Symantec™
Security Response

Windows 8 Security
November, 2011

Contents

Introduction

You have almost certainly heard by now about the exciting changes from Microsoft planned for Windows 8. If you have followed the press or, better yet, played with the Windows 8 Developer Preview, then you know that this OS could change the way people think of the traditional PC. By incorporating a "touch-first" interface and introducing the Metro-UI to PC users, Microsoft is attempting to combine the rich functionality we have come to expect from our laptops and desktops with the convenience and simplicity provided by tablet, or "slate," devices (figure 1). Consumers currently have a lot of options when it comes to Android tablets, full functioning e-Readers, and, of course, iPads. Windows 8 provides an all-in-one option for people who do not want to learn how to use a new operating system just so that they can surf the web from their couch.

In addition to the new range of computing experiences that Windows 8 provides, Microsoft is hoping that Windows 8 will also change the game with regard to Windows security. The folks in Redmond have been getting more serious about security for some time now. The Vista operating system, while a failure in terms of sales, was an honest attempt to lock down the operating system. This effort was tuned in the Windows 7 release to wide acclaim. With Windows 8, Microsoft is raising the bar once again by updating the default security solution provided with the OS, enhancing its reputation-based security, and by adding functionality to watch for the deadliest threats.

These changes are interesting and will undoubtedly change the face of Windows security. We have even seen some comments that suggest that these changes may put security vendors out of business. Those comments, though, are not well-founded. Anyone who has spent much time working to help secure Windows machines against attacks knows that attackers will adapt to any change in security as long as users have something that they want. And, in the end, every user has something that attackers want, whether that is a password to a bank account, sensitive documents, or even just your network bandwidth. That being said, it is worth taking a closer look at the new security features in Windows 8 to see which threats Microsoft views as the greatest threat to its platform. A clear understanding of these features will show that the changes proposed by Microsoft emphasize the need for solid, up-to-date security software as a key part of the Windows ecosystem. This is why products like Norton Internet Security, Norton 360, and Symantec Endpoint Protection will provide customers with the fastest, most secure Windows 8 experience

Figure 1

Windows 8 interface

Defender

The first security feature that Windows 8 users will notice is a revamped Windows Defender. In Windows 7, Defender was a basic feature that provided minimal protection against a subset of common threats. Defender did not include behavior-based protection, virus detection and removal, or network intrusion prevention—all key components in a full security solution. In Windows 8, Defender now includes all these components.

Is including Microsoft's own security solution for all Windows 8 users a territorial move to push security vendors like Symantec out of the market? This is most likely not the case. Microsoft learned that many users simply never installed security software on their Windows 7 machines. Even with a number of free security solutions (including MSE) available, close to a fourth of all Windows 7 machines were left unprotected. So Microsoft's move to increase Defender's scope was not an attempt to unseat traditional security vendors, but to protect those that would not even install a free security software package.

You might think, though, that with a more powerful Defender already built-in, users that might have bought a full-featured security solution such as Norton Internet Security will no longer bother. The fact is, though, that users have consistently

chosen to pay for a higher level of performance and security, and with good reason. Analysis shows that Windows 8 Defender does not compare well in head-to-head, real-world protection tests against many third-party security software suites such as Norton Internet Security. Internal Symantec tests using Windows 8 developer preview builds from MSDN and those given out at this year's BUILD conference show that early versions of Windows 8 Defender failed to block over 38 percent of threats, compared to Norton Internet Security blocking 100 percent of threats in a real-world test methodology. In the same tests, Defender's performance in file copy tests—a pretty common operation—was more than 20 percent slower than Norton's.

While the quality of Windows Defender may improve over time, the fact that it is included with the OS means that getting around it will be the first priority of the bad guys. Malware authors will make it a priority to elude Windows Defender. Once they have cracked that one security product, they will have millions of machines they can target with confidence of success.

Customers know that you get what you pay for. Free security software is nothing new. Building security software into the OS is nothing new, either. What Microsoft gets with this updated Defender is the assurance that customers who would not have installed security software before, will now at least have something basic protecting their machines. Customers who want complete high-performance protection will continue to turn to products like Norton Internet Security, Norton 360, or Symantec Endpoint Protection to secure their machines.

