

**Statement of Scott Culp**

**Senior Security Strategist, Trustworthy Computing Team  
Microsoft Corporation**

**Testimony Before the  
Subcommittee on Technology, Information Policy,  
Intergovernmental Relations and the Census  
House Committee on Government Reform  
U.S. House of Representatives**

**Hearing on “Cybersecurity and Vulnerability Management”**

**June 2, 2004**

Chairman Putnam, Ranking Member Clay, and Members of the Subcommittee:

My name is Scott Culp, and I am a Senior Security Strategist for Microsoft. Thank you for the opportunity to appear today. I would like to discuss patch management tools and processes that we have deployed and are continuing to improve, as well as the ongoing support we are providing and the innovation-driven technology solutions we are developing to help the federal government and all of our customers enhance the security of their computing environments. I am a member of Microsoft's Trustworthy Computing Security Strategies Team; its mission is to deliver on the security portion of Microsoft's Trustworthy Computing initiative. This is one of our company's top priorities, and I am focused on, among other topics, leading a corporate-wide initiative to improve patch management. Before joining the Trustworthy Computing Security Strategies team, I helped establish and, until 2003, managed the Microsoft Security Response Center, where I coordinated Microsoft's patch management and incident response programs.

As this subcommittee is aware, cybercrime is an industry-wide challenge, and we have developed sophisticated mechanisms designed to identify and mitigate software vulnerabilities before criminal hackers are able to exploit them. These steps, which include effective and rapid development, delivery, and installation of updates, are essential, but are not enough by themselves. One of the key security trends over the past three years has been the dramatic shortening of the time between issuance of a patch that fixes a vulnerability and the appearance of a worm carrying exploit code targeting that vulnerability. For the NIMDA virus, that period was 331 days. Only two years later, the Blaster worm shortened the window to just 26 days. And with the Sasser worm outbreak,

which was first identified on April 30, 2004, a mere 17 days passed between patch and worm.

As a result of this narrowing window, effective patch management, while essential, is not sufficient. We as an industry are innovating to develop and deliver new defenses designed to improve the security of users' systems. And for users who for one reason or another cannot apply patches to their systems, these other defenses are even more vital means to protect their systems. To help meet this need, Microsoft is employing a defense-in-depth strategy that goes beyond patch management to include advanced and security-focused software engineering, industry and government collaboration, and public education. My testimony today will focus both on patch management improvements we and our customers have made, and on how Microsoft's defense-in-depth approach can help to secure federal agencies' computing environments.

I. Microsoft's Patch Management Strategies

Microsoft recognizes that the most effective patch management strategy is to require fewer patches. We are making substantial progress in reducing the incidence of security vulnerabilities in our software. Nevertheless, the process of designing, writing and producing software is intensely complex, and software will never be completely free of vulnerabilities. So, even as we improve our software, we recognize that we must also continue to improve the quality of our updates, and the tools and processes that will help customers use them most effectively.

A. Streamlining Patch Management Processes and Incident Response Practices

Microsoft has made substantial progress in helping customers streamline their patch management processes and in enhancing our own practices with improved patch management tools, better patch delivery schedules and systems, and coordinated responses to vulnerability exploits. By working closely with our customers and partners, including federal government agencies and financial services firms, we have developed practices, processes and tools to help secure systems throughout the software lifecycle.

1. Enhancing Patch Management Tools

Microsoft actively participated in the National Cyber Security Partnership (“NCSP,” [www.cyberpartnership.org](http://www.cyberpartnership.org)) task force on Security Across the Software Development Lifecycle; we helped to develop the NCSP’s recommendations on patch management, which were released in April 2004. Our efforts to improve and streamline the patching process by enhancing the quality, accessibility, and ease of use of our patches and tools are consistent with those recommendations, and we are currently benchmarking our progress against them. Our efforts in this area have focused on:

- Improving the quality of our patches and our testing and release of patches.
  - Standardizing our testing processes with the goal of having a single company-wide testing process that delivers patches quickly and with consistently high quality.
  - Conducting a formal after-action review by the Microsoft Security Response Center (“MSRC”) and the Secure Windows Initiative Team of any security patch so that we understand how the vulnerability occurred

and what changes are needed in the development process to reduce the likelihood of introducing such vulnerabilities in the future. We also identify any security response and patch-related problems so that they too can be rectified.

