), we have not had a chance to do an exhaustive study of applications and services which make use of it. However, it sounds like InstantGo will allow developers to provide some interesting new features in several areas. Here are a few scenarios we envisioned:

- additional remote device management
- updates to software (including downloading anti-malware signature updates)
- improvements to anti-theft tracking and reporting

It's important to bear in mind that conventional activities which require a fully-powered system can't be performed while a system is in low-power mode. So (for example) don't expect to install software or run an on-demand scan for malware on a PC while it is asleep, but it should eventually be possible to push updates and new configurations to devices, and have those install or come into effect when the device goes to full-power mode.

It should also be noted that while the system requirements for InstantGo are modest, it only works on the latest hardware, so organizations wishing to take advantage of it will need to upgrade their fleet of computers in order to realize any of its benefits.

Evolutionary encryption

File system level encryption is not a new feature to Windows: It was in Windows 2000 that Microsoft introduced the Encrypting File System[9] (EFS) almost fifteen years ago, a feature which has allowed the operating system to encrypt individual files, directories or disk volumes. It was not until the release of Windows Vista in 2006 that full disk encryption (FDE) was added in the form of BitLocker Drive Encryption[10,11]. Since then, BitLocker has been updated in each subsequent version of Windows, adding improved functionality and even providing limited support under Windows XP for reading (but not writing to) BitLocker-encrypted drives. Regardless of which encryption technology or technologies are being used, though, there is always one feature that has remained the same, and that is that they have always had to be enabled by the person managing the computer.

With Windows 8.1, Microsoft has introduced pervasive Device Encryption[12]. And what exactly does that mean, pray tell? It means that if the PC's hardware supports it, all disks will automatically be encrypted. To simplify key management, a backup copy of the recovery key for the system is either stored in

the *Active Directory Domain Services* if the user account is a domain account, or "in the cloud" on SkyDrive if the user account is Microsoft Account.

With device theft a continuing issue for businesses, institutions and any organization with portable devices, encryption has become a topic at the forefront of most IT departments' radar (and budgets). Having FDE integrated at the operating system level and managed using familiar existing tools will greatly reduce the administrative overhead for IT managers. However, like the aforementioned InstantGo technology, only the newest systems are capable of taking advantage of this technology.

Defender of the Realm, Revisited

For Windows 8.0, Microsoft re-badged its Microsoft Security Essentials product, renaming it as Windows Defender, creating a new modern user interface, introducing drivers for Early Launch Anti Malware support and bundling it into the operating system. While Windows 8.1's Windows Defender does not have as many changes as its predecessor, it does contain some new and improved functionality[13,14,15]:

- Windows 8.1's Windows Defender now implements an intrusion detection system (IDS) at the network level to continuously monitor the connections and identify potentially malicious behavior patterns. In this respect, the software is behaving like a classic virus scanner, except that instead of scanning files it is scanning network traffic.
- Similarly, Windows Defender adds another technology to Windows Defender 8.1 at the operating system level: its *Host Intrusion Prevention System*, or HIPS, will allow it to monitor system memory, the registry and file system for malicious activity.
- Another new addition is that ActiveX controls downloaded by Internet Explorer are now scanned automatically before execution.
- Unspecified improvements to cloud-based detection.

While none of these announcements address novel technologies (in particular, IDS technology first in first appeared in third-party Windows programs in the Windows 95 era) all of these steps mean *additional* layers of protection for users of Windows 8.1, and that is definitely a good practice from a security perspective.

New features, yes, but new risks as well?

Microsoft classifies some of these improvements under the umbrella term *Microsoft User and Device Authentication*[16]: for example biometric authorization, TPM 2.0 and virtual smart cards. These technologies are designed to make mobile devices more secure and manageable in the enterprise, but do improvements in user authentication have further implications for security and privacy as well?

As noted above, Microsoft's pervasive drive encryption technology will potentially store decryption keys for users' drives in their SkyDrive accounts. This brings up some interesting and potential risks for people such as investigative reporters, whistleblowers and peaceful activists when their computers are seized by a government. Microsoft, like other businesses, has to respond to legal requests from

law enforcement agencies for access to things like user accounts. Does this include the decryption keys for the computers' hard disk drives? If so, it may be better for those with privacy requirements to continue to rely on third-party disk encryption technologies for which decryption keys cannot be obtained through legal mechanisms.

Should I stay or should I go?

These are, I should mention, not the only enhancements to Windows 8.1's security: Internet Explorer 11 now defaults to Enhanced Protected Mode (EPM) on the Desktop[17] ; Windows 8.1 contains mitigations for a type of "pass the hash" (PtH) attack—at least when when used in conjunction with Windows Server 2012 R2[18]; Assigned Access allows certain versions of Windows 8.1 to be locked down to running a single Modern Windows app[19,20]; and there are additional improvements to security and usability throughout the operating system as well. These, along with other features, mean that Windows 8.1 is *more* than a service pack when it comes to improving security, while the incremental nature of many improvements mean Windows 8.1 is less than a brand new operating system version.

