White Paper

A New Paradigm Shift: Comprehensive Security Beyond the Operating System

Table of Contents

The Security Architect's Dilemma 3

Special-Purpose Security Monitor 5

McAfee DeepSAFE Technology 6

About the Authors 7

Security reports and the popular press consistently report the ever-increasing sophistication of security attacks. Shining a spotlight on the issue are highly targeted advanced persistent threats (APTs). Targeted APT attacks, such as Operation Aurora, demonstrated the use of standard IT-supported tools by cybercriminals to penetrate large corporations, steal numerous classified materials, and threaten to undermine critical infrastructure systems.

Due to inherent architectural limitations of a number of operating systems, APTs or stealth attacks utilizing rootkit techniques, are spreading widely in corporate and consumer systems. Zero-day stealth attacks, such as Stuxnet, exploit unknown system software vulnerabilities to propagate and cause damage. This constantly morphing, stealthy malware residing on storage media and in memory hides itself from operating system (OS)-resident security scanners. Rootkits also hide within a wide variety of IP-enabled devices like printers and VoIP phones, capturing data in these devices or using the devices as launching pads for computer and network infections.

The evidence is clear: traditional security methods are insufficient for dealing with the complexity of today's threats, so a new way of thinking about security is needed to fully protect against the ever-evolving threat landscape.

The Security Architect's Dilemma

Security is often deployed as an extension to a well-defined component of the operating system and its applications. For example, antivirus software operates as an addition to the file system, examining accessed files against signature lists. Another example is the firewall, which operates as an extra element to the network stack to monitor access to network resources. Similarly, host intrusion prevention systems (HIPS) control an application's access to processes, services, registry databases, documents, scripts, and more. Nevertheless, all these efforts to provide comprehensive user and system software security have proven inadequate.

The problem is this: operating system and application vendors often differ on how to protect common assets, such as documents, photos, and videos, while preserving the privacy and confidentiality of user activities. For end users and IT managers who seek comprehensive security coverage for personal and corporate assets, this leads to heterogeneous, incompatible solutions from a variety of vendors that manifest performance and manageability challenges.

Most difficult of all, software security solutions operate at the same privilege level as the malware they defend against. An effective, high-quality, low-overhead security solution must balance ideal defenses against the available monitoring and control methods provided within a specific operating system. For example, it is difficult to isolate and repair malware infections in system memory due to the absence of adequate, consistent functions across operating systems. This prevents the operating system from being fully trusted and leaves computer systems vulnerable to serious rootkit and Trojan attacks.

The security architect's dilemma is not the same for the malware developer. Malware authors do not have to adhere to any legal or product quality practices like performance, stability, and compatibility. Furthermore, malware code can and does employ destructive and improper techniques to compromise the system. A typical example is malware exploiting software buffer overflow vulnerabilities for code injection.

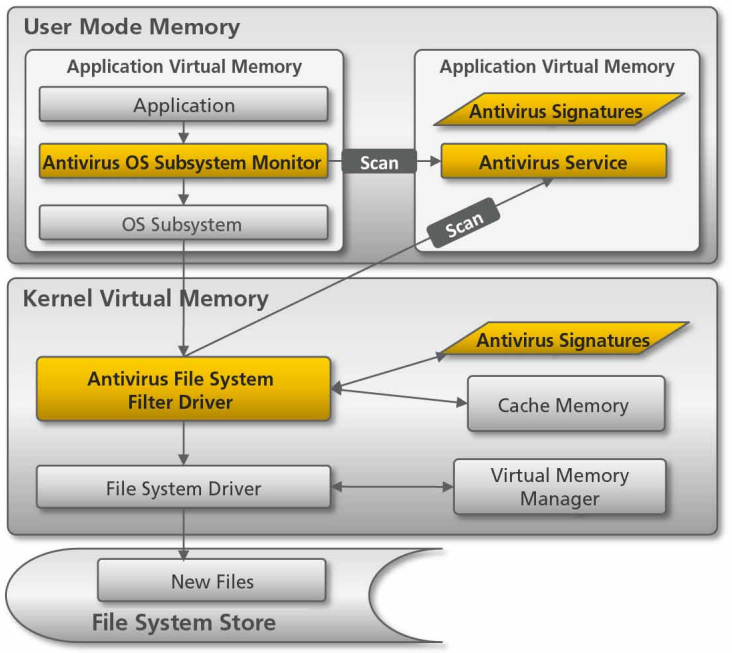

Figure 1. As illustrated in the diagram, there are numerous modules in memory and call links where malware can attack to subvert antivirus software and install stealthy attacks.

Fortunately, a potential solution to these problems emerged when virtualization became a key capability supported by processors a few years back. Security experts believe that virtualization is a new avenue to securing operating systems from outside threats. In reality, the benefit of these efforts has been limited, largely because of the following:

- A focus on device virtualization and workload migration features leading to a large trusted computing base (TCB) for the virtual machine monitor (VMM) which is at odds with optimal security properties
- Performance of VMMs optimized for multiple virtual machines sharing the same physical resources
- Costs incurred by adding security slows virtualization product releases, impacting market leadership efforts and product competitiveness

To summarize, there has not been sufficient success in designing the hardware and software solutions needed to enable security from the ground up. This demands a true paradigm shift, and it has led to joint efforts by McAfee and Intel to utilize virtualization for delivering comprehensive security beyond traditional software boundaries.