- Standardizing our patches' operation and standardizing the technologies they use, to provide users with a consistent, simpler patch experience.
- Working to make all patches reversible, in order to enable customers to “roll back” a patch if they encounter an unanticipated issue, such as a conflict between the patch and a legacy application.
- Ensuring that patches register their presence on the system in a consistent, standard way -- and producing improved scanning tools that make use of this registration information -- so users can quickly determine if their machines are patched appropriately.
- Providing a consistent patch release schedule, which currently is once a month. We will provide security bulletins and patches outside this schedule when necessary, such as when exploit code for a vulnerability becomes publicly available.
- Reducing the need to reboot systems after installing a patch, as our customers are more likely to apply a patch more quickly if server availability is not interrupted. In just the final six months of 2003, we reduced reboots by 10%.

- Reducing the size of the patches whenever possible to make it easier to distribute patches across low-bandwidth networks.

## 2. Patch Management Software

In addition to the enhancements above, Microsoft also offers patch management services and tools that can assist customers, regardless of their size, in conducting more effective patch management. Microsoft offers an online update service called Windows Update which can identify missing patches for the Windows operating system and install them automatically if the user elects to do so. Later this year, we plan to deploy Microsoft Update, which will perform the same functions as Windows Update for other major Microsoft software. Users may also obtain and install updates automatically through the Automatic Update feature included in recent Microsoft operating systems; in the future, automatic updating will be available for a wider scope of updates (including service packs, for example) and software (drivers and additional types of Microsoft software).

For businesses with straightforward patch management requirements, we also offer our free System Update Server (“SUS”) patch distribution tool, which lets them, in essence, host their own Windows Update service for their companies. Windows Update Services (“WUS”), an enhanced version of SUS that will enable updating for additional Microsoft software lines as well as providing expanded automation and control capabilities, will be released soon. For customers who have more sophisticated needs such as the need to integrate patch management with application deployment and asset management, we offer System Management Server (“SMS”). Microsoft also offers a free

security scanning tool called Microsoft Baseline Security Analyzer which can scan for common system misconfigurations and missing security updates in Windows and other Microsoft applications.

Finally, we are developing advanced tools that will ease the management burden associated with managing updates. One example is called Strider, a tool that will help customers determine what level of interaction an update will have with their critical applications, thereby enabling them to tailor the amount of testing accordingly. By using Strider, customers will be able to identify the appropriate level of pre-deployment testing – a level that avoids unnecessarily lengthy and costly testing, while still giving them confidence that the update will work cooperatively with mission critical systems.

### 3. Microsoft Security Response Center and Emergency Assistance

Deploying state of the art patches and working with our customers to improve patch management processes are essential, but of equal importance is responding and communicating with our customers when vulnerabilities are discovered or there are issues that threaten our customers. MSRC is charged with providing this service by coordinating the investigation of reported vulnerabilities, the development of patches, and, together with our field teams, our customer outreach efforts. These outreach efforts include detailed security bulletins that provide information on the vulnerability, the risk it poses, and how to apply and manage the patch. In addition, Microsoft communicates with its customers through field bulletins, email outreach to more than one million subscribers, webcasts, outreach to the media and industry, and coordination with government agencies.

Should an attack or other extraordinary security incident occur, MSRC responds according to the protocols set forth in our Incident Response Process. Through this plan, we have honed our processes to rapidly mobilize Microsoft's worldwide resources when a worm like Blaster hits, to deliver information quickly to customers, and to help them protect their systems. The Incident Response Process also brings our engineering and communications departments together, enabling us to deliver the best information we can on defined timelines and to update that information at regular intervals.

The operation of the MSRC, our Incident Response Process, and our other efforts helped blunt the impact of the recent Sasser worm. Before the worm attacked, Microsoft had already significantly streamlined the patching process and launched the public awareness "Protect Your PC" campaign which led consumers to increasingly patch their systems. On April 13, 2004 Microsoft released a security bulletin and patch addressing a "critical" vulnerability. These and other efforts led to a 300% increase in the number of users who successfully patched their systems shortly after outbreak when compared with the Blaster experience.