That does not, however, answer the question of whether all users of Windows 8.0 should adopt Windows 8.1. From strictly a security perspective, the answer is *yes, you should upgrade*, however, there are also some important factors to consider, which means a probably has to be thrown somewhere in there.

Windows 8.1's curious processor affinity

First, there are some additional hardware requirements in Windows 8.1 over the previous Windows 8.0. In particular, if wish to install a 64-bit version of Windows 8.1, both the CPU and motherboard's chipset must support three particular processor features, `CMPXCHG16b`[21], `PrefetchW`[22] and `LAHF/SAHF`[23].

- The first CPU instruction, `CMPXCHG16b`, is used by the processor to exclusively fetch and perform operations on the contents of memory in small 16-byte increments.
- The second CPU instruction, `PrefetchW` is used to load 32-bytes of data into the processors L1 (on-die) cache.
- The third pair of CPU instructions, `LAHF/SAHF`, are used to manage instructions used for virtualization and handling floating-point conditions.

Now, all of these processor instructions have been in use by various AMD and Intel processors and their accompanying motherboard chipsets for at least the last six to eight years. If you are still using a computer that is this old, it may be time to purchase a new computer, as opposed to trying to run Windows 8.1 on it. There are a few alternatives available, though. (1) You can remain on Windows 8.0, which will be supported until 2015; or you could (2) install the 32-bit version of Windows 8.1, which does not have these requirements; or (3) downgrade to Windows 7, which will be supported until 2020.

To check whether your computer's CPU is compatible with Windows 8.1, you should check with the manufacturer, run a program like

Microsoft Sysinternals' *Coreinfo*, or even run a third-party program such as *AIDA64*, *CPU-Z* or *HWiNFO*. I would be remiss, though, if I did not note that ESET is not in a position to endorse these programs or guarantee their accuracy, and therefore cannot accept responsibility for any problems they might cause with your system.

The hard truth about operating system upgrades

Somewhat related, although definitely less esoteric than processor instruction sets, are concerns about software compatibility. Most software that is written for Windows 8.0 should work under Windows 8.1 without adjustment. But there are certain classes of software which may themselves need an update for Windows 8.1 compatibility. In particular:

- security software, which not only includes anti-malware software like ESET's but also biometric authentication, file and disk encryption and VPN software;
- software which directly controls hardware, such as that used for tape backups and creating some kinds of optical media and data recovery;
- device drivers for certain types of hardware such as printers, storage controllers and network adapters, which may need to be updated as well to make use of new features in the operating system

In ESET's case, both versions 6 and 7 of our consumer software are compatible with Windows 8.1—version 6 needs to perform a regular signature update, though, before a machine is upgraded from Windows 8.0 to Windows 8.1, while version 7 is compatible as-is when downloaded, installed from a CD, and so forth. Version 7 is also a free upgrade for users with an existing, valid license. For ESET's business users, support for Windows 8.1 is forthcoming, and the latest information may be found in ESET Knowledgebase Article #2893, *"What operating systems are ESET's business products compatible with?"*

If you have a concern about software or hardware compatibility, it is always a good idea to check with your computer and software vendors before upgrading to Windows 8.1. You may also decide to perform a clean install of Windows 8.1 and then reinstall any applications and data you need.

Microsoft Windows 8 handles upgrades much better than previous versions of Windows, and Microsoft provides excellent advice and instructions throughout the upgrade process. However, regardless of what decision you make about how to install Windows 8.1 on your computers, we strongly recommend that you first make a backup of any valuable data. For more information backups, I refer you to an earlier blog post at ESET's We Live Security, *Backup Basics*, along with the paper that accompanies it.

A double-edged sword

The last concern I wish to touch on is perhaps the most difficult one to communicate, and that is the potential risks associated with the decryption of drives encrypted using Device Encryption. To date, this feature is only available on a handful of devices, but it does remain a real-world concern, especially as new computers enter the market with this functionality built-in to them. And let's be clear:

It does offer users a genuine advantage in security if there computer is lost or stolen.

But the implementation of how recovery keys are stored, at least for home and small business users who use a homegroup or workgroup and not an Active Directory domain, means that users will have to carefully take a look at the risks involved and in particular at who might be able to access those keys.

While this is probably a problem that is not going to affect most home or even most business users, a careful accounting of the risks needs to made if your computer is being used for something a government may not like, as mentioned above in the section, "*New features, yes, but new risks as well?*" It is worth noting, though, that Windows 8.1 is still relatively new, and we still might see improvements on how Microsoft Windows 8.1 stores recovery keys for Device Encryption.

Conclusion

On the face of it, Windows 8.1 seems to be a worthwhile upgrade to Windows 8. the improvements to biometrics, manageability and, yes, even Windows Defender make it an obvious choice. However, there are potential privacy concerns, as well as potential hardware compatibility issues as well. If you verify these are non-issues for your computers, Windows 8.1 is a useful and meaningful upgrade.

The author would like to thank his colleague, ESET Senior Research Fellow David Harley, for his assistance with this paper.

