WORM AND VIRUS DEFENSE: HOW CAN WE PROTECT THE NATION'S COMPUTERS FROM THESE THREATS?

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 10, 2003

Serial No. 108–123

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

92–654 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
CHIP WALKER, *Professional Staff Member*
URSULA WOJCIECHOWSKI, *Clerk*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

Page

Hearing held on September 10, 2003 1

Statement of:

Akers, Greg, senior vice president, chief technology officer, government solutions and corporate security programs, Cisco Systems, Inc.; Phil Reitinger, senior security strategist, Microsoft Corp.; Vincent Gullotto, vice president, antivirus emergency response team, Network Associates, Inc.; and John Schwarz, president and chief operating officer, Symantec Corp. 125

Dacey, Robert, Director, IT Security, General Accounting Office; Richard Pethia, Director, Cert Coordination Center; Lawrence Hale, Director, FedCIRC, Department of Homeland Security; Norman Lorentz, Acting Administrator, Electronic Government and Information Technology, Office of Management and Budget; and John Malcolm, Deputy Assistant Attorney General, Criminal Division, Department of Justice 7

Eschelbeck, Gerhard, chief technology officer and vice president of engineering, Qualys, Inc.; Christopher Wysopal, co-founder, Organization for Internet Safety and director of research and development, @stake.Inc.; and Ken Silva, vice president, operations and infrastructure, Verisign, Inc. 87

Letters, statements, etc., submitted for the record by:

Akers, Greg, senior vice president, chief technology officer, government solutions and corporate security programs, Cisco Systems, Inc., prepared statement of 128

Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of 71

Dacey, Robert, Director, IT Security, General Accounting Office, prepared statement of 9

Eschelbeck, Gerhard, chief technology officer and vice president of engineering, Qualys, Inc., prepared statement of 89

Gullotto, Vincent, vice president, antivirus emergency response team, Network Associates, Inc., prepared statement of 157

Hale, Lawrence, Director, FedCIRC, Department of Homeland Security, prepared statement of 46

Lorentz, Norman, Acting Administrator, Electronic Government and Information Technology, Office of Management and Budget, prepared statement of 52

Malcolm, John, Deputy Assistant Attorney General, Criminal Division, Department of Justice, prepared statement of 58

Pethia, Richard, Director, Cert Coordination Center, prepared statement of 31

Putnam, Hon. Adam H., a Representative in Congress from the State of Florida, prepared statement of 4

Reitinger, Phil, senior security strategist, Microsoft Corp., prepared statement of 142

Schwarz, John, president and chief operating officer, Symantec Corp., prepared statement of 175

Silva, Ken, vice president, operations and infrastructure, Verisign, Inc., prepared statement of 110

Wysopal, Christopher, co-founder, Organization for Internet Safety and director of research and development, @stake.Inc., prepared statement of 98

WORM AND VIRUS DEFENSE: HOW CAN WE PROTECT THE NATION'S COMPUTERS FROM THESE THREATS?

WEDNESDAY, SEPTEMBER 10, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam, Miller, and Clay.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Chip Walker, Scott Klein, and Lori Martin, professional staff members; Ursula Wojciechowski, clerk; Suzanne Lightman, fellow; Jamie Harper and Erik Glavich, legislative assistants; David McMillen, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. PUTNAM. The quorum being present, the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order. Good morning.

Today we continue our in-depth review of cyber security issues affecting our Nation. There are several things unique to cyber attacks that make the task of preventing them difficult. Cyber attacks can occur from anywhere around the globe, from the caves of Afghanistan to the battlefields of Iraq, from the most remote regions in the world or right here in our own back yard. The technology used for cyber attacks is readily available and changes continually, and perhaps most dangerous of all is the failure of many people, including those who are critical to securing these networks and information from attack, to take the threat seriously, to receive adequate training and take proactive steps needed to secure their networks. A severe cyber attack would have devastating repercussions throughout the Nation in a physical sense and in real economic dollars.

The initial plan for this hearing was to focus primarily on strategies and methodologies within the agencies of the Federal Government for identifying and mitigating computer vulnerabilities through a system of patch management. Recent events, however, have caused us to expand the boundaries of this hearing to include computer systems throughout the Nation.

This summer, everyone once again realized how vulnerable our computer networks are to cyber attack. The Blaster worm and SoBig.F virus brought home the reality that unsecured computer systems are all too prevalent and that as a Nation across all levels, government, business and home users, we must take computer security more seriously than we have in the past. The Blaster worm infected over 400,000 computers in under 5 days. In fact, 1 in 3 Internet users are infected with some type of virus or worm every year.

The speed at which worms and viruses can spread is astonishing and a contributing fact to that rapid spread is the lethargic pace at which people deploy the patches that can prevent infection in the first place. Microsoft announced the vulnerability and had the patch available weeks before the exploit appeared.

Recent viruses and worms have been blamed for bringing down train signaling stations throughout the East, affecting the entire CSX railroad system, which covers 23 States. Additionally, new information is coming to light that the Blaster worm is being linked to the severity of the power blackout of last month. The North American Electric Reliability Council blames another worm, Slammer, for impairing bulk electric system control by bringing down networks. We learned last week that the U.S. Nuclear Regulatory Commission issued a formal information notice to nuclear power plant operators warning them about an incident in January in which the Slammer computer worm penetrated networks in Ohio's Davis-Besse nuclear plant and disabled two important monitoring systems for hours.

A recent Gartner study predicts that by the year 2005, 90 percent of cyber attacks will attempt to exploit vulnerabilities for which a patch is already available or a solution known. So why aren't systems patched and why aren't anti-virus programs kept up to date? This hearing will examine the issues surrounding these incidents, including how vulnerabilities are discovered, how the public is notified about potential vulnerabilities, the mechanisms for protection, the real and potential problems presented by patch systems and the scope of the problem confronting the Federal Government, the business community, and the general public.

System administrators are often overwhelmed with simply maintaining all the systems they have responsibility for overseeing. Challenges that organizations face in maintaining their systems are significant. With an estimated 4,000 vulnerabilities being discovered every year, it is an enormous challenge for any but the best resourced organizations to install all of the software patches that are released by the manufacturer. Not only is the sheer quantity of patches overwhelming for administrators and everyone else to keep up with, but patches can be difficult to apply and have unexpected side effects on other systems that administrators must then evaluate and address. As a result, after a patch is released, administrators often take a long time to fix all of their vulnerable computer systems. Obviously small organizations and home users who lack the skills of system administrators are even less likely to keep up with the flow of patches.

The Department of Homeland Security's Federal Computer Incident Response Center recently let a $10.8 million 5-year contract

for governmentwide patch management service to notify agencies about security holes in commercial software for systems on their networks and the availability of patches to fix them. The service is known as the patch authentication and dissemination capability [PADC]. The goal is to simplify patch management by providing administrators only with information relevant to their systems and ensuring that patches are genuine and affected. PADC went on-line in January of this year. According to officials, once agency system administrators have provided a profile of their systems and software, PADC will alert them to potential vulnerabilities, provide interim security advice until a patch is available, disseminate available patches and keep management informed of available patches and which ones their systems administrators have downloaded.

Large organizations such as business and educational institutions often rely on commercial firms to notify them of vulnerabilities. For example, there are several firms that offer vulnerability notification combined with analysis of the customer's computer system for those vulnerabilities. These firms also provide information on where to get the patches and prioritize them for administrators. In addition, the commercial critical infrastructure sectors depend on information from their information sharing analysis centers [ISACs], to help them respond to potential cyber threats. These ISACs are designed to allow members of a sector to share information about incidents to help increase preparedness and vigilance. The progress of Blaster demonstrates the importance of the early warning systems that ISACs are tasked with developing.

Independent researchers discover most vulnerabilities. These researchers may be academics, consultants or Black Hats. The Organization for Internet Security is working with software vendors, consultants and other interested parties to formalize procedures for dealing with vulnerabilities, including vendor notification and control disclosures. There's a very important role for government to play in these disclosure procedures. It is no longer acceptable for vendors to determine on their own schedule who gets notified and when. Given the potential national security risk that can emanate from the exploitation of a vulnerability, it is imperative that the appropriate government entities be involved in this process from the beginning.

Vulnerabilities in software and the worms and viruses that exploit them have become a fact of life for the Internet. The government, law enforcement and private industry must develop and continue to update a plan to deal with these emerging threats.

How can we educate home and small business users to minimize the risk posed by zombie computers? How can researchers, the government and software industry work together to identify and remedy vulnerabilities in the most instructive manner? And how will the Federal Government evolve an effective patch management program? What can be done to expedite the discovery and prosecution of cyber criminals who release worms and viruses? And most important of all, how can the Federal Government, law enforcement and industry work together to protect the vital infrastructure of the Internet?

[The prepared statement of Hon. Adam H. Putnam follows:]

TOM DAVIS, VIRGINIA
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER, MARYLAND
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT
INDEPENDENT

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

Oversight Hearing

"Worm and Virus Defense: How Can We Protect the Nation's Computers from These Serious Threats?"

Wednesday, September 10, 2003
10:00 a.m.

Opening Statement

Chairman Adam Putnam (R-Fl)

Good morning. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Today we continue our in-depth review of cyber security issues affecting our nation. There are several things unique to cyber attacks that make the task of preventing them particularly difficult. Cyber attacks can occur from anywhere around the globe: from the caves of Afghanistan to the war fields of Iraq, from the most remote regions of the world or simply right here in our own back yard.

The technology used for cyber attacks is readily available and changes continually. And, maybe most dangerous of all, is the failure of many people – including many of those who are critical to securing these networks and information from attack -- to take the threat seriously, to receive adequate training, and to take proactive steps needed to secure their networks. A severe cyber attack could have serious repercussions throughout the nation both in a physical sense and in very real economic dollars.

The initial plan for this hearing was to focus primarily on strategies and methodologies within the agencies of the federal government for identification and mitigation of computer vulnerabilities through a system of "patch management". However, recent events caused us to expand the boundaries of this hearing to include computer systems throughout our nation. This summer everyone -- once again -- realized just how vulnerable our computer networks are to cyber attack. The Blaster worm and SoBigF virus brought home the reality that unsecured computer systems are all too prevalent and that – as a nation – across all levels, government, business and home users, we absolutely must take computer security more seriously.

The Blaster worm infected over 400,000 computers in less than five days. In fact, about one in three Internet users are infected with some type of virus or worm every year. The speed at which worms and viruses can spread is astonishing. What's equally astonishing is the lethargic pace at which people deploy the patches that can prevent infection in the first place. Microsoft announced the vulnerability, and had the patch available… weeks before the exploit appeared.

The recent viruses and worms have been blamed for bringing down train signaling systems throughout the East, affecting the entire CSX system, which covers 23 states. Additionally, new information coming to light shows that the Blaster worm is being linked to the severity of the power blackout of last month. The North American Electric Reliability Council blames another worm, Slammer, for impairing bulk electric system control by bringing down networks. We learned last week that The U.S. Nuclear Regulatory Commission issued a formal Information Notice to nuclear power plant operators warning them about an incident in January in which the Slammer computer worm penetrated networks at Ohio's Davis-Besse nuclear plant and disabled two important monitoring systems for hours.

A recent Gartner study predicts that by the year 2005, 90 percent of cyber attacks will attempt to exploit vulnerabilities for which a patch is available or a solution known. So, why aren't systems patched and anti-virus programs kept up to date? This hearing will examine the issues surrounding these incidents, including how vulnerabilities are discovered, how the public is notified about potential vulnerabilities, the mechanisms that exist for protecting systems, the real and potential problems presented by patching systems, and the scope of the problem confronting the federal government, the business community and the general public.