Smart Screen Technology

The second visible feature in Windows 8 is an updated version of Microsoft's Smart Screen technology. This technology was initially deployed as part of Internet Explorer to protect users from inadvertently visiting malicious sites. The technology also included a reputation component that would warn Internet Explorer users about never-before-seen files downloaded through the browser. In Windows 8, Microsoft is extending support for download protection to customers who do not use Internet Explorer as their browser of choice.

At Symantec, we definitely see the value in reputation as one layer of protection. Symantec led the industry in being the first to introduce reputation-based security with our Insight technology. Microsoft's Smart Screen technology, while better than nothing for users who do not choose to install a security product, does not yet afford the same level of protection found in the Norton and Symantec lines of reputation-enabled products. Internal Symantec tests show that even when both Defender and Smart Screen are enabled in Windows 8, both technologies together still missed nearly 24 percent of threats compared to Norton. Additionally, early analysis shows that the user interaction experience with Smart Screen technology could even desensitize users to real threats because of the frequency of alerts that users get used to just blindly accepting.

Boot Time Protection

The third security feature in Windows 8, boot time protection, is not as visible to users as the other changes in Windows Defender and the expansion of Smart Screen technology. By adding new boot time protection features, Microsoft hopes to close a hole in the security profile of Windows 8. In spite of great advances in anti-malware technology, the modern PC remains most vulnerable and essentially unprotected in the few moments after power up and before any countermeasure can launch. Microsoft has tackled this problem head on with the "Secure Boot" feature available in Windows 8.

Recently, PC users have been faced with a particularly dangerous class of threats that includes StuxNet, TidServ, and Mebroot. These threats insert themselves into the boot sequence and ultimately corrupt the Windows kernel itself. Once the platform is compromised, no application can be trusted. Even security applications must rely on system APIs; and if the operating system itself is corrupt, the APIs return false information.

The normal boot process relies on a chain of control passed from component to component until there is enough functionality present to start the host operating system. A typical computer bootstrap process executes the following chain of modules:

BIOS flash -> Option ROMS -> MBR and Volume Boot Record -> OS loader -> Windows kernel -> Boot drivers

If malware succeeds in corrupting any point along that chain, subsequent modules can be corrupted in turn. The operating system and all of the loaded applications will be untrustworthy.

Secured Boot Architecture

One of the reasons that the boot process is so vulnerable is the nature of the BIOS architecture itself. The process is substantially the same as it was 30 years ago, when the first PCs were introduced. Many of the original features are still present today. With Windows 8, Microsoft has presented new features, collectively known as the "Secured Boot Architecture," that hopes to directly address these vulnerabilities. The architecture includes three main components:

- Unified Extensible Firmware Interface (UEFI)
- Early Launch Anti-Malware (ELAM) driver
- Remote Attestation

UEFI

The first component, UEFI, is not a Microsoft component and not even provided by the company. It is an interface specification created by a consortium of industry leaders. The specification defines the modern day successor to the BIOS firmware that has been used in PCs since the 1980s. In addition to providing for a secure pre-OS environment, UEFI offers many other valuable features, including:

- Platform independence
- An enhanced pre-boot graphic interface (GOP)
- Support for large storage drives (>2.2TB)

Even for Windows, UEFI support is not a new feature. It was first supported in Windows XP (64 bit Itanium edition), with general support subsequently appearing in Windows Vista. What is new is that Microsoft will now require UEFI in all logo-certified computers for Windows 8. Windows 8 will continue to support non-UEFI machines (such as upgraded legacy systems), but such machines will not be able to take advantage of the secured boot environment.

The UEFI module works by building a "chain-of-trust," beginning with first instructions executed at power on and extending to the point where control is transferred to the operating system. UEFI specifically addresses vulnerabilities in the boot chain by requiring each module in the boot chain to be signed and requiring each module to verify the signature of the following module before allowing it to execute. The UEFI can be updated by its manufacturer with white-listed and black-listed certificates used for image verification. In this way, it can be updated if certificates are compromised or updated.

There are some wrinkles in the solution, though. First, the MBR and volume boot record portion of the boot sequence do not fit easily into the UEFI design. Traditionally, the MBR partition scheme is used to organize disk drives into logical volumes. The problem, though, is that the MBR and volume boot record design cannot accommodate any form of signage or verification. To overcome this limitation, UEFI natively uses an alternative partitioning scheme known as the "GUID partition table" (GPT). UEFI Secure Boot requires the use of GPT and is capable of navigating to OS-loading components without the use of any boot sectors, and these can be verified directly by the UEFI.