Then, less than 24 hours after Sasser's discovery, we again contacted US-CERT with an alert and our perspective on the worm. Additionally, for those who could not patch in time, we provided, at no cost, a Sasser scanning and cleaning tool to identify the presence of the worm and remove it.

The existence of Microsoft's Anti-Virus Rewards Program encouraged individuals to provide information to law enforcement that contributed to the arrest of the Sasser author. Microsoft also worked with law enforcement, as we frequently do when

we or our customers are criminally attacked. We provide such assistance consistent with legal requirements and with respect for the privacy of our customers.

These actions, combined with the contributions of our partners in industry, the vigilance of our customers, our streamlined patching process, and the Engineering Excellence initiatives discussed below, helped the government and our customers worldwide to reduce the impact of Sasser on their systems and to limit or deter future attacks. Going forward, we are committed to continuing to meet the federal government's evolving security needs and to further improving our patch management processes.

B. Awareness and Planning

Microsoft's patches and tools rely in part on increasing awareness and education about good patch management practices and on individualized, appropriate patch management processes developed by our customers that take into account their specific mission, computing needs, system configurations, and user base. We continue to help our customers, including the federal government, to become more aware of vulnerabilities and defensive strategies and to develop effective patch management processes. Microsoft is working with key industry partners to help make federal agencies aware of security software and services that address the requirements of the Federal Information Security Management Act ("FISMA"). And through our Microsoft Services team, we mobilize security training in the field and help assess our customers' environments so that they may better prepare their systems and networks for inevitable criminal attacks.

## II. Microsoft's Defense-In-Depth Strategy

While effective patch management and emergency response capabilities are vital to creating a more secure computing environment, Microsoft's defense-in-depth strategy goes well beyond these two aspects. The security pillar of our Trustworthy Computing initiative provides the overall framework and objectives for the defense-in-depth strategy:

- **Secure by Design:** Building security into the software from day one, by conducting threat modeling on software as part of the design stage, implementing that design faithfully and using solid coding techniques, and then confirming software security via architectural and code-level reviews;
- **Secure by Default:** Installing only minimal services by default, in order to reduce the attack surface area of our software;
- **Secure in Deployment:** Providing tools and guidance to help customers deploy systems more securely in production and to maintain that security through the system's lifetime; and
- **Communications:** Working with customers and partners to provide the fastest, most accurate updates on security issues.

Within this framework, we are pursuing a five-part strategy: Building technical innovations to provide greater Isolation and Resiliency on computers and networks, Authentication and Access Control improvements, Updating (discussed above),

Engineering Excellence, and, at the same time, providing security guidance to all of our customers, including federal agencies, and working with the government on public policy initiatives.

A. Engineering Excellence

As part of Trustworthy Computing, we are strongly committed to reducing vulnerabilities by using state of the art engineering practices, standards, and processes throughout the entire cycle of creating our software. We have undertaken a rigorous “engineering excellence” initiative designed to continue to advance the state of the art in software design, development, testing and release, and to keep our engineers trained in these techniques.

At Microsoft, we have formally integrated security into many of our software development processes through the Trustworthy Computing Initiative. We are designing and developing our software with security as one of our top priorities, and we have made security an integral part of the requirements that software must pass at various milestones in the development process. Essentially, security remains a constant focal point throughout software development.

Creating more secure software starts with a formal design process that verifies the security properties of the software at each well-defined stage of construction. The need to consider security “from the ground up” is a fundamental tenet of secure system development. Such a process is intended to minimize the number of security vulnerabilities injected into the design, code, and documentation in the first place and to detect and remove those vulnerabilities as early in the development lifecycle as possible.

From inception to release, a development team along with our central security team will evaluate the security of the software at each stage of development and testing.

Because new security threats constantly arise, we provide our software teams with updates on new threats and new defensive techniques. Training for our developers, testers, and Program Managers is a critical component of the Trustworthy Computing Initiative.

This improved development process has already resulted in a notable decline of vulnerabilities in some of our server software, and a corresponding reduction in the number of patches to be developed, tested, and made available to users. For example, the number of critical or important security bulletins issued for Windows Server 2003 during its first year in the market has been approximately one-third the number reported for Windows Server 2000 during its first year in the market.