Special-Purpose Security Monitor

Intel® Virtualization Technology (Intel® VT) offers a variety of capabilities that can be used by virtualization solutions and security solutions alike. One capability is that Intel VT redefines the highest privilege level in the system via VMX root. Typical virtualization solutions provide a virtual machine monitor (VMM) that utilizes Intel VT to virtualize the underlying hardware for the purpose of running multiple operating systems. However, for reasons stated in the previous section, general purpose VMMs have not focused on providing the security properties the industry needs.

To maximize security, it is important to ensure that the highest privilege code executing on a platform has a small trusted computing base (TCB). This is because it must be acknowledged that any code introduced into a system has potential bugs, and these bugs can be exploited as vulnerabilities. There is simply a higher probability of bugs in a large quantity of code over a small quantity of code. Thus, in a secure system, the highest-privilege core components from which the rest of the system derives its security must be designed to be as minimalistic as possible. Unlike a general-purpose VMM, there are no device drivers, schedulers, or general-purpose hardware virtualization components needed for a specialized security monitor—only the essential security functionality. This approach fundamentally minimizes the exposure of the core high-privilege security code.

Minimal code and security specialization also enable a low-overhead solution. By keeping the tasks of the VMX root components as minimal as possible, we create a system where the transitions into and out of VMX root are minimized. Maintaining a single operating system view and allowing a single operating system to retain full control over resource scheduling means that processor time does not have to be shared with other guest operating systems or programs.

Additionally, a security specialized monitor using VMX root actually improves the overall compatibility of the system as well. For example, device drivers in the Intel VT system stay in the same form when loaded within the operating system and do not need to be ported or replicated in the VMM layer as they would with a general-purpose VMM. Thus, existing update mechanisms, hardware interactions, and system services are entirely preserved. There is no need for IT or consumers to update additional components, change their existing images, or wait for specialized compatible drivers to become available in order to deploy a security monitor. Advanced power management, 3D graphics, storage, and networking operate unobstructed.

McAfee DeepSAFE Technology

McAfee® DeepSAFE™ technology, jointly developed by McAfee and Intel, allows McAfee to develop hardware-assisted security products that take advantage of a "deeper" security footprint than previously available. McAfee DeepSAFE technology platform, using Intel VT capabilities on Intel® Core™ i3, i5, and i7 processors, executes in a privileged mode to fight against stealthy software attacks. McAfee DeepSAFE uses processor features to monitor system behavior, including memory and CPU state changes. Memory events detected by McAfee DeepSAFE technology instantly raise runtime integrity violations when they occur and thus give anti-malware tools the critical ability to mitigate stealthy rootkit and malware attacks in real time. McAfee DeepSAFE technology protects anti-malware engines and provides them with visibility to observe and audit changes to key processes and the operating system kernel. McAfee DeepSAFE technology utilizes CPU-derived events to detect integrity violations and notifies verified security agents of these violations, even in the face of never-before-seen, zero-day malware attacks.

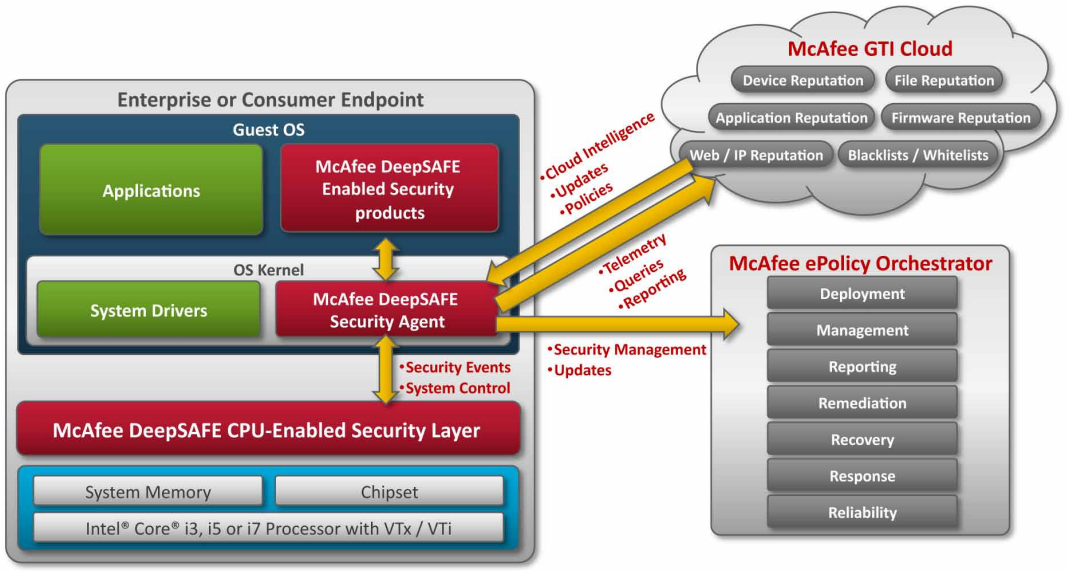

Figure 2. McAfee DeepSAFE technology utilizes hardware features in the Intel Core i3, i5, and i7 processors to monitor beyond the operating system and allows products like McAfee Deep Defender to detect and stop hidden stealth attacks.

