

# OT (FW: Microsoft Progress Report: Security)

*Source:* <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2004-04/0032.html>

---

*From:* Tom Linden ([tom\\_at\\_kednos.com](mailto:tom_at_kednos.com))

*Date:* 04/01/04

Date: Wed, 31 Mar 2004 16:12:06 -0800

I thought some might find this interesting, for a variety of reasons.

-----Original Message-----

From: Bill Gates [<mailto:billgates@chairman.microsoft.com>]

Sent: Wednesday, March 31, 2004 12:43 PM

To: [tom@kednos.com](mailto:tom@kednos.com)

Subject: Microsoft Progress Report: Security

Malicious software code has been around for decades. But only in the last few years have the Internet, high-speed connections and millions of new computing devices converged to create a truly global computing network in which a virus or worm can circle the world in a matter of minutes.

Meanwhile, criminal hackers have become more sophisticated, creating and distributing digital epidemics like Slammer, Blaster, Sobig and Mydoom that spread almost instantaneously, threatening the potential of technology to advance business productivity, commerce and communication.

The kinds of threats are evolving too. Blaster, for example, hijacked individual computers, turning innocent users into unknowing and innocent worm propagators. These kinds of attacks – "swarming" attacks that are coordinated to cause multiplied, cascading effects – change the landscape of security threats. They put new demands on IT professionals and consumers to take preventative measures, and on the technology industry to continue to innovate and develop new solutions.

While there are considerable challenges ahead, Microsoft and our industry are making significant progress on the security front. This email, which you're receiving as a subscriber to executive emails from Microsoft, offers insights into Microsoft's significant investments in four areas of security:

- Isolation and Resiliency
- Updating

- Quality
- Authentication and Access Control

Additionally, we are committed to major investments in customer education and partnerships that will help make the computing environment safer and more secure.

Given human nature, evolving threat models and the increasing interconnectedness of computers, the number of security exploits will never reach zero. But we can dramatically blunt the impact of cybercriminals, and are dedicating a major portion of our R&D investments to security advances.

## ISOLATION AND RESILIENCY

Central to our security efforts is preventing malicious code from being able to exploit a vulnerability by isolating such code, providing more effective control over what computer processes can talk to or work with, and making systems more resilient so they are able to identify and stop suspicious or bad behavior in its tracks.

Windows XP Service Pack 2: We are working on a number of isolation and resiliency advances that address four specific modes of attack in our flagship client operating system. These will be available in late spring/early summer.

- Network Protection: Windows Firewall will be turned on by default, and global firewall settings and central administration of firewall configuration will be enabled. This reduces the "attack surface" of PCs and networks.
- Safer Web Browsing: To reduce the impact of malicious code and Web sites that can damage computers or defraud users, Internet Explorer will automatically block unsolicited downloads from Web sites as well as block unwanted pop-ups unless a user clicks on a download link. IT administrators will also be able to manage this capability to enforce a consistent policy across their organizations. In addition, wireless setup will be improved for more secure browsing on wireless home networks.
- Safer Email and Instant Messaging: To reduce the risk of attacks, we are building better file attachment handling in Outlook Express and Windows Messenger instant messaging, and offering increased customer control over downloads of external content in Outlook Express that could enable a sender to identify your computer.
- Memory Protection: Malicious software designed to exploit buffer overruns can allow too much data to be copied into areas of the computer's memory. Although no single technique can completely eliminate this type of vulnerability, Microsoft is

employing a number of security technologies to mitigate these attacks. First, core Windows components have been recompiled with the most recent version of our compiler technology to protect against stack and heap overruns. Microsoft is also working with microprocesso  
r companies, including Intel and AMD, to help Windows support hardware-enforced data execute protection (also known as NX, or no execute). NX uses the CPU to mark all memory locations in an application as non-executable unless the location explicitly contains executable code. This way, when an attacking worm or virus inserts program code into a portion of memory marked for data only, it cannot be run.

Windows Server 2003: In an environment in which every computer can be seen as living in a "hostile world," our work on Windows Server 2003 has focused on how to help reduce, mitigate or contain threats. We plan to ship security advances in Windows Server 2003 Service Pack 1 in the second half of 2004 that will include the server-relevant security technologies found in Windows XP SP2. To improve the isolation capabilities, the Windows Firewall will be enabled during setup on new server installs so that the s  
erver is more protected from potential network-based exploits during configuration. A security configuration wizard will also be included so that once server roles (such as file server, app server, etc.) are enabled, they can be further locked down based on the specific usage model for that role.