B. Isolation and Resiliency

The traditional approach to security has been to design solid security into the platform and then reactively fix any bugs that are found. But we believe there is an additional step that could be taken – namely, improving protection against entire vectors of attack in an effort to protect the customer in the interim between discovery of the vulnerability and release of the patch. We are pursuing this level of protection by increasing system isolation and resiliency, with the goal of preventing malicious code from gaining a foothold on systems or limiting its effect.

Some of our major advances in increasing system isolation and resiliency are being included in our forthcoming Windows XP Service Pack 2. Those advances include:

- Increasing network protection by turning the Windows Firewall on by default, blocking all but desired networking traffic to a particular computer.
- Making use of a capability available in some chipsets to provide memory protection to help prevent exploitation of buffer overrun vulnerabilities.
- Providing better file attachment handling for email clients and instant messaging programs such as Windows Messenger. These email and instant messaging advances will significantly help reduce the risk of email viruses and worms.
- Reducing the threat posed by malicious code on web sites by preventing downloads from web sites except with explicit user approval.
- Altering how some network-aware services operate; for example, restricting by default a computer's response to remote procedure call requests unless the requester has been authenticated.
- Adding Windows Security Center, a feature that will provide centralized security management and monitoring functions and recommend guidance when action needs to be taken. This will improve security functionality by alerting users, via a pop up message, that their anti-virus software, for example, is off and providing them with an option for help.

Similar advances will be released for Windows Server 2003 in Service Pack 1. In addition, that service pack will include technologies that give IT administrators more control over how their servers are configured and stronger firewall protection for their networks.

A technology we have already delivered is client inspection, sometimes referred to as “quarantine,” that can, for example, inspect PCs before they are given permission to connect to the network, to ensure they are patched and running an appropriately configured firewall. PCs that do not pass this inspection can be blocked and isolated from the network until they meet the corporate standards for safe access. The base capability of client inspection for VPN connections shipped in Windows Server 2003, and our research and development teams are looking at other protocols, beyond VPN, to determine how to advance this concept further and deliver it to customers.

Finally, we are developing what we call “Active Protection Technologies.” Two of these technologies are Dynamic System Protection and Behavior Blocking. Dynamic System Protection refers to technologies that adjust the appropriate level of protection when an activity happens that affects a computer’s susceptibility to attack. For instance, through Dynamic System Protection, a system might note that a particular update was not installed on the system, and automatically change some security settings to compensate. Once the patch is installed, the system will revert to its previous settings. In contrast, behavior blocking focuses on monitoring, identifying and intercepting code that acts suspiciously. User permission would then be requested before that code would be executed.

### C. Authentication and Access Control

Another important focus for us is working with other industry leaders on next-generation technologies that control who gets access to networks and computers, and how they get that access. For example, working with industry partners, we have implemented authentication solutions, such as the 802.1x protocol, which significantly improves the security protections of a wireless network. This technology has now been included in Windows XP Service Pack 1 and Windows Server 2003. We have deployed this solution on our own network, a measure that has not only improved our own network security, but has also helped us develop deployment guides for customers.

Another such technology, built into Windows Server 2000 and 2003 and Windows XP, is IPSec. IPSec protects private data in a public environment by encrypting all network traffic and requiring authentication at the individual computer level. As a result, it sets a much higher bar for network access, making it harder for outsiders to eavesdrop and representing a dramatic improvement in network security. Again, deploying this technology on our network has helped us to understand the technology better, to help customers deploy it widely within their networks, and to develop prescriptive guidance for customers such as the US Air Force, which has successfully deployed IPSec on its own networks.

Finally, Microsoft continues to work with industry partners to increase use of smart cards and other emerging, highly secure two-factor authentication techniques, and to develop future technologies that allow a computer to recognize and identify an individual with greater confidence.

#### D. Security Guidance

All the foregoing technologies, however, will not realize their full potential unless our customers, including federal agencies and their employees, have the information and training necessary to exercise appropriate security choices. That is why Microsoft has partnered with the federal government on cyber-security issues, invested in education initiatives, and provided security tools and resources on the Microsoft web site.