System administrators are often times overwhelmed with simply maintaining all the systems they have responsibility for overseeing. Challenges that organizations face in maintaining their systems are significant: with an estimated 4,000 vulnerabilities being discovered each year, it is an enormous challenge for any but the best-resourced organizations to install all of the software patches that are released by the manufacturer. Not only is the sheer quantity of patches overwhelming for administrators to keep up with, but patches can be difficult to apply and also have potentially unexpected side effects on other system components that administrators must then evaluate and address. As a result, after a security patch is released, system administrators often take a long time to fix all their vulnerable computer systems. Obviously, small organizations and home users, who lack the skills of system administrators, are even less likely to be able to keep up with the flow of patches.

The Department of Homeland Security's (DHS) Federal Computer Incident Response Center recently awarded a $10.8 million, five-year contract for a government-wide patch

management service to notify agencies about security holes in commercial software for systems on their networks, and the availability of patches to fix them. The service is known as the Patch Authentication and Dissemination Capability (PAD C).

The goal is to simplify patch management by providing administrators only with information relevant to their IT systems and ensuring that patches are genuine and effective. PAD C went on-line in January of this year.

According to officials, once agency system administrators have provided a profile of their systems and software, PAD C will alert them to potential vulnerabilities, provide interim security advice until a patch is made available, disseminate available patches, and keep management informed of available patches and which ones their systems administrators have downloaded.

Large organizations, such as business and educational institutions, often rely on commercial firms to notify them of vulnerabilities. For example, there are several firms that offer vulnerability notification, combined with analysis of the customer's computer systems for vulnerabilities. These firms also provide information on where to get the patches and prioritize them for the system administrators.

In addition, the commercial critical infrastructure sectors depend on information from their Information Sharing and Analysis Centers (ISACs) to help them respond to potential cyber threats. These ISACs are designed to allow members of a sector to share information about incidents to help increase preparedness and vigilance. The progress of Blaster demonstrates the importance of the early warning systems that ISACs are tasked with developing.

Independent researchers discover most vulnerabilities. These researchers may be academics, consultants or black hats. The Organization for Internet Security is working with software vendors, consultants and other interested parties to formalize procedures for dealing with vulnerabilities, including vendor notification and controlled disclosures. There is a very important role for government to play in the disclosure procedures. It is simply not acceptable for vendors to determine on their own schedule who gets notified and when. Given the potential national security risk that could emanate from the exploitation of a vulnerability, it is imperative that the appropriate government entities be involved in this process from the very beginning.

Vulnerabilities in software, and the worms and viruses that exploit them, have become a fact of life for the Internet. The government, law enforcement and private industry must develop...and continue to update... a plan to deal with these emerging threats. How can we educate home and small business users to minimize the risk posed by zombie computers? How can researchers, the government and the software industry work together to identify and remedy vulnerabilities in the most constructive manner? How will the federal government evolve an effective patch management program? What can be done to expedite the discovery and prosecution of cyber criminals who release worms and viruses? And, most important of all, how can the federal government, law enforcement and industry work together to protect the vital infrastructure of the Internet?

We have an excellent line-up of witnesses this morning who will share with use their expertise as we explore Worms and Viruses, how can be better protect the Nation's computers?

Mr. PUTNAM. We have an outstanding line up of witnesses this morning who will share with us their expertise as we explore worms and viruses and how we can better protect the Nation's computers. As is the custom of this committee, we'll ask our witnesses as they are seated in panel one to rise and be sworn in.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all of the witnesses responded in the affirmative. We will begin with our first witness, and we have three panels. The panels are rather large panels. They are unusually large for this subcommittee, but the scope of our topic demanded it. But we would ask that all of our witnesses adhere as best they can to our 5-minute rule. And I will introduce Mr. Dacey.

Robert Dacey is currently Director of Information, Security Issues at the U.S. General Accounting Office. His responsibilities include evaluating information systems security in Federal agencies and corporations, including the development of related methodologies, assessing the Federal infrastructure for managing information security, evaluating the Federal Government's efforts to protect our Nation's private and public critical infrastructure from cyber threats and identifying best security practices at leading organizations and promoting their adoption by Federal agencies. In addition to his many years at information security auditing, Mr. Dacey has also led GAO's annual audits of the consolidated financial statements of the U.S. Government, GAO'S financial audit quality assurance efforts, including methodology and training and other GAO financial statement audits. We appreciate you being a part of this panel, and you are recognized for 5 minutes.

STATEMENTS OF ROBERT DACEY, DIRECTOR, IT SECURITY, GENERAL ACCOUNTING OFFICE; RICHARD PETHIA, DIRECTOR, CERT COORDINATION CENTER; LAWRENCE HALE, DIRECTOR, FEDCIRC, DEPARTMENT OF HOMELAND SECURITY; NORMAN LORENTZ, ACTING ADMINISTRATOR, ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET; AND JOHN MALCOLM, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, DEPARTMENT OF JUSTICE

Mr. DACEY. Thank you, Mr. Chairman. I am pleased to be here today to participate in the subcommittee's hearing on cyber incidents and the role of software patch management in mitigating the risks that these types of events will recur. I will briefly summarize my written statement.

The exploitation of software vulnerabilities by hackers and others can result in significant damage to both Federal and private sector computer systems, ranging from Web site defacements to gaining the ability to read, modify or delete sensitive information, destroy systems, disrupt operations or launch attacks against other organizations. The number of reported security vulnerabilities and software products has grown dramatically in recent years to over 11,000 cumulatively reported by CERT/CC since 1995.

Factors increasing the risk of system vulnerabilities and exploits include the increasing complexity and size of software programs, the increasing sophistication and availability of hacking tools, in-

creasing system interconnectivity combined with decreasing length of time from the announcement of a vulnerability until it is exploited, and decreasing length of time for attacks to infiltrate the Internet.

Although generally available before vulnerability exploits are launched, patches are too frequently not installed, resulting in damages to unpatched systems. My written testimony refers to several of these exploits and summarizes the responses to two recently reported serious vulnerabilities.

Given these increasing risks, effective patch management programs have become critical to securing both Federal and private sector systems. Key elements of a patch management program include top management support, standardized policies, procedures and tools; dedicated resources and clearly assigned responsibilities; current technology inventories; identification of relevant vulnerabilities and patches; patch risk assessment and testing; patch distribution; and monitoring system through networks and host vulnerability scanning.

There are several efforts to address software vulnerability in the Federal systems, including OMB reporting requirements concerning agency patch management programs as part of the Federal Information Security Management Act [FISMA]; NIST, patch management guidance, and FedCIRC incident reporting, handling and prevention handling services. For example, as you mentioned in your statement, FedCIRC provides PADC, a patch notification service, which provides agencies at no charge with information on trusted authenticated patches for their specific technologies. PADC currently has 41 agency subscribers, although OMB recently reported that actual usage of those accounts are extremely low.

A number of commercial tools and resources are available that can assist in performing patch management functions more efficiently and effectively, such as identifying relevant patches, deploying patches, scanning systems for vulnerabilities and providing management reporting. In addition to implementing effective patch management processes, several other steps can be taken to address software vulnerabilities. These include one, deploying other technologies such as antivirus software, firewalls and other network security and configuration tools to provide a layered defense against attacks; two, employing more rigorous software engineering practices in designing, implementing and testing software products to reduce the number of potential vulnerabilities; three, improving tools to more efficiently and effectively manage patching; four, researching and developing technologies to prevent, detect and recover from attacks as well as identify perpetrators; and five, ensuring effective tested contingency planning processes and procedures.

Mr. Chairman, this concludes my statement. I will be pleased to answer any questions that you have at this time.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, September 10, 2003

INFORMATION SECURITY

Effective Patch Management is Critical to Mitigating Software Vulnerabilities

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-03-1138T

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-03-1138T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform

Why GAO Did This Study

Attacks on computer systems—in government and the private sector—are increasing at an alarming rate, placing both federal and private-sector operations and assets at considerable risk. By exploiting software vulnerabilities, hackers can cause significant damage. While patches, or software fixes, for these vulnerabilities are often well publicized and available, they are frequently not quickly or correctly applied.

The federal government recently awarded a contract for a governmentwide patch notification service designed to provide agencies with information to support effective patching. Forty-one agencies now subscribe to this service.

At the request of the Chairman of the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, GAO reviewed (1) two recent software vulnerabilities and related responses; (2) effective patch management practices, related federal efforts, and other available tools; and (3) additional steps that can be taken to better protect sensitive information systems from software vulnerabilities.

www.gao.gov/cgi-bin/getrpt–GAO-03-1138T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

September 10, 2003

INFORMATION SECURITY

Effective Patch Management is Critical to Mitigating Software Vulnerabilities

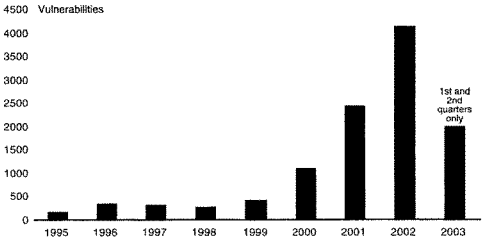
What GAO Found

The increase in reported information systems vulnerabilities has been staggering, especially in the past 3 years (see chart). Automated attacks are successfully exploiting such software vulnerabilities, as increasingly sophisticated hacking tools become more readily available and easier to use. The response to two recent critical vulnerabilities in Microsoft Corporation and Cisco Systems, Inc., products illustrates the collaborative efforts between federal entities and the information security community to combat potential attacks.

Patch management is one means of dealing with these increasing vulnerabilities to cybersecurity. Critical elements to the patch management process include management support, standardized policies, dedicated resources, risk assessment, and testing. In addition to working with software vendors and security research groups to develop patches or temporary solutions, the federal government has taken a number of other steps to address software vulnerabilities. For example, offered without charge to federal agencies, the federal patch notification service provides subscribers with information on trusted, authenticated patches available for their technologies. At present, the government is considering broadening the scope of these services and capabilities, along with the number of users. Other specific tools exist that can assist in performing patch management.

In addition to implementing effective patch management practices, several additional steps can be taken when addressing software vulnerabilities. Such steps include stronger software engineering practices and continuing research and development into new approaches toward computer security.

Security Vulnerabilities, 1995—First Half of 2003 (11,155 in the aggregate)



Source: Carnegie-Mellon University's CERT® Coordination Center.

United States General Accounting Office

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to participate in the Subcommittee's hearing on recent cyber incidents and the role of software patch management[1] in mitigating the risks that these types of events will recur. Current incidents inundating the Internet, coupled with the increasing number and sophistication of attacks, place both federal and private-sector operations and assets at considerable risk. Several of these incidents exploited software vulnerabilities for which patches were already publicly available.

In my testimony today I will discuss (1) two recent software vulnerabilities and related responses; (2) effective patch management practices, related federal efforts, and other available tools; and (3) additional steps that can be taken to better protect sensitive information systems from software vulnerabilities.

In preparing for this testimony, we analyzed professional information technology security literature, including research studies and reports about cybersecurity-related vulnerabilities. We also interviewed private-sector and federal officials about their patch management experiences. And we analyzed relevant documents and interviewed officials of the Patch Authentication and Dissemination Capability (PADC) service and supporting contractors to determine the service's current capabilities and usage. Finally, we reviewed actions taken by PADC and agency officials in response to recent cybersecurity vulnerabilities. Our work was performed in accordance with generally accepted government auditing standards, from June to September 2003.

[1]A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered. Patch management is the process of effectively applying available patches.