There are two capabilities in anti-malware software needed for runtime integrity monitoring of a large TCB and dynamic environment like today's operating systems. McAfee DeepSAFE technology provides both of these key capabilities and enhances them via Intel silicon. The first is execution protection (and availability) for security agents. McAfee DeepSAFE technology uses hardware virtualization and the VMX root privileged mode to operate beyond the operating system and provide runtime protection for anti-malware engines against malware attacks. Security agents are thereby isolated from malware executing at the same level. The second key capability is trusted system visibility. McAfee DeepSAFE uses a direct and scalable approach to continuously monitor system and process memory, allowing security agents to apply behavioral policies. Such behavioral policies complement McAfee whitelisting techniques to protect not only the anti-malware assets in memory, but also key operating system kernel assets targeted by rootkits. Runtime protection of the user's operating system is important to defend against the stealthy malware and blended attacks increasingly used in advanced persistent threats. McAfee DeepSAFE technology is a powerful platform that enables real-time and proactive behavioral anti-malware capabilities at the kernel level. McAfee DeepSAFE technology overlays whitelisting and blacklisting capabilities with behavioral policies to mitigate zero-day attacks when they attempt to install a rootkit and malware within the OS kernel.

The first product to utilize the McAfee DeepSAFE technology is McAfee Deep Defender. This solution utilizes McAfee DeepSAFE technology working below the OS to help protect systems against stealthy attacks that may go undetected with traditional system security methods. McAfee Deep Defender provides behavioral monitoring of real-time kernel operations to reveal and remove advanced, previously invisible attacks. Integrated with McAfee® ePolicy Orchestrator® software and McAfee Global Threat Intelligence™, McAfee Deep Defender yields a seamless defense that extends system security beyond the OS to preempt covert zero-day threats that go undetected by today's OS-based solutions. More information on McAfee Deep Defender can be found at www.mcafee.com/deepdefender.

In summary, APTs use a number of techniques to infect and hook themselves into the OS where they mask themselves from detection. Today's anti-malware solutions running as applications above the operating system are no match for the stealth techniques used by today's malware developers. McAfee DeepSAFE, developed jointly by McAfee and Intel, allows McAfee to deliver hardware-assisted security products like McAfee Deep Defender, which take advantage of a "deeper" security footprint. McAfee DeepSAFE technology sits below the operating system (and close to the silicon), allowing McAfee products to have an additional vantage point to better protect computing systems.

About the Authors

Ahmed Sallam is the CTO/chief architect of advanced technology at McAfee. Ahmed's vision and innovation led to the creation of proactive cloud-based McAfee behavioral protection, lightweight security, anti-rootkits, and virtualization-based security systems. Ahmed initiated and drove the Intel and McAfee relationship in the creation of McAfee DeepSAFE. He is sole inventor of more than 50 patent applications. A co-designer of VMsafe, VMware's VMM CPU security, he was a senior architect at Nokia Security Division (sold to Check Point) and a principal engineer at Symantec. He is a true entrepreneur, serving as chief architect of Cognicity (sold to DigiMarc), and chief designer at Panasas. His code runs on hundreds of millions of computer systems. Ahmed holds a B.S. in Computer Science and Automatic Control from the University of Alexandria.

David Durham is a principal engineer at Intel Labs. His team researched cryptographic security features currently found in hundreds of millions of Intel processors. Also at Intel, David developed policy-based network management standards, created security and manageability solutions shipping in Intel® vPro™ platforms, and worked with McAfee on advanced anti-malware technologies. He is a prolific author on computer communications, having written a book, multiple publications, and several Internet protocol standards now deployed in millions of connected devices. David holds more than 40 issued patents and has B.S. and M.S. degrees in computer engineering from Rensselaer Polytechnic Institute.

Ravi Sahita is a security researcher and architect at Intel Labs. He is working on processor and platform approaches to mitigate computer malware and protect software integrity. Ravi has been working with McAfee on advanced anti-malware and, in the past, has contributed to Intel® AMT System Defense and Agent Presence, Intel® NetStructure® products, and the open sourced Intel® Common Open Policy Services (COPS) client SDK. He is a contributing member of the IETF and TCG standards bodies. He received his B.E. in Computer Engineering from the University of Bombay, and an M.S. in Computer Science from Iowa State University. Ravi holds 21 patents and is the recipient of an Intel Achievement Award.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com/deepsafe.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

42200wp_a-new-paradigm-shift_0212