##### 1. Partnering With Government

Part of Microsoft's efforts at providing security guidance is directed at working with the federal government to protect its own computing environment and the country's critical infrastructure. For example, Microsoft has partnered with the Department of Homeland Security ("DHS") on two fronts. First, Microsoft has been working with DHS' National Cyber-Security Division to raise awareness of cyber-threats through the release of prompt security bulletins. And second, Microsoft has been working with DHS and other industry leaders in efforts to help foster sharing of security information within the homeland security community.

Microsoft has also been assisting the National Institute of Standards and Technology ("NIST") and the National Security Agency to develop IT security guidelines in areas such as minimum security standards and Windows operating system deployment guides for government agency systems. Those guidelines are expected to assist federal agencies in complying with NIST-developed standards which are to become mandatory in 2005. Further, Microsoft remains committed to meeting the standards set forth in the Common Criteria. Currently Windows 2000 has achieved the highest

Common Criteria certification achieved by commercial software (EAL 4), and we are now seeking certification for Windows XP, Windows Server 2003, Exchange Server, and SQL Server.

Finally, Microsoft officials have served as advisors to the President on policy and technical issues associated with information technology, cyber-security, and technology through participation in such organizations as the National Security Telecommunications Advisory Committee and the President's Information Technology Advisory Committee.

## 2. Education Initiatives

In addition to partnering with government, Microsoft has also worked with other industry members and acted on its own to improve cyber-security awareness. For example, Microsoft has joined forces with industry members and groups such as the Consumer Federation of America, the National Consumers League, Consumer Action, and the National Cybersecurity Alliance, which is supported by both DHS and the Federal Trade Commission, to promote security education.

Microsoft also is undertaking a Security Mobilization Initiative that includes in-person labs hosted by Microsoft-certified trainers to develop real-world security skills, one-day security summits and forums, and narrated security slides and demonstrations on our web site. The goal of the Initiative is to reach 500,000 business customers by the end of this year with information on how to configure and protect systems and networks to increase security. We are in the process of hosting 20 security summits around the country, including one that recently took place here in Washington D.C. on April 8, 2004. This builds on the long history of similar events Microsoft has sponsored with the federal

government, such as the biannual Government Security Summits we have hosted for the last seven years in both Washington D.C. and Redmond.

3. Microsoft.com Security Guidance

Finally, Microsoft.com offers an array of guidance forums to educate users on cyber-security. For example, we host monthly web chats where customers can ask questions relating to security in Microsoft software. Microsoft.com also hosts the Microsoft Security Developer Center where IT professionals can obtain a variety of educational materials and best practices for securing their systems. From there one can quickly reach the Security Guidance Center, which offers professionals the technical guidance, tools, training, and updates needed to assist in planning and managing a security strategy that is well-suited for their organization. Finally, Microsoft offers additional assistance in a variety of formats, including technical chats between Microsoft customers and Microsoft technology experts, Security E-Learning Clinics, and security newsletters.

E. Public Policy

Security is one of our top priorities; we have a tremendous amount of activity underway and are experiencing measurable success. Yet this is an area where we all have roles to play, including the government. As the Congress and the Administration address cybersecurity, we suggest the following actions:

First, we hope the Senate will ratify the Council of Europe Cyber Crime Treaty to help streamline international criminal investigations.

Second, our law enforcers are doing great work, and need more training and better equipment at all levels to help them investigate and prosecute cyber crimes effectively and thoroughly.

Third, government systems administrators would benefit from more intensive training in security.

Fourth, government participation in consumer education campaigns will help raise awareness about the criminal threats and the necessity of ongoing system protection.

Fifth, the NIAP/Common Criteria process is working and should be the primary information assurance certification process for government systems. We support reforms to make NIAP more efficient and cost-effective.

Finally, we support strongly increased basic research in cybersecurity and computer forensics.

We are eager to work with the government in each of these areas.

### Conclusion

We continue to pursue our Trustworthy Computing initiative, to improve our patch management processes and tools, and to assist our customers in developing and maintaining a multilayered approach to securing their systems. In the final analysis, a more secure computing environment is best achieved when industry leaders continue to innovate around security and work closely with their customers to help them keep their software up to date, configure their networks properly, train their IT staff to manage the

network appropriately and perform necessary maintenance activities, and benchmark their activities against security and patch management policies.