Results in Brief

Since 1995, over 11,000 security vulnerabilities in software products have been reported. Along with these increasing vulnerabilities, the sophistication of attack technology has steadily advanced. Attacks such as viruses and worms[2] that once took weeks or months to propagate over the Internet now take only hours, or even minutes. In just the past 3 months, two critical and widespread vulnerabilities were identified in products from Microsoft Corporation and Cisco Systems, Inc. Federal agencies were affected by the Blaster and Welchia worms, which exploited the Microsoft vulnerability. The response to these recent events illustrates how federal entities are communicating and coordinating with software vendors and security research groups to combat such attacks.

Effective patch management, one means of dealing with these increasing security threats, includes several critical elements, such as top management support, standardized policies, dedicated resources, risk assessment, and testing. In the federal arena, the Department of Homeland Security now provides agencies with information on trusted, authenticated patches for their specific technologies without charge. This service, known as PADC, currently has 41 agency subscribers. Other tools and resources also exist that can assist in performing patch management functions.

Patch management is but one—albeit important and essential—component in the protection of systems from security vulnerabilities. However, in the longer term, the nation's ability to withstand attacks may ultimately come from more rigorous software engineering practices and better tools and technologies. My statement today will highlight steps we can take now and in the future to help reduce our vulnerability to cyber intrusion.

Background: Vulnerabilities and Exploits

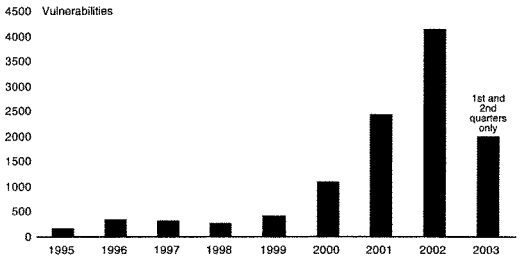
Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. For example, Microsoft Windows 2000 reportedly contains about 35 million lines of code, compared with about 15 million lines for Windows 95. As reported by the National Institute of Standards and Technology (NIST), based on various studies of code inspections, most estimates suggest that there are as many as 20 flaws per thousand lines of software code. While most flaws do not

[2]A virus is a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. In contrast, a worm is an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

create security vulnerabilities,[3] the potential for these errors reflects the difficulty and complexity involved in delivering trustworthy code.[4] By exploiting software vulnerabilities, hackers and others who spread malicious code can cause significant damage, ranging from Web site defacement to taking control of entire systems, and thereby being able to read, modify, or delete sensitive information, destroy systems, disrupt operations, or launch attacks against other organizations' systems.

Between 1995 and the first half of 2003, the CERT® Coordination Center[5] (CERT/CC) reported 11,155 security vulnerabilities that resulted from software flaws. Figure 1 illustrates the dramatic growth in security vulnerabilities over these years.

Figure 1: Security Vulnerabilities, 1995—first half of 2003



Source: GAO analysis based on Carnegie-Mellon University's CERT® Coordination Center data.

The growing number of known vulnerabilities increases the number of potential attacks created by the hacker community. As vulnerabilities are discovered, attackers may attempt to exploit them. Attacks can be launched against specific targets or widely distributed through viruses and worms.

[3] A vulnerability is the existence of a flaw or weakness in hardware or software that can be exploited resulting in a violation of an implicit or explicit security policy.

[4] National Institute for Standards and Technology, *Procedures for Handling Security Patches: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-40 (Gaithersburg, MD: August 2002).

[5] The CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie-Mellon University.

Worms and viruses are commonly used to launch denial-of-service attacks, which generally flood targeted networks and systems with so much transmission of data that regular traffic is either slowed or completely interrupted. Such attacks have been utilized ever since the groundbreaking Morris worm, which brought 10 percent of the systems connected to Internet systems to a halt in November 1988. In 2001, the Code Red worm used a denial-of-service attack to affect millions of computer users by shutting down Web sites, slowing Internet service, and disrupting business and government operations.[6] This type of attack continues to be used by recent worms, including Blaster, which I will discuss further later in my testimony.

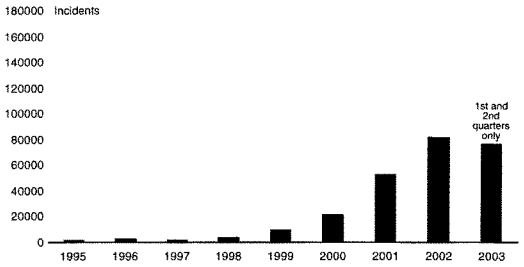
The sophistication and effectiveness of cyber attack have steadily advanced. Because automated tools now exist, CERT/CC has noted, attacks that once took weeks or months to propagate over the Internet now take just hours, or even minutes. Code Red achieved an infection rate of over 20,000 systems within 10 minutes, foreshadowing more damaging and devastating attacks. Indeed, earlier this year, the Slammer worm, which successfully attacked at least 75,000 systems, became the fastest computer worm in history, infecting more than 90 percent of vulnerable systems within 10 minutes.

Frequently, skilled hackers develop exploitation tools and post them on Internet hacking sites. These tools are then readily available for others to download, allowing even inexperienced programmers to create a computer virus or to literally point and click to launch an attack. According to a NIST publication, 30 to 40 new attack tools are posted to the Internet every month.[7]

The threat to systems connected to the Internet is illustrated by the increasing number of computer security incidents reported to CERT/CC. This number rose from just under 10,000 in 1999 to over 52,000 in 2001, to about 82,000 in 2002, and to over 76,000 for the first and second quarters of 2003. And these are only the incidents that are reported. According to the Director of CERT/CC, as much as 80 percent of actual incidents go unreported, in most cases because the organization was either unable to recognize that its systems had been penetrated (because there were no indications of penetration or attack) or because it was reluctant to report an incident. Figure 2 illustrates the number of incidents reported to CERT/CC from 1995 through the second quarter of 2003.

[6]U.S. General Accounting Office, *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures,* GAO-01-1073T (Washington D.C.: August 29, 2001).
[7]U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk,* GAO-01-751 (Washington D.C.: August 13, 2001).

Figure 2: Information Security Incidents, 1995—first half of 2003



Source: GAO analysis based on Carnegie-Mellon University's CERT® Coordination Center data.

According to CERT/CC, about 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches; however, such patches are often not quickly or correctly applied. Maintaining current patches is becoming more difficult, as the length of time between the awareness of a vulnerability and the introduction of an exploit is shrinking. For example, the Blaster worm was released almost simultaneously with the announcement of the vulnerability it exploited.

Successful attacks on unpatched software vulnerabilities have caused billions of dollars in damage. Following are examples of significant damage caused by worms that could have been prevented had available patches been effectively installed:

- In September 2001 the Nimda worm appeared, reportedly infecting hundreds of thousands of computers around the world, using some of the most significant attack methods of Code Red II and 1999's Melissa virus that allowed it to spread widely in a short amount of time. A patch had been made publicly available the previous month.

- On January 25, 2003, Slammer triggered a global Internet slowdown and caused considerable harm through network outages and other unforeseen consequences. As we discussed in our April testimony, the worm reportedly shut down a 911 emergency call center, canceled airline flights, and caused automated teller machine (ATM) failures.[5] According to media reports, First USA Inc., an Internet service provider, experienced network performance problems after an attack by the Slammer worm, due to a

[5]U.S. General Accounting Office, *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures,* GAO-03-564T (Washington, D.C.: April 8, 2003).

failure to patch three of its systems. Additionally, the Nuclear Regulatory Commission reported that Slammer also infected a nuclear power plant's network, resulting in the inability of the computers to communicate with each other, disrupting two important systems at the facility. In July 2002, Microsoft had released a patch for its software vulnerability that was exploited by Slammer. Nevertheless, according to media reports, some of Microsoft's own systems were infected by Slammer.

In addition to understanding the threat posed by security vulnerabilities, it is useful to understand the process of vulnerability identification and response. In general, when security vulnerabilities are discovered, a process is initiated to effectively address the situation through appropriate reporting and response. Typically, this process begins when security vulnerabilities are discovered by software vendors, security research groups, users, or other interested parties, including the hacker community. When a software vendor is made aware of a vulnerability in its product, the vendor typically first validates that the vulnerability indeed exists. If the vulnerability is deemed critical, the vendor may convene a group of experts, including major clients and key incident-response groups such the Federal Computer Incident Response Center (FedCIRC) and CERT/CC, to discuss and plan remediation and response efforts.

After a vulnerability is validated, the software vendor develops and tests a patch and/or workaround. A workaround may entail blocking access to or disabling vulnerable programs.

The incident response groups and the vendor typically prepare a detailed public advisory to be released at a set time. The advisory often contains a description of the vulnerability, including its level of criticality; systems that are affected; potential impact if exploited; recommendations for workarounds, and Web site links where a patch (if publicly available) can be downloaded. Incident-response groups as well as software vendors may continue to issue updates as new information about the vulnerability is discovered. When a worm or virus is reported that exploits a vulnerability, virus detection software vendors also participate in the process. Such vendors develop and make available to their subscribers downloadable "signature files" that are used, in conjunction with their software, to identify and stop the virus or worm from infecting systems protected by their software. The Organization for Internet Safety (OIS), which consists of leading security researchers and vendors, recently issued a voluntary framework for vulnerability reporting and response.[9]

[9]Organization for Internet Safety, *Guidelines for Security Vulnerability Reporting and Response, Version 1.0* (July 2003).

Collaborative Response to Two Recent Software Vulnerabilities

Recently, two critical vulnerabilities were discovered in widely used commercial software products. The federal government and the private-sector security community took steps, described below in chronological order, to collaboratively respond to the threat of potential attacks against these vulnerabilities.

Microsoft Remote Procedure Call Vulnerability Exploited by Hacker

Last Stage of Delirium Research Group discovered a security vulnerability in Microsoft's Windows Distributed Component Object Model (DCOM)[10] Remote Procedure Call (RPC)[11] interface. This vulnerability would allow an attacker to gain complete control over a remote computer.

- On June 28, 2003, the group notified Microsoft about the RPC vulnerability. Within hours of being notified, Microsoft verified the vulnerability.
- On July 16, Microsoft issued a security bulletin publicly announcing the critical vulnerability and providing workaround instructions and a patch.
- The following day, CERT/CC issued its first advisory.
- Nine days after Microsoft's announcement, on July 25, Xfocus, an organization that researches and demonstrates security vulnerabilities, released code that could be used to exploit the vulnerability.
- On July 31, CERT/CC issued a second advisory reporting that multiple exploits had been publicly released, and encouraged all users to apply the patches.
- On August 11, 2003, the Blaster worm (also known as Lovsan) was launched to exploit this vulnerability. When the worm is successfully executed, it can cause the operating system to crash. Experts consider Blaster, which affected a range of systems, to be one of the worst exploits of 2003. Although the security community had received advisories from CERT/CC and other organizations to patch this critical vulnerability, Blaster reportedly infected more than 120,000 unpatched computers in the first 36 hours. By the following day, reports began to state that many users were experiencing slowness and disruptions to their Internet service, such as the need to frequently reboot. The Maryland Motor Vehicle Administration was forced to shut down, and systems in both national and

[10]Distributed Component Object Model (DCOM) allows direct communication over the network between software components.
[11]Remote Procedure Call (RPC) is a protocol of the Windows operating system that allows a program from one computer to request a service from a program on another computer in a network, thereby facilitating interoperability.

international arenas have also been affected. The worm was programmed to launch a denial-of-service attack on Microsoft's Windows Update Web site www.windowsupdate.com (where users can download security patches) on August 16. Microsoft preempted the worm's attack by disabling the Windows Update Web site.

- On August 14, two variants to the original Blaster worm were released. Federal agencies reported problems associated with these worms to FedCIRC.

