

GLOBAL SECURITY
IBM Internet Security Systems White Paper

*IBM Internet Security Systems Supports
Microsoft Vista's Kernel-Locking for
Improved Customer Security*

**IBM Internet Security Systems
Ahead of the threat.™**

Table of Contents

SUMMARY	2
WHAT IS THE CONTROVERSY?	2
WHAT IS THE KERNEL?	2
WHAT IS <i>PATCHGUARD</i> ?	2
WHAT IS THE SOLUTION?	3
WHAT IS THE FUTURE FOR THIRD-PARTY PRODUCTS AND VISTA?	4
FREQUENTLY RAISED OBJECTIONS (AND ANSWERS)	5
ABOUT IBM INTERNET SECURITY SYSTEMS	5

Summary

Businesses want secure environments. Forward-thinking information security providers encourage software vendors to make platform improvements, with the overarching goal of improving customer security.

What is the Controversy?

When Microsoft announced plans this summer to lock down its operating system kernel in the upcoming Windows Vista release, many security vendors vehemently protested. Many security vendors have created businesses by adding additional functionality to the Windows product and have become worried that Microsoft's intent to disallow kernel patches will impair their ability to provide endpoint security for Windows.

Regulatory action was threatened; full page ads were run in the *Financial Times*; and large public relations campaigns were launched, all complaining about Microsoft's move, which we believe will actually provide greater user security. At issue is the new *PatchGuard* (defined below) feature being introduced in the 64-bit version of Vista.¹

Microsoft's decision to lock the kernel puts the onus on Microsoft to respond quickly as security problems develop in the kernel. Rather than fight Microsoft on its decision, which we believe will improve the security of its customers, third-party vendors should welcome the opportunity to work with Microsoft as kernel security situations arise and Microsoft customers require security solutions. Today's current solution – kernel patching – brings more insecurity, instability, and performance issues than the announced solution, both for the operating system and for the security vendors who patch it.

What is the Kernel?

In computing, the kernel is the lowest, most central component of a computer operating system, and one of the first pieces of code to load when a system starts. Its responsibilities include managing the system's resources and the communication between hardware and software components.

As a basic component of a computer operating system, a kernel provides an abstraction layer for the resources (especially memory, processors and I/O devices) that applications must utilize to perform their functions. It typically makes these facilities available to application processes through inter-process communication mechanisms and system calls. It is responsible for basic operating system housekeeping tasks such as memory management, process creation and termination, and managing the data on the disk. The integrity of the kernel is instrumental to the performance and security of the computer it resides upon.

What is PatchGuard?

One of Microsoft-created PatchGuard's primary reasons for existence is to prevent kernel-level rootkits. A rootkit is a set of software tools intended to conceal running processes, files or system data, thereby helping an intruder to gain and maintain access to a system while avoiding detection. Based on user studies, Microsoft estimates that about 14 percent of all computers harbor a rootkit.²

Rootkits can exhibit a number of different malicious techniques, including monitoring keystrokes, changing system log files or existing applications, and creating a backdoor into the system to gain remote access to a computer and launch attacks. Rootkits often try to gain access to the kernel of the operating system. Kernel rootkits can be especially dangerous because they can be difficult to detect and are almost impossible to remove.

1. PatchGuard was first introduced to 64-bit Windows in 2003, attracting scant attention.

2. <http://www.techweb.com/wire/security/192203375>

PatchGuard does not prevent all rootkits or other malware from attacking the operating system. However, it does mitigate one uniquely destructive way to attack the system, namely patching kernel structures and code to manipulate kernel functionality. Protecting the integrity of the kernel is a fundamental step in protecting the entire system from malicious attacks and the reliability problems that may result from even well-intentioned patching.

PatchGuard shuts down a computer when it detects that specific internal data structures have been *hooked*, which is a common way that malicious software starts doing its damage. Kernel-hooking or patching is commonly regarded as an undesirable way to conduct business.

Initially, *PatchGuard* will be enabled only in the 64-bit version of Windows Vista. Because there are few 64-bit applications written for Vista, and because so few Windows users for the foreseeable future will run in 64-bit mode, most initial users of Vista are expected to run the operating system in 32-bit mode and their security software will still be able to access the kernel. Because Microsoft is upgrading its security kernel foundation ahead of widespread 64-bit adoption, it is improving operating system security for the future without substantially disrupting security vendors' present protection models.

What is the Solution?

IBM Internet Security Systems' Position: Build Upon Microsoft's Operating System Security Improvements

To support past operating system releases, IBM Internet Security Systems has used code and system call trap patching³ – among other traditional techniques – to modify the Windows kernel to provide security. Predictably, altering the kernel sometimes led to system instability and other maintenance challenges.

IBM Internet Security Systems is well aware of the changes that Microsoft is making in Vista and, as a result, is making the appropriate corresponding architectural changes. Patching of the kernel is not the way to build reliable software. We believe Microsoft has a desire for its operating system to be more secure and it has made no secret of the fact that this release would entail major changes. Throughout the Vista development process, Microsoft has provided Software Development Kits, APIs, and example code so that security solution vendors could develop and test in a parallel path.

As the magnitude of Microsoft's projected Vista changes became clear, IBM Internet Security Systems had a decision to make. It could join the other independent software vendors in the fight against Microsoft and its attempt to lock its operating system kernel in order to provide security functionality for customers. Or IBM Internet Security Systems could figure out how to work with Vista's changes to provide the best security possible. We believe the decision to side with improved security for customers was the appropriate decision.

From the outset, IBM Internet Security Systems engineers and researchers participated actively in Microsoft technology forums, and made early use of the tools Microsoft has provided along the way. IBM Internet Security Systems has used the Windows Filter Platform and its APIs to drop and re-inject packets to enable the right level of security.