The second wrinkle in the UEFI solution is that Secure Boot does not allow untrusted modules to be loaded, even if they are part of a legitimate multi-boot configuration. This means that UEFI cannot be used on a machine that also hosts a previous version of Windows or another OS such as Linux. This feature has alarmed some members of the open source community. Some OEM vendors may make it difficult to disable the UEFI setting. This will make their machines unfriendly to Microsoft's competitors.

ELAM

In addition to adopting UEFI as a standard for the Secure Boot feature in Windows 8, Microsoft is also protecting the boot sequence by introducing a new type of driver, referred to as an "Early Load Anti-Malware" (ELAM) driver. Because of the open nature of the Windows platform, Microsoft relies on third-party security vendors to verify images before they are allowed to be installed. The Secure Boot environment is designed to protect the interval between power on and the time that security software starts protecting the environment. While the UEFI architecture can verify operating system images, the trust does not extend to the critical boot drivers required for system start. These boot drivers are supplied by a much larger set of device manufacturers, and the integrity of the certificate chain is much harder to guarantee.

To enlist anti-malware vendors to protect against malicious boot drivers, Windows 8 extends the "chain-of-trust" by introducing ELAM drivers in the load sequence. The ELAM driver will be the first non-Microsoft module to get control when a system boots and will be consulted for each subsequent boot driver to be verified. ELAM drivers require special certification from Microsoft and can only be created by a small set of security vendors. There is a separate series of software logo tests for this class of driver. The boot time environment that the ELAM driver runs in is restricted. There are no storage devices available, and the only persistent state is what can be represented in the registry. The ELAM driver will be notified when all boot drivers have been started and it is required to exit at this time. It is expected that a conventional anti-malware driver will be loaded and will take over at this point.

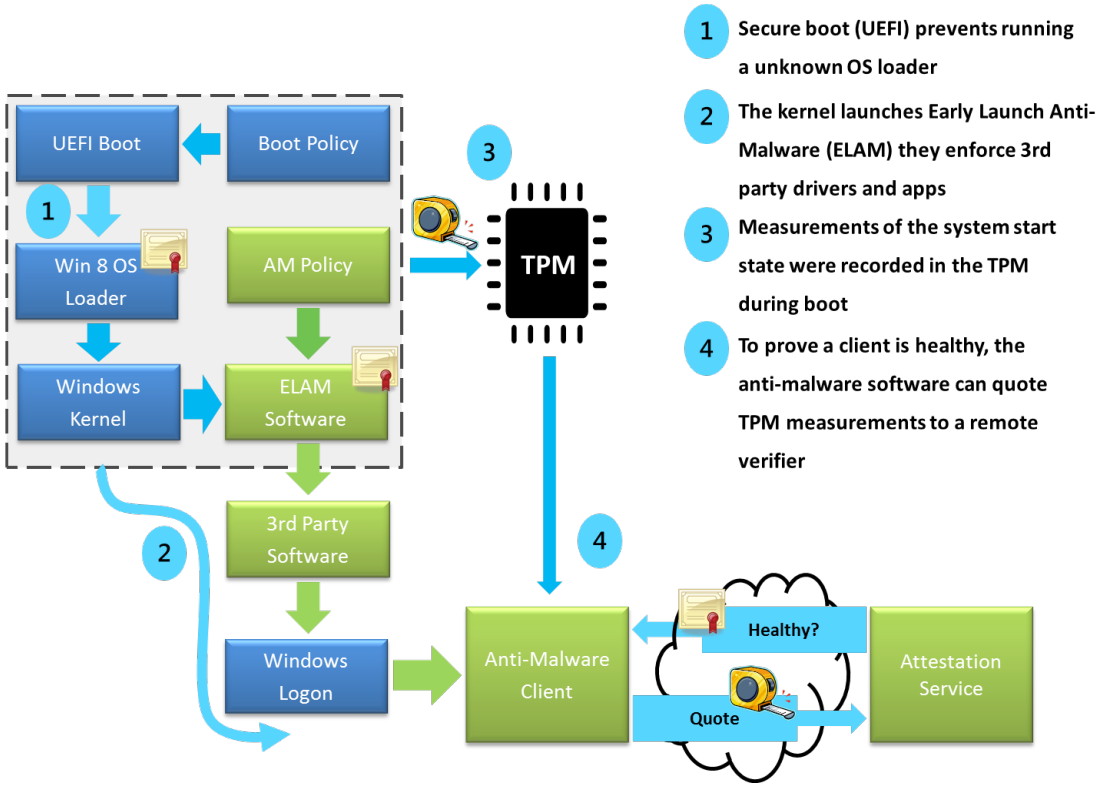
Because of the increasing emphasis on boot time performance, there are severe restrictions on how much time can be spent in the ELAM driver, and also on how much memory can be consumed. Because of these limitations, and the natural limitations inherent in running so early in the boot sequence, the role of the ELAM driver is reduced to one of certificate/hash management. Not much else is possible. In a world where there are hundreds of millions of unique threats being created each year—Symantec alone observed 286 million unique threat variants in 2010—the blacklisting of known bad hashes and certificates of boot start drivers offered by ELAM does little to improve security.