- On August 18, Welchia, a worm that also exploits this vulnerability, was reported. Among other things, it attempts to apply the patch for the RPC vulnerability to vulnerable systems, but reportedly creates such high volumes of network traffic that it effectively denies services in infected networks. Media reports indicate that Welchia affected several federal agencies, including components of the Departments of Defense and Veterans Affairs.

The federal government's response to this vulnerability included coordination with the private sector to mitigate the effects of the worm.

- On July 17, FedCIRC issued an advisory to encourage federal agencies to patch the vulnerability, followed by several advisories from the Department of Homeland Security (DHS).

- The following week, on July 24, DHS issued its first advisory to heighten public awareness of the potential impact of an exploit of this vulnerability.[12]

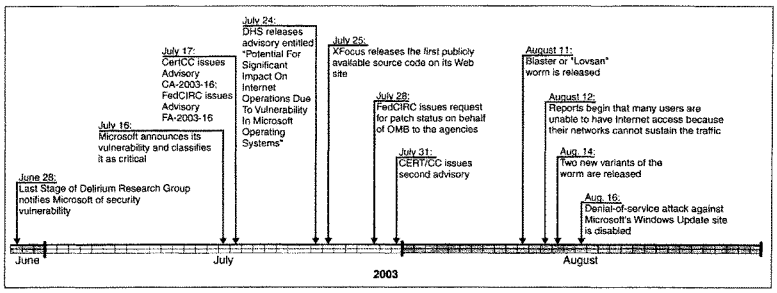
- On July 28, on behalf of the Office of Management and Budget (OMB), FedCIRC requested that federal agencies report on the status of their actions to patch the vulnerability.

- From August 12 to August 18, DHS's National Cyber Security Division hosted several teleconferences with federal agencies, CERT/CC, and Microsoft.

Figure 3 is a timeline of selected responses to the Blaster Internet worm.

[12]Department of Homeland Security, *Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems* (Washington, D.C.: July 24, 2003).

Figure 3: Event Timeline for the Blaster Internet Worm



Source: GAO.

Based on an analysis of the agencies reported actions, as requested on July 28, FedCIRC indicated that many respondents had completed patch installation on all systems at the time of their report and that only a minimal number of infections by the Blaster worm were reported.

Cisco IOS Vulnerability Exploits Attempted

Cisco Systems, Inc., which controls approximately 82 percent of the worldwide share of the Internet router[13] market, discovered a critical vulnerability in its Internet operating system (IOS) software. This vulnerability could allow an intruder to effectively shut down unpatched routers, blocking network traffic. Cisco had informed the federal government of the vulnerability prior to public disclosure, and worked with different security organizations and government organizations to encourage prompt patching.

- On July 16, 2003, Cisco issued a security bulletin to publicly announce the critical vulnerability in its IOS software, and provide workaround instructions and a patch. Cisco had planned to officially notify the public of the vulnerability on July 17, but early media disclosure led them to announce the vulnerability a day earlier. In addition, FedCIRC issued advisories to federal agencies and DHS advised private-sector entities of the vulnerability. In the week that the vulnerability was disclosed, FedCIRC, OMB, and DHS's National Cyber Security Division held a number of teleconferences with representatives from the executive branch.

[13]Routers are devices that forward Internet and network traffic between networks and are critical to their operation.

- On July 17, OMB requested that federal agencies report to CERT/CC on the status of their actions to patch the vulnerability by July 24.
- On July 18, DHS issued an advisory update in response to an exploit that was posted online, and OMB moved up the agencies' reporting deadline to July 22.

CERT/CC has received reports of attempts to exploit this vulnerability, but as of September 5, no incidents have yet been reported.

Patch Management: A Critical Process for Mitigating Cyber Vulnerabilities

Patch management is a process used to help alleviate many of the challenges involved with securing computing systems from attack. It is a component of configuration management[14] that includes acquiring, testing, and applying patches to a computer system. I will now discuss common patch management practices, federal efforts to address software vulnerabilities in agencies, and services and tools to assist in carrying out the patch management process.

Common Practices for Effective Patch Management

Effective patch management practices have been identified in security-related literature from several groups, including NIST, Microsoft,[15] patch management software vendors, and other computer-security experts. Common elements identified include the following:

- **Senior executive support.** Management recognition of information security risk and interest in taking steps to manage and understand risks, including ensuring that appropriate patches are deployed, is important to successfully implementing any information security–related process and ensuring that appropriate resources are applied.
- **Standardized patch management policies, procedures, and tools.** Without standardized policies and procedures in place, patch management can remain an ad-hoc process—potentially allowing each subgroup within an entity to implement patch management differently or not at all. Policies provide the foundation for ensuring that requirements are communicated across an entity. In addition, selecting and implementing appropriate patch management tools is an important consideration for facilitating effective and efficient patch management.

[14]Configuration management is the control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of a system.
[15]Microsoft Corporation, *Solutions for Security, Solutions for Management: The Microsoft Guide to Security Patch Management* (Redmond, WA: 2003).

- **Dedicated resources and clearly assigned responsibilities.** It is important that the organization assign clear responsibility for ensuring that the patch management process is effective. NIST recommends creating a designated group whose duties would include supporting administrators in finding and fixing vulnerabilities in the organization's software. It is also important that the individuals involved in patch management have the skills and knowledge needed to perform their responsibilities, and that systems administrators be trained regarding how to identify new patches and vulnerabilities.

- **Current technology inventory**. Creating and maintaining a current inventory of all hardware equipment, software packages, services, and other technologies installed and used by the organization is an essential element of successful patch management. This systems inventory assists in determining the number of systems that are vulnerable and require remediation, as well as in locating the systems and identifying their owners.

- **Identification of relevant vulnerabilities and patches**. It is important to proactively monitor for vulnerabilities and patches for all software identified in the systems inventory. Various tools and services are available to assist in identifying vulnerabilities and their respective patches. Using multiple sources can help to provide a more comprehensive view of vulnerabilities.

- **Risk assessment**. When a vulnerability is discovered and a related patch and/or alternative workaround is released, the entity should consider the importance of the system to operations, the criticality of the vulnerability, and the risk of applying the patch. Since some patches can cause unexpected disruption to entities' systems, organizations may choose not to apply every patch, at least not immediately, even though it may be deemed critical by the software vendor that created it. The likelihood that the patch will disrupt the system is a key factor to consider, as is the criticality of the system or process that the patch affects.

- **Testing**. Another critical step is to test each individual patch against various systems configurations in a test environment before installing it enterprisewide to determine any impact on the network. Such testing will help determine whether the patch functions as intended and its potential for adversely affecting the entity's systems. In addition, while patches are being tested, organizations should also be aware of workarounds, which can provide temporary relief until a patch is applied. Testing has been identified as a challenge by government and private-sector officials, since the urgency in remediating a security vulnerability can limit or delay comprehensive testing. Time pressures can also result in software vendors' issuing poorly written patches that can degrade system performance and require yet another patch to remediate the problem. For instance, Microsoft has admittedly issued security patches that have been recalled because they have caused systems to crash or are too large for a computer's capacity. Further, a complex, heterogeneous systems

environment can lengthen this already time-consuming and time-sensitive process because it takes longer to test the patch in various systems configurations.

- **Distributing patches.** Organizations can deploy patches to systems manually or by using an automated tool. One challenge to deploying patches appropriately is that remote users may not be connected at the time of deployment, leaving the entity's networks vulnerable from the remote user's system because they have not yet been patched. One private-sector entity stated that its network first became affected by the Microsoft RPC vulnerability when remote users plugged their laptops into the network after being exposed to the vulnerability from other sources.

- **Monitoring through network and host vulnerability scanning.** Networks can be scanned on a regular basis to assess the network environment, and whether patches have been effectively applied. Systems administrators can take proactive steps to preempt computer security incidents within their entities by regularly monitoring the status of patches once they are deployed. This will help to ensure patch compliance with the network's configuration.

Federal Efforts to Address Software Vulnerabilities

The federal government has taken several steps to address security vulnerabilities that affect federal agency systems, including efforts to improve patch management. NIST has taken a number of steps, including, as I previously mentioned, providing a handbook for patch management. In addition, NIST offers a source of vulnerability data, which I will discuss later in this testimony. Further, in accordance with OMB's reporting instructions for the first year implementation of the Federal Information Security Management Act (FISMA), maintaining up-to-date patches is a part of FISMA's system configuration requirements. As such, OMB requires that agencies report how they confirm that patches have been tested and installed in a timely manner.[16] In addition, certain governmentwide services are offered to federal agencies to assist them in ensuring that software vulnerabilities are patched. For example, FedCIRC was established to provide a central focal point for incident reporting, handling, prevention, and recognition for the federal government. Its purpose is to ensure that the government has critical services available in order to withstand or quickly recover from attacks against its information resources.

In addition, for the two recent vulnerabilities just discussed in my testimony, OMB and FedCIRC held teleconferences with agency Chief information officers to discuss vulnerabilities and request that agencies

[16] *Title III—Federal Information Security Management Act of 2002, E-Government Act of 2002*, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.

report on the status of their actions to patch them. An OMB official indicated that they planned to hold meetings with agencies to discuss ways to improve communication of and followup on critical vulnerabilities, including addressing some of the challenges identified in the two recent exercises, such as delays in reaching key security personnel in certain instances.

FedCIRC also initiated PADC to provide users with a method of obtaining information on security patches relevant to their enterprise and access to patches that have been tested in a laboratory environment. The federal government offers PADC to federal civilian agencies at no cost. According to FedCIRC, as of last month, 41 agencies were using PADC. Table 2 lists its features and benefits, as reported by FedCIRC. OMB reported that while many agencies have established PADC accounts, actual usage of those accounts is extremely low.

Table 2: Reported Features and Benefits of the Patch Authentication and Dissemination Capability

Features	Benefits
• Authorized government users subscribe from a secure Web interface.	• Notifications to subscribers will occur when a patch is available for subscriber-selected systems or applications.
• Subscribers create customized notification profiles, including operating systems, firewalls, routers, antivirus software, intrusion-detection systems, and servers.	• FedCIRC will ensure that the patch originates from a reliable source.
• Subscribers are notified when new threats or vulnerabilities are discovered; notifications are updated as vendor patches are released and authenticated.	• FedCIRC will validate that the patch eliminates the intended vulnerability.
• Subscribers may visit a secure site to download validated patches.	• All aspects of the system are secure from subscriber information to the secure download of patches.
• Subscribers may contact the PADC Help Desk to verify information or to seek assistance.	• Single consolidated source for all patch updates. • No cost to federal civilian government agencies.

Source: FedCIRC.

To participate in PADC, subscribers (who could be one or more individuals within an agency) receive an account license that allows them to receive notifications and log into the secure Web site to download the patch. To establish an account, each subscriber must set up a profile defining the technologies that they use. The profiles act much like a filtering service and allow PADC to notify agencies of only the patches that pertain to their systems. The profiles do not include system–specific information because of the sensitivity of that information. Subscribers using PADC receive notification of threats, vulnerabilities, and the availability of patches on the basis of the submitted profiles. They are notified by E-mail or pager message that a vulnerability or patch has been posted to a secure Web site that affects one or all of their systems.

When a patch is identified, FedCIRC, through contractor support, ensures that it originates from a reliable source. The patch is then tested on a system to which it applies. The installation of the patch and the operation of the system are monitored to ensure that the patch causes no problem. Next, if an exploit had been developed, exploit testing is performed to ensure that the patch fixes the vulnerability. Any issues identified with a patch are summarized and provided to the users. The validated patch is then uploaded to PADC servers and made available to users. A patch is considered validated when it has been downloaded from a trusted source, authenticated, loaded onto an appropriate system, tested, exploit–tested, verified, and posted to the PADC server. This type of testing and validation is performed for over 60 technologies that, according to FedCIRC officials, account for approximately 80 percent of the technologies used by federal agencies. Also available is notification of patches that are not validated for over 25,000 additional technologies.