Internet Security and Acceleration Server 2004: Security advances in Internet Security and Acceleration Server 2004 include much deeper content inspection, which will enable customers to better protect their Microsoft applications and fortify remote VPN connections. An enhanced user interface and management tools will make it easier for customers to implement and manage security policies, reducing the potential for misconfiguration – a common cause of network breaches.

Exchange Edge Services: This new technology addresses the evolving security problems associated with Internet email. Exchange Edge Services is designed to block incoming or outgoing malicious email and junk mail, defend against email server attacks and email-borne viruses, and encrypt messages to optimize for security. It is also designed to provide a foundation on which third-party developers can build technologies such as next-generation email filters, email encryption products and email compliance soluti  
ons.

Active protection technologies: Making computers even more resilient in the presence of increasingly sophisticated worms and viruses is key in preventing and containing attacks. To this end,

Microsoft is investing in the development of an integrated set of protection technologies that include:

- Dynamic system protection that proactively adjusts defenses on each computer based on changes in its "state." For example, installing new software, making a configuration change, the need for a new update, or connecting to different networks can make a computer more vulnerable. Dynamic system protection detects these changes and adjusts the level of protection accordingly. Today, customers benefit from Automatic Update in Windows, which detects when a computer requires a new security update. In the future, Microsoft envisions computers not only being able to detect changes, but proactively responding to them too. For example, a laptop moving from a corporate network to a home cable modem or DSL connection could cause the integrated firewall to close more ports for additional protection.
- Behavior blocking that limits the ability of a computer infected with a worm or virus to cause further damage, by intercepting suspicious behavior, determining if it is out of the ordinary, and stopping it if it is. For example, the Blaster worm exploited a vulnerability that caused Windows to replicate the worm to other computers. Behavior blocking would contain this attack.
- Application-aware firewall and intrusion prevention that is designed to identify malicious traffic and block it. Traditional firewalls can be bypassed by worms and viruses embedded in what appears to be valid network traffic. This new technology will enable deep inspection of network traffic and stop or limit distribution of this malicious content.

**Spam Tools:** Because viruses, worms and other malicious code often spread via spam, Microsoft is waging a multi-pronged anti-spam effort. Last November, Microsoft announced SmartScreen Technology, a filter used in our client and online email programs. It gets progressively "smarter" as email users train the filter to identify unwanted spam. Last month, Microsoft unveiled a pilot implementation of Caller-ID, a technology that authenticates the origin of email, much like telephone Caller-ID. On the enforcement front, meanwhile, the company took 66 legal actions last year against spammers worldwide.

**Client Inspection:** At the corporate level, one of the biggest concerns is home computers or remote laptops infected with a virus or worm that are connected to a corporate network. We are working on technologies that will inspect these remote devices and block network access if they don't pass a health inspection.

**Web Services:** The delivery in 2002 of WS-Security, a standardized specification that improves the integrity, confidentiality and

security of Web Services, will help businesses link systems internally and externally in a more secure, cost-efficient and flexible way by allowing for the encryption of messages and support for digital signatures. A recent report by the WS-I Security Profile Working Group outlines new countermeasures to combat challenges and threats in building interoperable Web services

## UPDATING

Until now, software updates have been the primary way that customers protect against security vulnerabilities. Although the evolving nature of threats requires a broader, multi-pronged response, Microsoft is continuing to make significant upgrades to the quality of our updates and associated processes, and building more advanced tools to help IT administrators optimize their infrastructure for security.

Last fall, we moved to monthly releases of updates to improve predictability and manageability, and to reduce the burden on IT administrators (although we will continue to release updates out-of-cycle to protect customers in the case of an active threat). We also are improving testing processes to minimize update inconsistencies and recall rates, and by this summer most of our updates will have full rollback capabilities.

System Management Server 2003, launched last November, is a comprehensive update and software management and distribution solution that enables organizations to quickly and easily deploy the latest updates in a systematic manner. In January, we released Microsoft Baseline Security Analyzer v1.2, a free tool that provides a streamlined method of identifying common security misconfigurations.