Remote Attestation

The final component of the boot time protection in Windows 8 enlists remote verification that a machine is not compromised. Malware can tamper with a system so that the system's ability to verify itself is disabled. An industry consortium, "Trusted Computing Group" (TCG), has defined a series of protocols designed to verify the sequence of images loaded during the boot process. To take advantage of this capability, the client computer must contain a "Trusted Platform Module" (TPM), which is a device that can record measurements of loaded modules that cannot be modified by any running software (figure 2). The total "measurement log" can be retrieved later and verified against its expected value.

Figure 2

Windows 8 Platform Integrity Architecture



Like the UEFI specification, TPM-based boot measurement is not new. It has been part of the internal workings of the BitLocker Drive Encryption feature first introduced in Windows Vista. In that implementation, the measurement log was required to allow the TPM to reveal the BitLocker key. Windows 8 extends the process all the way to the kernel load image, and ELAM drivers may optionally add subsequent boot driver measurements to the log as well.

Since malware can tamper with the checking process itself, the final step in verifying a trusted platform is to send the measurement log to a remote computer for independent verification. This last step is called "remote attestation," and Windows 8 provides a new set of cryptographic APIs to support this process.

There are questions, though as to the extent to which this feature will be used. Unlike the UEFI Secure Boot feature, the remote attestation feature is optional. Since the measurement process adds precious milliseconds to the boot time it will not be popular with OEM vendors. Additionally, remote attestation requires network access and remote infrastructure to perform attestation. Any configuration change that will affect the measurement log will need to be propagated to the server. The feature may be appealing to institutions and businesses that require high security and that have well-defined configurations and update procedures, but it is not likely to be useful on consumer machines.

Conclusion

In addition to the security features that Microsoft is rolling out with Windows 8, one must also remember that Microsoft is adding a lot of new functionality with this OS as well. We will begin to see an entirely new type of application that will run in the context of the Metro-UI and depend on a new Windows layer of functionality, called the Windows Runtime or WinRT. This is an exciting change that will undoubtedly offer software developers many opportunities to provide fun and useful new applications. These changes will also offer a new target for malware authors. We fully expect that we will see the first WinRT targeted attacks well before the Windows 8 release, or shortly thereafter. Security software vendors such as Symantec will be in the best position to detect, analyze, and prevent those attacks on customer's machines.

Even if these new Metro-UI apps do not end up being an easy target for malware authors, they can rest assured that the threats they wrote for previous versions of Windows will still run on the Windows 8 desktop. Microsoft has made it clear that most applications that run on Windows 7 will run on Windows 8 without any changes. This means that the vast majority of malware that runs on Windows 7 will still run on Windows 8 without any modification. The new Windows 8 OS itself is not going to make Windows machines more secure. Microsoft knows this, which is why it has improved its default security product, Defender, installed with Windows 8. Ultimately, though, it is up to customers to determine which security product is best for their needs. This is why products like Norton Internet Security, Norton 360, and Symantec Endpoint Protection will provide customers with the fastest, most secure Windows 8 experience.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Moutain View, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Credits

Peter Linhardt, Technical Director
Security Technology and Response

Spencer Smith, Technical Director
Security Technology and Response

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527-8000
www.symantec.com