According to FedCIRC officials, high-priority patches are to be tested and posted on the PADC server within the same business day of availability. Medium- and low-priority patches are to be completed by the following business day, but are generally available sooner. However, because PADC has several early warning mechanisms in place and arrangements with software vendors, some patches may be available as soon as a vulnerability is made public. FedCIRC officials emphasize that although the contractor tests the security patches, these tests do not ensure that the patch can be successfully deployed in another environment; therefore, agencies still need to test the patch for compatibility with their own business processes and technology.

PADC offers a reporting capability that is hierarchical. Senior managers can look at their complete system and see which subsystems have been patched. These enterprisewide reports and statistics can be generated for a "reporting user" subscriber who has read-only capability within the system.

According to agency officials, there are limitations to the PADC service. Although it is free to agencies, only about 2,000 licenses or accounts are available because of monetary constraints. According to FedCIRC

officials, this requires them to work closely with participating agencies to balance the number of licenses that a single agency requires with the need to allow multiple agencies to participate. For example, the National Aeronautics and Space Administration initially requested over 3,000 licenses—one for each system administrator. Another agency, NIST, thought that each of its users should have his or her own PADC account. Another limitation is the level of services currently provided by PADC. At present, the government is considering broadening the scope of these services and capabilities, along with the number of users.

Services and Tools Also Provide Means for Improving Patch Management

Several services and automated tools are available to assist entities in performing the patch management function, including tools designed to be stand-alone patch management systems. In addition, systems management tools can be used to deploy patches across an entity's network. Some of the features in services and tools typically include methods to

- inventory computers and the software applications and patches installed;
- identify relevant patches and workarounds and gather them in one location;
- group systems by departments, machine types, or other logical divisions to easily manage patch deployment;
- scan a network to determine the status of the patches and other corrections made to network machines (hosts and/or clients);
- assess the machines against set criteria;
- access a database of patches;
- test patches;
- deploy effective patches; and
- report information to various levels of management about the status of the network.

Patch management vendors also offer central databases of the latest patches, incidents, and methods for mitigating risks before a patch can be deployed or a patch has been released. Some vendors provide support for multiple software platforms, such as Microsoft, Solaris, Linux, and others, while others focus on certain platforms exclusively, such as Microsoft.

Patch management tools can be either scanner-based (non agent) or agent-based. While scanner-based tools can scan a network, check for missing patches, and allow an administrator to patch multiple computers,

these tools are best suited for smaller organizations due to their inability to serve a large number of users without breaking down or requiring major changes in procedure. Another difficulty with scanner-based tools is that part-time users and turned-off systems will not be scanned.

Agent-based products place small programs, or agents, on each computer, to periodically poll a patch database—a server on the network—for new updates, giving the administrator the option of applying the patch. Agent-based products require up-front work to integrate agents into the workstations and in the server deployment process, but are better suited to large organizations due to their ability to generate less network traffic and provide a real-time network view. The agents maintain information that can be reported when needed. Finally, some patch management tools are hybrids—allowing the user to utilize agents or not.

Instead of an automated stand-alone system, entities can also use other methods and tools to perform patch management. For example, they can maintain a database of the versions and latest patches for each server and each client in their network and track the security alerts and patches manually. While labor-intensive, this can be done. In addition, entities can employ systems management tools with patch-updating capabilities to deploy the patches. This method requires monitoring for the latest security alerts and patches. Entities may also need to develop better relationships with their vendors to be alerted to vulnerabilities and patches prior to public release. In addition, software vendors may provide automated tools with customized features to alert system administrators and users of the need to patch, and if desired, automatically apply patches.

A variety of resources are also available to provide information related to vulnerabilities and their exploits. As I mentioned earlier, one resource is CERT/CC, a major center for analyzing and reporting vulnerabilities as well as providing information on possible solutions. Another useful resource is NIST's ICAT, which offers a searchable index leading users to vulnerability resources and patch information. ICAT links users to publicly available vulnerability databases and patch sites, thus enabling them to find and fix vulnerabilities existing on their systems. It is based on common vulnerability and exposures (commonly referred to as CVE) naming standards. These are standardized names for vulnerabilities and other information security exposures, compiled in an effort to make it easier to share data across separate vulnerability databases and tools.

Many other organizations exist, including the Last Stage of Delirium Research Group, that research security vulnerabilities and maintain databases of such vulnerabilities. In addition, mailing lists, such as BugTraq, provide forums for announcing and discussing vulnerabilities, including information on how to fix them. In addition, Security Focus monitors thousands of products to maintain a vulnerability database and provide security alerts. Finally, vendors such as Microsoft and Cisco provide software updates on their products, including notices of known vulnerabilities and their corresponding patches.

Additional Steps That Can Be Taken

In addition to implementing effective patch management practices, several additional steps can be considered when addressing software vulnerabilities, including:

- deploying other technologies, such as antivirus software, firewalls, and other network security tools to provide additional defenses against attacks;
- employing more rigorous engineering practices in designing, implementing, and testing software products to reduce the number of potential vulnerabilities;
- improving tools to more effectively and efficiently manage patching;
- researching and developing technologies to prevent, detect, and recover from attacks as well as identify their perpetrators, such as more sophisticated firewalls to keep serious attackers out, better intrusion-detection systems that can distinguish serious attacks from nuisance probes and scans, systems that can isolate compromised areas and reconfigure while continuing to operate, and techniques to identify individuals responsible for specific incidents; and
- ensuring effective, tested contingency planning processes and procedures.

Actions are already underway in many, if not all, of these areas. For example, CERT/CC has a research program, one goal of which is to try to find ways to improve technical approaches for identifying and preventing security flaws, for limiting the damage from attacks, and for ensuring that systems continue to provide essential services in spite of compromises and failures. Also, Microsoft recently initiated its Trustworthy Computing strategy to incorporate security-focused software engineering practices throughout the design and deployment of its software, and is reportedly considering the use of automated patching in future products.

———————

In summary, it is clear from the increasing number of reported attacks on information systems that both federal and private-sector operations and assets are at considerable—and growing—risk. Patch management can be an important element in mitigating the risks associated with software vulnerabilities, part of overall network configuration management and information security programs. The challenge will be ensuring that a patch management process has adequate resources and appropriate policies, procedures, and tools to effectively identify vulnerabilities and patches that place an entity's systems at risk. Also critical is the capability to adequately test and deploy the patches, and then monitor progress to ensure that they work. Although this can currently be performed, the

eventual solution will likely come from research and development to better build security into software and tools from the beginning.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time. Should you have any further questions about this testimony, please contact me at (202) 512-3317 or at daceyr@gao.gov.

Individuals making key contributions to this testimony included Shannin G. Addison, Michael P. Fruitman, Michael W. Gilmore, Sophia Harrison, Elizabeth L. Johnston, Min S. Lee, and Tracy C. Pierson.

(310507)

Mr. PUTNAM. Thank you very much, Mr. Dacey. I appreciate you adhering to our 5-minute rule as well.

Our next witness is Richard Pethia. Mr. Pethia directs the CERT Coordination Center, which conducts security incident response activities and fosters the development of incident response infrastructures that leads to rapid correction of vulnerabilities and resolution of incidents. Working out of the software engineering institute at Carnegie Mellon University, he has been tracking vulnerabilities for 15 years. Before coming to SEI, Mr. Pethia was the Director of Engineering at the Decision Data Co. He has over 30 years experience in both technical and managerial positions.

You are recognized for 5 minutes, Mr. Pethia.

Mr. PETHIA. Thank you, Mr. Chairman, and thank you especially for the opportunity to testify on the issue of defending against cyber viruses and worms. At the CERT Coordination Center since 1988, we have handled over 260,000 security incidents and have helped to resolve over 11,000 vulnerabilities, published hundreds of security alerts and security best practice guides and provide training in a variety of security topics.

Worms and viruses are both in a more general category of programs called malicious code. Both exploit weaknesses in computer software, replicating themselves and are attaching themselves to other programs. They spread quickly. By definition, worms are programs that spread without human intervention once they have been introduced into the system. And viruses are programs that require some action on the part of the user, such as opening an e-mail attachment. Today these worms and viruses are causing damage more quickly than those created in the past and are spreading to the most vulnerable of all systems, computer systems of home users.

The Code Red worm spread around the world faster in 2001 than the Melissa virus did in 1999. Just months later, the NIMDA worm caused serious damage within an hour of the first reported infection. And in January of this year Slammer had significant impact in just minutes. Virus and worm attacks alone have resulted in millions of dollars of loss in just the last 12 months. The 2003 computer crime survey states that viruses are the most cited form of attack with an estimated cost of over $27 million across the approximately 500 respondents to the survey. Estimates on the Blaster worm and the SoBig.F virus range from $525 million to more than $1 billion in loss. The cost estimates include lost productivity, wasted hours, lost sales and extra bandwidth cost.

For the past 15 years we have relied heavily on fast reaction to ensure the damage is minimized. But today it's clear that reactive solutions alone are no longer adequate. Many attacks are now fully automated and spread with blinding speed. The attack technology has become increasingly complex, increasing the time it takes to analyze the attack and produce countermeasures. We have been increasingly dependent on the Internet. Even short interruptions in service cause significant loss and can jeopardize critical service.

Aggressive, coordinated, continually improving response will continue to be necessary, but we also must move quickly to put other solutions in place. System operators must adopt security practices such as information security risk assessments, security manage-

ment policies and secure system administrations practices. Senior managers must provide visible endorsement and financial support for these security improvement efforts. They must also keep their skills and knowledge current and educate their users to raise awareness of security issues and improve their ability to recognize and respond to problems. Technology vendors must also take steps such as producing virus resistant or virus proof software, dramatically reducing the number of implementation errors in their products that lead to vulnerabilities, and providing secure out of the box configurations that have security options turned on rather than require users to enable the functions.

The government can also help by taking a multi-pronged approach: Using its buying power to demand higher quality software, holding vendors more accountable for defects in released products and providing incentives for low defect products and for products that are highly resistant to viruses.

Information assurance research is also needed to yield networks capable of surviving attacks while preserving sensitive information. Among the activities should be the creation of a unified and integrated framework for all information assurance, rigorous methods to assess and manage risk, quantitative techniques to determine the cost benefit of risk mitigation strategies, systematic tools and simulation tools to analyze cascade effects of attacks and new technologies for resisting, recognizing and recovering from attacks, accidents and failures.

More technical specialists should be trained to expand its scholarship programs to build the university infrastructure we will need for the long-term development of trained security professionals. And to encourage safe computing the government should support the development of education material and programs about cyber space for all users, including home users and small businesses, support programs to provide early training and security practices in appropriate use.

In conclusion, our dependence on interconnected computing systems is rapidly increasing and even short-term disruptions from viruses and worms have major consequences. Our current solutions are not keeping pace with the increased strength and speed of attack and our information infrastructures are at risk.

The National Cyber Security Division formed by the Department of Homeland Security is a critical step toward implementation of some of these recommendations. However, implementing a safer cyber space will require the NCSD and the entire Federal Government to work with State and local governments, the private sector to drive better software practices, more secure products, higher awareness at all levels, increase research and development activities and increase training for special computer users and all users.

Thank you.

[The prepared statement of Mr. Pethia follows:]

Viruses and Worms: What Can We Do About Them?