Windows Update Services, an evolution of Software Update Services 1.0 (SUS), is a major step forward in Microsoft's patch and update management strategy. A free component of Windows Server, Windows Update Services gives IT administrators a seamless update, scanning and installation capability for Windows servers and desktops. New features include the ability to provide customers with additional automation and control that reduces interruption when updating systems, and expanded functionality to update SQL Server, Exchange Server, Office 2003 and Office XP, in addition to Windows. It is currently in beta and scheduled for release in the second half of 2004. For consumers, we are also complementing Windows Update with a new service to automatically keep consumers up to date on a broader set of Microsoft products beyond Windows. This new service, called Microsoft Update, will be available later this year.

We are also incorporating the ability to automatically check the status of crucial security functionality such as firewall, automatic update and anti-virus. A new Security Center feature in the Windows XP Control Panel will tell a customer whether key security capabilities are turned on and up to date. When a problem is detected, they will receive a notification and recommended actions to help them become more secure.

## AUTHENTICATION AND ACCESS CONTROL

Computer networks are no longer closed systems in which a user's mere presence on the network can serve as proof of identity. In an era where millions of computing devices are interconnected, and vendors and partners often have access to an organization's network, there are many potential opportunities for unauthorized individuals to gain access to digital information such as e-mail, e-commerce transactions or proprietary files. In this environment, access control (who, what and when) and authentication are critical aspects of ensuring an organization's security.

**Passwords:** Passwords provide the most common mechanism for authenticating users who need access to computers and networks. They also can be a weak link if users choose common passwords to more easily remember them. The Windows Server 2003 family has a new feature that checks the complexity of the password for the Administrator account during setup. If the password is blank or does not meet complexity requirements, a dialog box warns of the dangers of not using a strong password. We also are expanding our support for strong, two-factor authentication mechanisms through partnerships with companies like RSA Security, Inc. and VeriSign, Inc.

**Smartcards:** Windows Server 2003 and Windows XP also support smart cards, credit-card-sized devices that securely store certificates, public and private keys, passwords, and other types of personal information. Logging on to a network with a smart card provides a strong form of authentication because it uses cryptography-based identification and proof of possession of the private key held on the smartcard when authenticating a user to a network; in other words, something you have and something you know.

**Public Key Infrastructure (PKI):** Windows Server 2003 includes features to help organizations implement a public key infrastructure, including certificates and associated services and templates. A PKI provides the mechanisms needed to support issuance and life-cycle management of digital certificates. By trusting the digital certificate issuing authorities, other parties can independently determine the identity of clients presenting the digital certificates for authentication purposes. Use of this authentication technology can provide strong authentication based on industry standard public key cryptographic technology.

Biometric ID Card: Farther out, the Tamper-Resistant Biometric ID Card system will provide an innovative, simple and affordable solution for providing cryptographically secure photo-ID cards using a unique combination of public key cryptography, compression and barcode technologies.

IPsec: Another important component of a comprehensive defense-in-depth information protection strategy, IPsec eliminates many threats by mutually authenticating computers and restricting incoming network traffic based on that authentication. In addition, it provides for digitally signing traffic to ensure integrity, and encrypting traffic to provide privacy. Microsoft's IPsec implementation-in use in our own corporate network-is completely standards-compliant and will interoperate with all other compliant IPsec implementations, including those that support network address translation.

## QUALITY

As we've said before, Microsoft is strongly committed to using state-of-the-art engineering practices, standards and processes in the creation of our software. We have undertaken a rigorous "engineering excellence" initiative so that our engineers understand and use best practices in software design, development, testing and release.

The security development processes we instituted prior to releasing Windows Server 2003 last year are a prime example of where this effort is showing results that benefit customers. The number of "critical" or "important" security bulletins issued for Windows Server 2003, compared to Windows 2000 Server, dropped from 40 to 9 in the first 320 days each product was on the market. Similarly, for SQL Server 2000, there were 3 bulletins issued in the 15 months after release of Service Pack 3, compared to 13 bulletins in the 15 months prior to its release. With Exchange 2000 SP3, there was just 1 bulletin in the 21 months after its release, compared to 7 bulletins in the 21 months prior.

We also have had some great success developing new internal tools that automatically check code for common errors, and more thoroughly test software before its release. For example, we use code-checking tools that automatically search for classes of bugs that can lead to security vulnerabilities, program crashes and hangs. We have committed to making these engineering advances available to other software developers through training and tools, including the next release of Visual Studio.

In Service Pack 1 for Windows Server 2003, we will continue efforts to reduce surface attack area by removing older, unused

technology.