For most aspects of malware protection, it is the correct and accepted manner to proceed by deploying a filter driver, which is a type of driver that has been a method of securing Windows environments for many years. Filter drivers provide a means for monitoring and processing user mode requests for accessing files. IBM Internet Security Systems was among the first of the third-party vendors to develop a Vista file system filter driver, and we have continued developing our Vista support capabilities as Microsoft releases new information. IBM Internet Security Systems' new file system filter driver leverages the documented and supported file system filter infrastructure that is provided by the underlying operating system and the associated development kits.

3. System call trap patching, defined: "A method of patching the kernel where the entry point in the system call trap table is modified such that the flow of control is passed to another function as the target of the system call prior to the actual code that implements the system call is invoked"

IBM Internet Security Systems decided that it was best to do the needed filter driver development right – once. Since IBM Internet Security Systems had to develop drivers for Vista, it decided to rebuild the drivers, making them available for a number of other Windows platforms, including the following:

- XP + SP2
- XPx64
- Windows 2000 + SP4
- Windows 2003 + SP1
- Windows 2003x64

This driver development has been successful and has rendered benefits beyond the ability to provide a higher level of overall security for IBM Internet Security Systems customers after Vista's release – a notable side effect is that, through this reworking of device drivers, IBM Internet Security Systems has improved compatibility with third party encryption and compression products.

IBM Internet Security Systems will continue to work closely with Microsoft as the beta process is completed to release a best-in-class Vista protection solution as soon as possible after Microsoft moves Vista to general availability.

What is the future for third-party products and Vista?

Preventing unwanted kernel patching is good for security and those vendors who want to do what's best for customers will enhance Vista with the best security possible. Microsoft's effort to lock out rootkits and other kernel-level attacks will help customers.

Microsoft recently announced its intention to release APIs for third parties to work more closely with Vista. Regardless, using techniques such as those IBM Internet Security Systems has employed, third-party vendors should be able to work with Microsoft to provide superior outcomes for their customers.

It is conceivable that some security product categories may be rendered redundant as a result of fundamental changes in Windows architecture in Vista and beyond. Innovative vendors must keep their eyes on the future, working to meet security needs that will arise.

IBM Internet Security Systems is working closely with Microsoft and understands the intricacies of the new operating system environment and how to secure it for the benefit of our customers. We will continue to add value quickly by deploying solutions within the market that fill the security gaps that will appear as bad guys look for holes in Vista.

IBM Internet Security Systems is well-equipped to tackle this new operating system's security needs because of its long history of security innovation and preemptive protection. Powered by industry-leading vulnerability research from its X-Force® research and development team, IBM Internet Security Systems' solutions help prevent attacks from multiple vectors, including those affecting new operating systems platforms. We know that locking the operating system kernel is only a step in keeping malicious, profit-driven attackers from succeeding, but it is an important step.

Frequently Raised Objections (and Answers)

<i>What Some Vendors Say...</i>	<i>The Truth Is...</i>
<i>Hackers can work around locked kernel, so locking it doesn't help protect against all attacks indefinitely.</i>	Smart bad guys can do almost anything if the profit motive is strong enough. As with any security effort, Microsoft should try to prevent most problems, making it more difficult for cyber-criminals to achieve their objectives. Microsoft Vista is advancing security at the kernel level, reducing rootkits, a pernicious attack medium. It is up to security vendors to adjust their views to the new playing field
<i>If Microsoft doesn't allow hooks from all vendor products, customers can't select best of breed.</i>	We believe best-of-breed vendors normally provide the best security; if that means doing it on a platform that changes the nature of the vendor tool, then we believe that's the optimal approach.
<i>Vista does not provide perfect security.</i>	Exactly. That's why security companies have a wonderful opportunity to add differentiating and unique value in providing the best overall security while solving next-generation problems. Bad guys don't stand still. Many still want to damage targets, steal IP, and make money. Rather than bemoaning positive security moves, security vendors should help the market move to the next level.
<i>It's not fair!</i>	It is fair to require vendors to work with Vista to provide heightened security through groundbreaking solutions to customers. With so few 64-bit environments currently out there, vendors have time to build the right APIs now to make their tools work.

About IBM Internet Security Systems

IBM Internet Security Systems is the trusted security advisor to thousands of the world's leading businesses and governments, providing preemptive protection for networks, desktops and servers. An established leader in security since 1994, the IBM Internet Security Systems protection platform automatically protects against both known and unknown threats, keeping networks up and running and shielding customers from online attacks before they impact business assets. IBM Internet Security Systems products and services are based on the proactive security intelligence of its X-Force® research and development team – the unequivocal world authority in vulnerability and threat research. The product line is complemented by comprehensive Managed Security Services and Professional Security Services. For more information, visit the IBM Internet Security Systems Web site at www.iss.net or call 800-776-2362.

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS

Australia and New Zealand
Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838-1555
Fax: +61 (0)7 3832-4756
e-mail: aus-info@iss.net

Asia Pacific
Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: jp-sales@iss.net

Europe, Middle East and Africa
Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America
6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (509) 756-5406
e-mail: isslatam@iss.net

©Copyright 2007 IBM ICompany. All rights reserved worldwide.

Internet Security Systems is a trademark and X-Force is a registered trademark of IBM Internet Security Systems Inc. All other marks or trade names are the property of their owners and used in an editorial context without intent of infringement. Specifications and content subject to change without notice.

Distribution: General
PM-VISTAPOSITION-0207

IBM Internet Security Systems
Ahead of the threat.™