Testimony of Richard D. Pethia
Director, CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Before the Subcommittee
on Technology, Information Policy,
Intergovernmental Relations and the Census

September 10, 2003

Introduction

Mr. Chairman and Members of the Subcommittee:
My name is Rich Pethia. I am the director of the CERT® Coordination Center (CERT/CC). Thank you for the opportunity to testify on the important issue of cyber security. Today I will discuss viruses and worms and the steps we must take to protect our systems from them.

The CERT/CC was formed in 1988 as a direct result of the first Internet worm. It was the first computer security incident to make headline news, serving as a wake-up call for network security. In response, the CERT/CC was established by the Defense Advanced Research Projects Agency at Carnegie Mellon University's Software Engineering Institute, in Pittsburgh. Our mission is to serve as a focal point to help resolve computer security incidents and vulnerabilities, to help others establish incident response capabilities, and to raise awareness of computer security issues and help people understand the steps they need to take to better protect their systems. We activated the center in just two weeks, and we have worked hard to maintain our ability to react quickly. The CERT/CC staff has handled 260,000 incidents, cataloged and worked on resolutions to more than 11,000 computer vulnerabilities, and published hundreds of security alerts. Today, with continued sponsorship from the Department of Defense and from the Department of Homeland Security, we continue our work and disseminate security information and warnings through multiple channels—a web site (www.cert.org), an online vulnerability database, and an electronic mailing list of more than 161,000 addresses. We have relationships with major media outlets, which help us distribute accurate information about major security events to the broad community. We also work with over 600 technology vendors to facilitate their response to product vulnerabilities and warn the community of vulnerabilities that require immediate attention.

The CERT/CC is now recognized by both government and industry as a neutral, authoritative source of data and expertise on information assurance. In addition to handling reports of computer security breaches and vulnerabilities in network-related technology, we identify and publish preventive security practices, conduct research, and provide training to system administrators, managers, and incident response teams.

Growing Risk from Worms and Viruses

Worms and viruses are in a more general category of programs called "malicious code." Both exploit weaknesses in computer software, replicating themselves and/or attaching themselves to other programs. They spread quickly and easily from system to system. By definition, worms are programs that spread with no human intervention after they are started. Viruses are programs that require some action on the part of the user, such as opening an email attachment, before they spread. Users are often enticed to open email attachments, sometimes because of an intriguing or legitimate-sounding subject line and sometimes, when address books have been compromised, because the email appears to be from someone the user knows. Worms and viruses can bypass security measures, such as firewalls, and clog systems to the point that response is slow or shut off.

Today, worms and viruses are causing damage more quickly than those created in the past and are spreading to the most vulnerable of all systems – The computer systems of home users. The Code Red worm spread around the world faster in 2001 than the so-called Morris worm moved through U.S. computers in 1988, and faster than the Melissa virus in 1999. With the Code Red worm, there were days between first identification and widespread damage. Just months later, the Nimda worm caused serious damage within an hour of the first report of infection. In January of this year, Slammer had significant impact in just minutes.

The figures attached to the end of this testimony show the speed and magnitude of the Blaster worm compared to previous worms, as well as indications of Blaster's and Sobig.F's continued impact. Figure 1, *Blaster, Slammer, and Code Red Growth Over Day 1,* shows how quickly Slammer infected a significant number of computer systems. It shows that Blaster was slightly slower than Slammer, but still much faster than Code Red. After 24 hours, Blaster had infected 336,000 computers; Code Red infected 265,000; and Slammer had infected 55,000. Figure 2, *Comparing Blaster and Code Red in the First 18 Hours,* shows the growth in the number of computers reached by the Blaster and Code Red worms in the first 18 hours. In both cases, 100,000 computers were infected in the first 3 to 5 hours. The fast exploitation limits the time security experts like those at the CERT/CC have to analyze the problem and warn the Internet community. Likewise, system administrators and users have little time to protect their systems.

Figure 3, *Blaster-Infected Systems Scanning per Hour: Long-Lasting Effects,* demonstrates how far-reaching worms and viruses can be. After the initial surge of infections from the Blaster worm and subsequent patching, the impact reached a steady-state of 30,000 computers in any given hour However, it is a different 30,000 computers (an average of 150,000 in any given day), depending on the time of day. Peaks represent activity in different parts of the world, cycling through business days. Even the Northeast blackout only slowed the worm down for a few hours. The Blaster worm is still active and continues to have impacts on computer systems across the globe.

Impact of Worms and Viruses

At best, worms and viruses can be inconvenient and costly to recover from. At worst, they can be devastating. Virus and worm attacks alone have resulted in millions of dollars of loss in just the last twelve months.

In the 2003 CSI/FBI Computer Crime and Security Survey (www.gocsi.com), viruses were the most cited form of attack (82% of respondents were affected), with an estimated cost of $27,382,340. The lowest reported cost to a victim was $40,000, and the highest was $6,000,000. The Australian Computer Crime and Security Survey found similar results, with 80% of respondents affected by viruses or worms. Of the victims, 57% reported financial losses, totaling $2,223,900. According to the Australian survey, one-third (33%) of the victims recovered in less than one day, and 30% recovered in one to seven days. The other 37% took more time, including two organizations that believe they might never recover.

So far, damages from the Blaster worm are estimated to be at least $525 million, and Sobig.F damages are estimated to be from $500 million to more than one billion dollars (*Business Week,* the London-based mi2g (www.mi2g.com), among other reports in the media).The cost estimates include lost productivity, wasted hours, lost sales, and extra bandwidth costs. *The Economist* (August 23, 2003) estimated that Sobig.F was responsible for one of every 16 email messages that crossed the Internet. In our own experience, Sobig.F has accounted for 87% of all email to our cert@cert.org address since August 18. We have received more than 10,000 infected messages a day, or one message every 8.6 seconds. Figure 4, *Emails messages per Day to cert@cert.org,* shows this in a graph. Sobig.F was so effective because it could send multiple emails at the same time, resulting in thousands of messages a minute. Moreover, Sobig has been refined many times, making it harder to stop (the "F" stands for the 6th version).

Implications for the Future

The significance of our recent experience with Blaster and Sobig.F lies beyond their specific activity. Rather, the worms represent a larger problem with Internet security and forecasts what we can expect in the future.

My most important message today is that the Internet is not only vulnerable to attack today, but it will stay vulnerable to attack in the foreseeable future. This includes computers used by government organizations at all levels and computers used at research laboratories, in schools, in business, and at home. They are vulnerable to problems that have already been discovered, sometimes years ago, and they are vulnerable to problems that will be discovered in the future.

The implications for Federal, state, and local governments and for critical infrastructure operators is that their computer systems are vulnerable both to attack and to being used to further attacks on others. With more and more government and private sector organizations increasing their dependence on the Internet, our ability to carry on business reliably is at risk.

Reactive Solutions are Limited

For the past 15 years, we have relied heavily on the ability of the Internet community as a whole to react quickly enough to security attacks to ensure that damage is minimized and attacks are quickly defeated. Today, however, it is clear that reactive solutions alone are no longer adequate. To briefly summarize the factors,

- The Internet now connects over 171,000,000 computers and continues to grow at a rapid pace. At any point in time, there are millions of connected computers that are vulnerable to one form of attack or another.
- Attack technology has now advanced to the point where it is easy for attackers to take advantage of these vulnerable machines and harness them together to launch high-powered attacks.
- Many attacks are now fully automated and spread with blinding speed across the entire Internet community, regardless of geographic or national boundaries.
- The attack technology has become increasingly complex and in some cases intentionally stealthy, thus increasing the time it takes to discover and analyze the attack mechanisms in order to produce antidotes.
- Internet users have become increasingly dependent on the Internet and now use it for many critical applications as well as online business transactions. Even relatively short interruptions in service cause significant economic loss and can jeopardize critical services.

These factors, taken together, indicate that we can expect many attacks to cause significant economic losses and service disruptions within even the best response times that we can realistically hope to achieve. Aggressive, coordinated, continually improving response will continue to be necessary, but we must also move quickly to put other solutions in place.

Recommended Actions – What Can System Operators Do?

Addressing the threat of worms and viruses is not easy. With approximately 4,000 vulnerabilities being discovered each year, system and network administrators are in a difficult situation. They are challenged with keeping up with all the systems they have and all the patches released for those systems. Patches can be difficult to apply and might even have unexpected side effects. We have found that, after a vendor releases a security patch, it takes a long time for system operators to fix all the vulnerable computer systems. It can be months or years before the patches are

implemented on 90-95 percent of the vulnerable computers. For example, the CERT/CC still receives reports of outbreaks of the Melissa virus, which exploits vulnerabilities that are more than four years old.

There are a variety of reasons for the delay. The job might be too time-consuming, too complex, or just given too low a priority. Because many managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Moreover, business policies sometimes lead organizations to make suboptimal tradeoffs between business goals and security needs. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.

In the face of this difficult situation, there are steps system operators and their organizations can take to help protect systems:

Adopt security practices: It is critical that organizations, large and small, adopt the use of effective information security risk assessments, management policies, and security practices. While there is often discussion and debate over which particular body of practices might be in some way "best," it is clear that descriptions of effective practices and policy templates are widely available from both government and private sources, including the CERT/CC. The Internet Security Alliance, for example, has recently published a "Common Sense Guide For Senior Mangers" that outlines the security management and technical practices an organization should adopt to improve its security. Guidelines and publications are also available from the National Institute of Standards and Technology, the National Security Agency, and other agencies.

What is often missing today is management commitment: senior management's visible endorsement of security improvement efforts and the provision of the resources needed to implement the required improvements.

Keep skills and knowledge current. System operators should attend courses that enhance their skills and knowledge, and they should be given the necessary time and support to do so. They need to keep current with attack trends and with tools that help them protect their systems against the attacks. The security problem is dynamic and ever-changing with new attacks and new vulnerabilities appearing daily.

Help educate the users of their systems. System operators must provide security awareness programs to raise users' awareness of security issues, improve their ability to recognize a problem, instruct them on what to do if they identify a problem, and increase their understanding of what they can do to protect their systems,

Recommended Actions – What Can Technology Vendors Do?

The steps available to system operators will help, but will only solve parts or the problem. Technology vendors are in a position to prevent the spread of worms and viruses more effectively. Although some companies have begun moving toward improvement in the security in their products, there is a long way to go. Software developers do not devote enough effort to applying lessons learned about the causes of vulnerabilities. The CERT/CC continues to see the same types of vulnerabilities in newer versions of products that were in earlier versions.

Additional vulnerabilities come from the difficulty of securely configuring operating systems and applications. These products are complex and often shipped to customers with security features disabled, forcing the technology user to go through the difficult and error-prone process of

properly enabling the security features they need. While the current practices allow the user to start using the product quickly and reduce the number of calls to the product vendor's service center when a product is released, it results in many Internet-connected systems that are misconfigured from a security standpoint. This opens the door to worms and viruses.