Aryeh Goretsky, MVP, ZCSE
Distinguished Researcher

References

1) Microsoft. "What's Changed in Security Technologies in Windows 8.1." Published Aug. 21, 2013. Microsoft TechNet. http://technet.microsoft.com/en-us/library/dn344918.aspx
2) Ingalls, Dustin. "Black Hat 2013: Windows 8.1 Helps keep Data Secure in a Modern Environment." Published Aug. 2, 2013. Microsoft Windows Blog. http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/windows-8-1/enterprise-edition.aspx
3) Microsoft. "What's new with Windows 8.1 Enterprise." Microsoft. http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/windows-8-1/enterprise-edition.aspx
4) Goretsky, Aryeh. "Six months with Windows® 8." ESET. http://www.eset.com/us/resources/white-papers/ESETNA-5165-Six-Months-with-Windows8-v5FIN-WP-20130603.pdf
5) Microsoft. "What's New in Biometrics in Windows 8.1." Published July 24, 2013. Microsoft TechNet. http://technet.microsoft.com/en-us/library/dn344916.aspx
6) White, Christopher. "Windows 8.1 will focus on biometrics for authentication." Published June 5, 2013. Neowin. http://www.neowin.net/news/windows-81-will-focus-on-biometrics-for-authentication
7) Soni, Himanshu. "Biometrics – fingerprints for apps." Microsoft Build 2013 conference. Microsoft Developer Network. http://channel9.msdn.com/Events/Build/2013/2-9110
8) Microsoft. "Introduction to Connected Standby." Published Sept. 28, 2012. Microsoft Developer Network. http://msdn.microsoft.com/en-us/library/windows/hardware/jj248729.aspx
9) Wikipedia. "Encrypting File System." Retrieved Oct. 19, 2013. https://en.wikipedia.org/wiki/Encrypting_File_System
10) Microsoft. "BitLocker Driver Encryption." Retrieved Oct. 19, 2013. http://windows.microsoft.com/en-US/windows7/products/features/bitlocker
11) Wikipedia. "BitLocker." Retrieved Oct. 19, 2013. https://en.wikipedia.org/wiki/Bitlocker
12) Microsoft. "What's New in BitLocker for Windows 8.1 and Windows Server 2012 R2." Microsoft TechNet. Published June 24, 2013. http://technet.microsoft.com/en-us/library/dn306081.aspx
13) Microsoft. "Windows 8.1: Frequently Asked Questions." Microsoft TechNet. http://technet.microsoft.com/en-us/windows/jj721676.aspx#security
14) Roman, Pierre. "Windows 8.1 Preview Security Revisited." Microsoft TechNet. Published Aug. 8, 2013. https://blogs.technet.com/b/canitpro/archive/2013/08/08/windows-8-1-preview-security-re-visited.aspx
15) Ingalls, Dustin. "Black Hat 2013: Windows 8.1 Helps Keep Data Secure in a Modern Environment." Windows Blog. Published Aug. 2, 2013. http://blogs.windows.com/windows/b/business/archive/2013/08/02/black-hat-2013-windows-8-1-helps-keep-data-secure-in-a-modern-environment.aspx
16) Porter, Nelly. "What's New in Windows 8.1 Security: Modern Access Control Deep Dive." Microsoft TechEd Europe 2013. Published 28 June 2013. http://channel9.msdn.com/Events/TechEd/Europe/2013/WCA-B375#fbid=RZXR8Jf2X0D
17) Microsoft. "Privacy and Security." Internet Explore Dev Center. Published 10 Oct. 2013. http://msdn.microsoft.com/en-us/library/ie/dn265040%28v=vs.85%29.aspx
18) Falde, Kurt. "Restricted Admin Mode for RDP in Windows 8.1 2012 R2." Microsoft TechNet Blogs. Published 14 Aug. 2013. https://blogs.technet.com/b/kfalde/archive/2013/08/14/restricted-admin-mode-for-rdp-in-windows-8-1-2012-r2.aspx
19) Morrison, Blake. "Windows 8.1 / Windows Server 20123 R2 – Assigned Access." Microsoft TechNet Blogs. Published 28 Oct. 2013. https://blogs.technet.com/b/askperf/archive/2013/10/28/windows-8-1-windows-server-2012-r2-assigned-access.aspx
20) Morowczynski, Mark. "How to setup Assigned Access in Windows 8.1 (Kiosk Mode!)." Microsoft TechNet blogs. Published 27 Oct. 2013. https://blogs.technet.com/b/askpfeplat/archive/2013/10/28/how-to-setup-assigned-access-in-windows-8-1-kiosk-mode.aspx
21) Wikipedia. "X86-64." Retrieved 5 Nov. 2013. https://en.wikipedia.org/wiki/X86-64#Older_implementations
22) Wikipedia. "3DNow!" Retrieved 6 Nov. 2013. https://en.wikipedia.org/wiki/3DNow!
23) Rhian Cohen. "LAHF and SAHF CPU Instructions." Electric Monk Blog. Published Mar. 13, 2013. http://www.electricmonk.org.uk/2012/03/13/