## CUSTOMER EDUCATION AND PARTNERSHIPS

The best technologies in the world are ineffective if people don't know how to use them, or aren't aware they exist. With hundreds of millions of computer users around the globe, and varying levels of knowledge about security, this is a major challenge, but Microsoft is investing significantly to help customers understand how they can make their environments more secure.

By the end of this year, our aim is to reach 500,000 business customers worldwide with information on how to optimize their systems and networks for security. We're partnering with other industry leaders to help business customers optimize update management and security solutions. And we're providing seminars and publications for developers to help them build secure applications and Web services.

Starting in April, Microsoft will host the first of 21 Security Summits in cities across the U.S., intended to provide deep technical security training for IT and Developer professionals. This training, offered at no charge, complements a variety of other opportunities Microsoft is providing for customers to help protect their computers and networks, including Webcasts, self-paced learning and hands-on labs. We also are providing security training for customers worldwide, and more information is available from regional Microsoft offices.

We have also created a Security Guidance Center for developers and IT pros at [microsoft.com/security/guidance](http://microsoft.com/security/guidance), where customers can find in-depth technical guidance, tools, training and updates to help plan and manage more effective security strategies. This free information includes checklists to help perform security-related checks and processes, step-by-step instructions for a broad range of security tasks, and product- and technology-specific guidance to help protect platforms, networks, desktops and data.

For consumers, we're working on a worldwide education campaign with computer manufacturers, retailers, ISPs and other partners to create broader awareness of best practices in PC "hygiene," and how to make protection technologies easier to enable. This has three aspects: installing antivirus software, using an Internet firewall, and using the Automatic Update features in Windows to automatically download the latest Microsoft security updates.

We have joined forces with companies such as Computer Associates, Network Associates, Symantec, Trend Micro, F-Secure, ISS

(BlackICE), Tiny Software and Zone Labs to provide special offers on third-party antivirus and personal-firewall software.

We helped form the Virus Information Alliance, which includes 10 leading anti-virus vendors, to help Internet users find information about the latest virus threats affecting Microsoft technology.

Last month, the Global Infrastructure Alliance for Internet Safety (GIAIS) was announced to enable even stronger collaboration between Microsoft and Internet Service Providers regarding security issues. Already, GIAIS members performed a critical role in working with Microsoft to identify the virus signatures for MyDoom, and to develop remediation tactics to ensure consumer safety.

Security experts from Microsoft also are participating in initiatives sponsored by the Department of Homeland Security and Congress aimed at strengthening the nation's critical infrastructure, ranging from recommended engineering processes in software development, to effective patch management, to how best to create the business ecosystem required to broadly support robust security practices.

Microsoft is also working with law enforcement on a global basis to deter hackers from software sabotage. Last November Microsoft established the Anti-Virus Rewards Program, which offers cash rewards for information provided to the FBI or Secret Service that results in the arrest and conviction of those responsible for unleashing viruses and worms.

## THE FUTURE

Security is as big and important a challenge as any our industry has ever tackled. It is not a case of simply fixing a few vulnerabilities and moving on. Reducing the impact of viruses and worms to an acceptable level requires fundamentally new thinking about software quality, continuous improvement in tools and processes, and ongoing investments in resilient new security technologies designed to block malicious or destructive software code before it can wreak havoc. It also requires computer users to be proactive about deploying and managing products. Detailed information to help customers become more secure is at [www.microsoft.com/security](http://www.microsoft.com/security).

Technology has come an incredibly long way in the past two decades, and it is far too important to let a few criminals stop the rest of us from enjoying its amazing benefits.

Bill Gates

comp.os.vms: OT (FW: Microsoft Progress Report: Security)

To cancel your subscription to future executive emails, please reply to this email with the word UNSUBSCRIBE in the subject line. To contact us, write to us at One Microsoft Way, Redmond, Wash., 98052. To manage your Microsoft.com subscriptions, please sign in at the Microsoft Profile Center here: <http://register.microsoft.com/regsys/pic.asp>. To see the Microsoft.com Privacy Statement, please go to <http://www.microsoft.com/info/privacy.mspc>.

---

Incoming mail is certified Virus Free.  
Checked by AVG anti-virus system (<http://www.grisoft.com>).  
Version: 6.0.593 / Virus Database: 376 - Release Date: 2/20/2004

---

Outgoing mail is certified Virus Free.  
Checked by AVG anti-virus system (<http://www.grisoft.com>).  
Version: 6.0.593 / Virus Database: 376 - Release Date: 2/20/2004