It is critical for technology vendors to produce products that are impervious to worms and viruses in the first place. In today's Internet environment, a security approach based on "user beware" is unacceptable. The systems are too complex and the attacks happen too fast for this approach to work. Fortunately, good software engineering practices can dramatically improve our ability to withstand attacks. The solutions required are a combination of the following:

- **Virus-resistant/virus-proof software.** There is nothing intrinsic about computers or software that makes them vulnerable to viruses. Viruses propagate and infect systems because of design choices that have been made by computer and software designers. Designs are susceptible to viruses and their effects when they allow the import of executable code, in one form or another, and allow that code to be executed without constraint on the machine that received it. Unconstrained execution allows program developers to easily take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack. To effectively control viruses in the long term, vendors must provide systems and software that constrain the execution of imported code, especially code that comes from unknown or untrusted sources. Some techniques to do this have been known for decades. Others, such as "sandbox" techniques, are more recent.
- **Dramatically reducing implementation errors**. Most vulnerabilities in products come from software implementation errors. They remain in products, waiting to be discovered, and are fixed only after they are found while the products are in use. In many cases, identical flaws are continually reintroduced into new versions of products. The great majority of these vulnerabilities are caused by low level design or implementation (coding) errors. Vendors need to be proactive, study and learn from past mistakes, and adopt known, effective software engineering practices that dramatically reduce the number of flaws in software products.
- **High-security default configurations**. With the complexity of today's products, properly configuring systems and networks to use the strongest security built into the products is difficult, even for people with strong technical skills and training. Small mistakes can leave systems vulnerable and put users at risk. Vendors can help reduce the impact of security problems by shipping products with "out of the box" configurations that have security options turned on rather than require users to turn them on. The users can change these "default" configurations if desired, but they would have the benefit of starting from a secure base configuration.

Recommended Actions – What Can the Government Do?

The government can help by taking a multi-pronged approach. Actions that I believe should be investigated include the following:

Provide incentives for higher quality/more security products. To encourage product vendors to produce the needed higher quality products, we encourage the government to use its buying power to demand higher quality software. The government should consider upgrading its contracting processes to include "code integrity" clauses—clauses that hold vendors more accountable for defects, including security defects, in released products and provide incentives for

vendors that supply low defect products and products that are highly resistant to viruses. The lower operating costs that come from use of such products should easily pay for the incentive program.

Also needed in this area are upgraded acquisition processes that put more emphasis on the security characteristics of systems being acquired. In addition, to support these new processes, acquisition professionals need to be given training not only in current government security regulations and policies, but also in the fundamentals of security concepts and architectures. This type of skill building is essential in order to ensure that the government is acquiring systems that meet the spirit, as well as the letter, of the regulations.

Information assurance research. It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.

Thus, the government should support a research agenda that seeks new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Among the activities should be the creation of

- A unified and integrated framework for all information assurance analysis and design
- Rigorous methods to assess and manage the risks imposed by threats to information assets
- Quantitative techniques to determine the cost/benefit of risk mitigation strategies
- Systematic methods and simulation tools to analyze cascade effects of attacks, accidents, and failures across interdependent systems
- New technologies for resisting attacks and for recognizing and recovering from attacks, accidents, and failures

More technical specialists. Government identification and support of cyber-security centers of excellence and the provision of scholarships that support students working on degrees in these universities are steps in the right direction. The current levels of support, however, are far short of what is required to produce the technical specialists we need to secure our systems and networks. These programs should be expanded over the next five years to build the university infrastructure we will need for the long-term development of trained security professionals.

More awareness and training for Internet users. The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life to the Internet. As a result, many Internet users have little understanding of Internet technology or the security practices they should adopt. To encourage "safe computing," there are steps we believe the government could take:

- Support the development of educational material and programs about cyberspace for all users. There is a critical need for education and increased awareness of the security characteristics, threats, opportunities, and appropriate behavior in cyberspace. Because the survivability of systems is dependent on the security of systems at other sites, fixing one's own systems is not sufficient to ensure those systems will survive attacks. Home

users and business users alike need to be educated on how to operate their computers most securely, and consumers need to be educated on how to select the products they buy. Market pressure, in turn, will encourage vendors to release products that are less vulnerable to compromise.

- Support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries.[1] Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need be educated as well and should reinforce lessons in security and behavior on computer networks.

The National Cyber Security Division (NCSD), formed by the Department of Homeland Security in June 2003, is a critical step towards implementation of these recommendations. The mission of NCSD and the design of the organization are well-aligned to successfully coordinate implementation of the recommendations that I have described here. However, implementing a "safer-cyberspace" will require, the NCSD and the entire Federal government to work with state and local governments and the private sector to drive better software practices, higher awareness at all levels, increased research and development activities, and increased training for technical specialists.

Conclusion

Our dependence on interconnected computing systems is rapidly increasing, and even short-term disruptions from viruses and worms can have major consequences. Our current solutions are not keeping pace with the increased strength and speed of attacks, and our information infrastructures are at risk. Solutions are not simple but must be pursued aggressively to allow us to keep our information infrastructures operating at acceptable levels of risk. We can make significant progress by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge level of users, and increasing research into secure and survivable systems. Additional government support for research, development, and education in computer and network security would have a positive effect on the overall security of the Internet.

---

[1]National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, 1991, recommendation 3c, p. 37.

Attachments

Figure 1	Blaster, Slammer, and Code Red Growth Over Day 1
Figure 2	Comparing Blaster and Code Red in the First 18 Hours
Figure 3	Blaster-Infected Systems Scanning per Hour: Long-Lasting Effects
Figure 4	Email Messages per Day to cert@cert.org

Figure 1

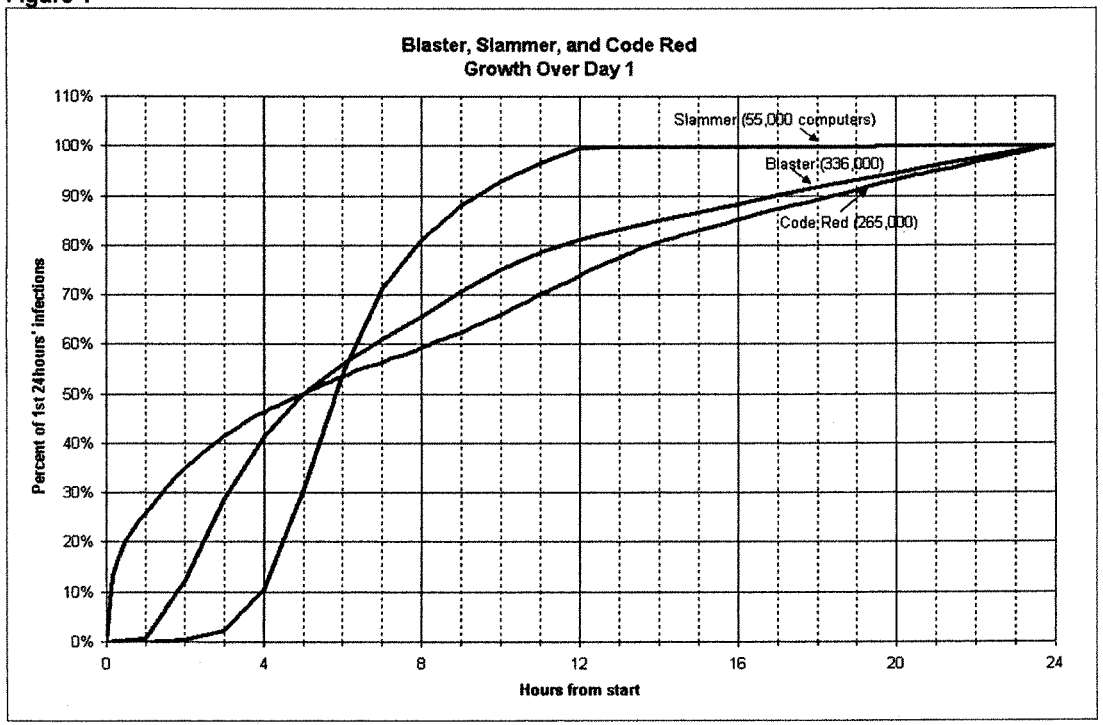

Blaster, Slammer, and Code Red
Growth Over Day 1
Slammer (55,000 computers)
Blaster (336,000)
Code Red (265,000)
Percent of 1st 24hours' infections
110%
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
0
4
8
12
16
20
24
Hours from start

Figure 2

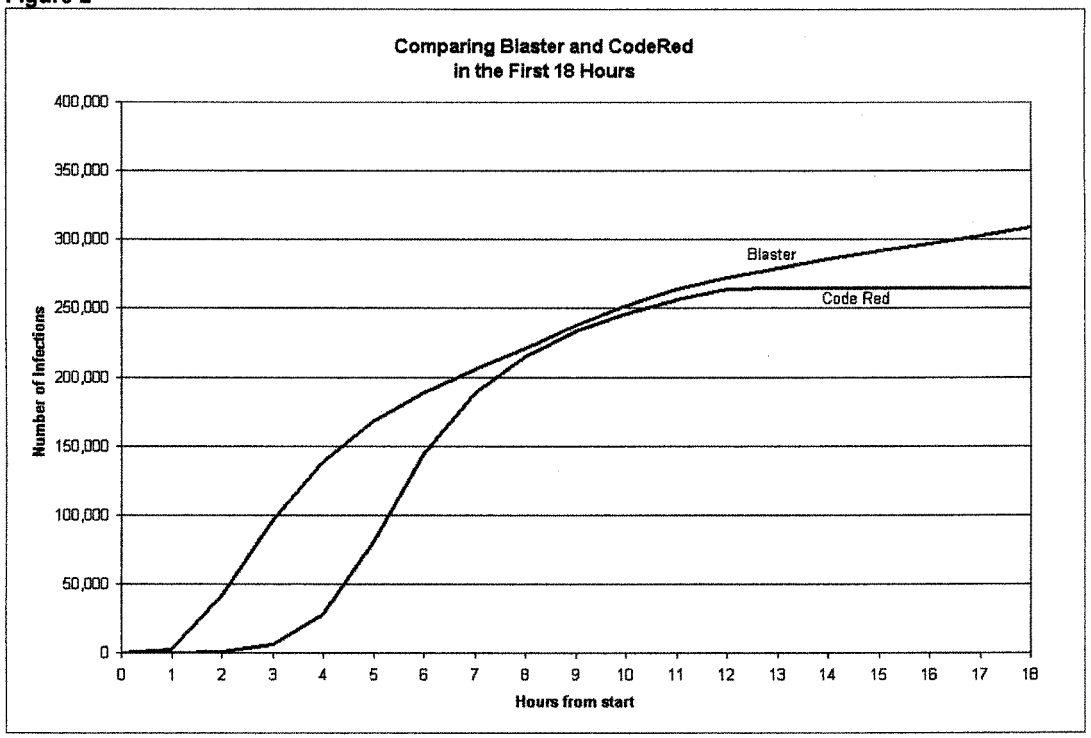

Comparing Blaster and CodeRed
in the First 18 Hours
Number of Infections
400,000
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
Hours from start
Blaster
Code Red

Figure 3

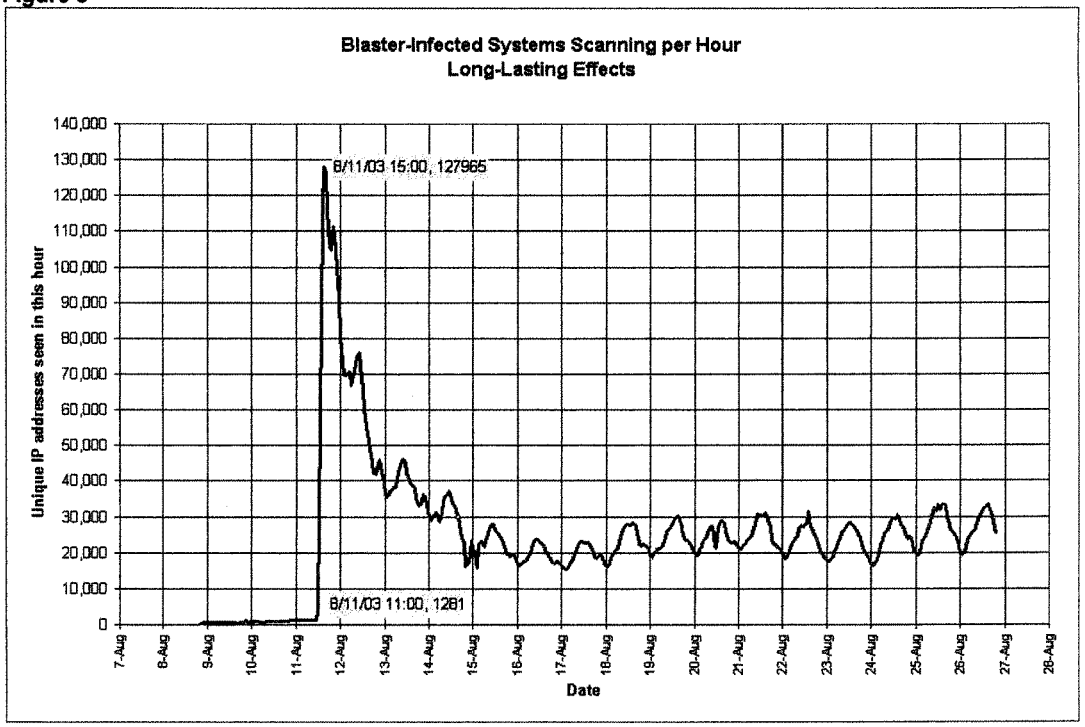
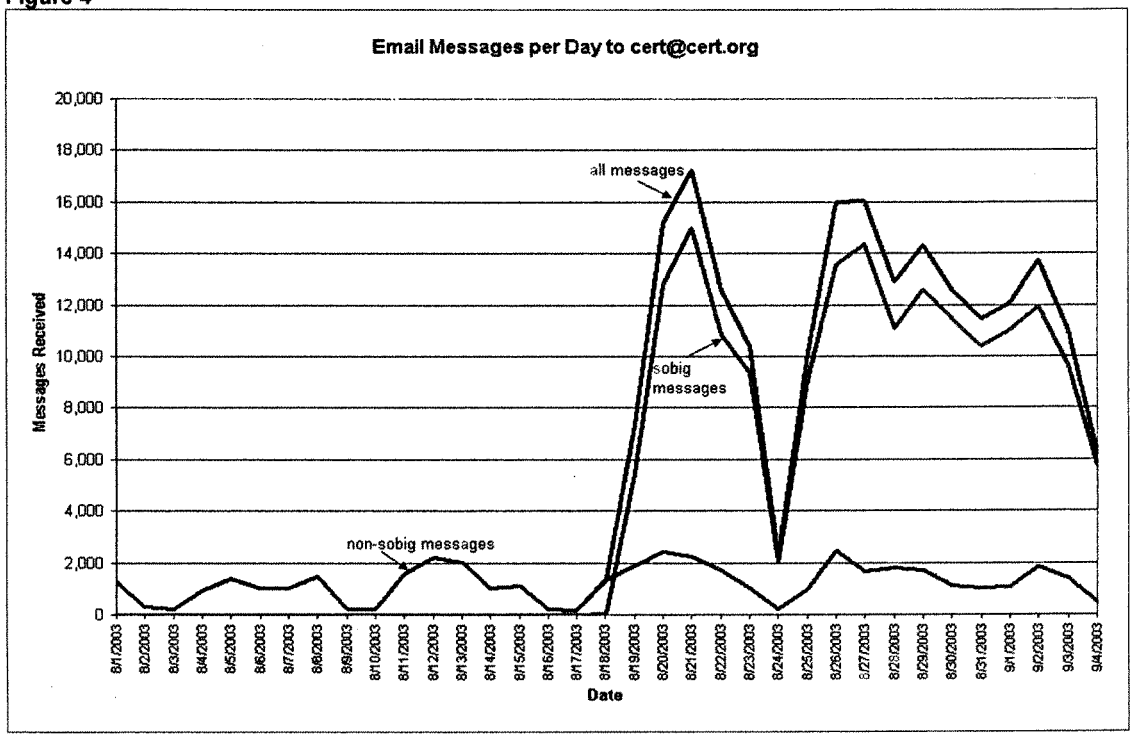

Blaster-Infected Systems Scanning per Hour
Long-Lasting Effects
Unique IP addresses seen in this hour
140,000
130,000
120,000
110,000
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
8/11/03 15:00, 127965
8/11/03 11:00, 1281
7-Aug
8-Aug
9-Aug
10-Aug
11-Aug
12-Aug
13-Aug
14-Aug
15-Aug
16-Aug
17-Aug
18-Aug
19-Aug
20-Aug
21-Aug
22-Aug
23-Aug
24-Aug
25-Aug
26-Aug
27-Aug
28-Aug
Date

Figure 4


Email Messages per Day to cert@cert.org
Messages Received
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
all messages
sobig messages
non-sobig messages
8/1/2003
8/2/2003
8/3/2003
8/4/2003
8/5/2003
8/6/2003
8/7/2003
8/8/2003
8/9/2003
8/10/2003
8/11/2003
8/12/2003
8/13/2003
8/14/2003
8/15/2003
8/16/2003
8/17/2003
8/18/2003
8/19/2003
8/20/2003
8/21/2003
8/22/2003
8/23/2003
8/24/2003
8/25/2003
8/26/2003
8/27/2003
8/28/2003
8/29/2003
8/30/2003
8/31/2003
9/1/2003
9/2/2003
9/3/2003
9/4/2003
Date

Mr. PUTNAM. Thank you very much. Our next witness is Mr. Hale. Lawrence Hale is the Director of the Department of Homeland Security Federal Computer Incident Response Center [FedCIRC]. He has been active in the information assurance community since 1996, when he served the chairman of the joint Chiefs of Staff as an information assurance action officer working on security interoperability issues. While at the Pentagon Mr. Hale was a member of the Joint Staff Information Operations Response Cell during a number of exercises and actual cyber events, which have helped to shape U.S. Government policy in dealing with computer security.

In January 1999, Mr. Hale became the first uniformed military officer assigned to the National Infrastructure Protection Center at the FBI Headquarters. While there he worked to improve the process of issuing warnings of cyber related events and served on the Y2K task force for the FBI. He retired from the U.S. Navy as a commander in May 2001, has a Master's Degree in national security and strategic studies from the Naval War College and a Master's in aeronautical science from Embry-Riddle.

Welcome to the subcommittee.

Mr. HALE. Good morning, Mr. Chairman and Ranking Member Clay. On behalf of the Federal Computer Incident Response Center of the Department of Homeland Security, thank you for this opportunity to appear before you to discuss how we can protect the Nation's computers. I am Lawrence Hale, Director of the FedCIRC, which is part of the Department of Homeland Security's Information Analysis and Infrastructure Protection Directorate. FedCIRC is the Federal-civilian government's trusted focal point for computer security incident reporting, providing assistance with incident prevention and response.

Within the Department of Homeland Security Information Analysis and Infrastructure Protection Directorate is the newly established National Cyber Security Division. The National Cyber Security Division is responsible for coordinating the implementation of the national strategy to secure cyberspace. Key functional areas within the division include Risk Threat and Vulnerability Identification and Reduction, Cyber Security Tracking, Analysis and Response Center and Outreach Awareness and Training. The FedCIRC is now a component of Cyber Security Tracking, Analysis and Response Center.

The National Cyber Security Division has combined the information gathering and analytical capabilities of the cyber watch elements of the National Infrastructure Protection Center and the FedCIRC and coordinates with the National Communication System. By doing this, the National Cyber Security Division not only has the added benefit of enhanced resources but the synergy of knowledge created from the unique resources from each of these watch elements.

The Federal Government's ability to limit the effects of the recent wave of worms and viruses on its networks demonstrate how these collaborative relationships work and how each participant's contributions help to assess and mitigate potential damage. FedCIRC has the goal of securing the Federal Government's cyberspace. FedCIRC, as noted in the e-Government Act of 2002, the

Federal Information Security Management Act, serves as the Federal information security incident center for the Federal civilian government. FedCIRC is the central government non-law enforcement focal point for coordination of response to attacks, promoting incident reporting and cross agency sharing of data about common vulnerabilities. As such, FedCIRC must compile and analyze information about incidents that threaten information security and inform Federal agencies about current and potential information security threats and vulnerabilities.

FedCIRC demonstrated the National Cyber Security Division's enhanced coordination role during the recent wave of worms and viruses. Working closely with the CERT Coordination Center and software providers, FedCIRC identified the potential impact of newly disclosed vulnerabilities and developed corrective actions in mitigating strategies. Federal civilian agencies were advised of the existence of these vulnerabilities and given actionable information on reducing their exposure to the threats before attack programs were released. Patches were developed, validated and disseminated to agencies. And working closely with OMB and the Federal CIO Council, agencies were instructed to take action to address the vulnerabilities and report their status. As a result of these measures, the Federal Government was better prepared to avoid damaging impact when the exploit codes that were released in the attack phase of these events occurred.

The National Cyber Security Division has a number of initiatives underway to aid in threat vulnerability reduction. As was mentioned, the majority of successful attacks on computer systems result from hackers exploiting the most widely known vulnerabilities in commercial software products. The problem is not that patches to fix these vulnerabilities don't exist, but that existing patches are not quickly and correctly applied. Agencies must have a plan on how patch management is integrated into their configuration management process. FedCIRC's patch authentication and dissemination capability [PADC], a Web enabled service that provides a trusted source of validated patches and notifications on new threat and vulnerabilities, is a first step.

FedCIRC's vision is to build from the ability of providing validated patches to developing a more enhanced IT configuration and vulnerability management program that will automate the process. By automating the process, agencies will no longer have the burden of having to manually apply patches which will enable them to have more time to focus on building a more robust configuration management program.

In closing, I would like to assure the committee that the National Cyber Security Division is committed to building on the success the FedCIRC has achieved in helping Federal civilian agencies protect their information systems from the most damaging effects of malicious code. National Cyber Security Division must now translate this success to a national scale. I look forward to continuing to work with OMB and the Congress to ensure that we are successful in this important endeavor.

[The prepared statement of Mr. Hale follows:]

Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate's
National Cyber Security Division
Testimony of Lawrence C. Hale,
Director, Federal Computer Incident Response Center
Before the
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

Good morning, Mr. Chairman and Members of the Committee. On behalf of the Federal Computer Incident Response Center of the Department of Homeland Security let me thank you for this opportunity to appear before you to discuss "How we can protect the Nation's Computer from threats". Let me introduce myself, I am Lawrence Hale, the director of the Federal Computer Incident Response Center (FedCIRC), which is part of the DHS, Information Analysis and Infrastructure Protection Directorate. FedCIRC is the Federal Civilian Government's trusted focal point for computer security incident reporting, providing assistance with incident prevention and response.

Background

> *The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace. Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector and the American people.*
>
> "The National Strategy to Secure Cyberspace, February 2003"

The Homeland Security Act of 2002, which established the Department of Homeland Security (DHS), was one of a number of important steps taken to improve our ability to protect the Nation's Critical Infrastructures. Within DHS, Information Analysis and Infrastructure Protection Directorate is the newly established National Cyber Security Division (NCSD). The NCSD is responsible for coordinating the implementation of the National Strategy to Secure Cyberspace. Key functional areas within the Division include Risk, Threat and Vulnerability Identification and Reduction; Cyber Security Tracking, Analysis and Response Center (CSTARC); and Outreach, Awareness, and Training. The FedCIRC is an important component of the CSTARC.

The NCSD has combined the information gathering and analytical capabilities of the Cyber Watch elements of the National Infrastructure Protection Center and the Federal Computer Incident Response Center, and coordinates with the National Communications System. By doing this the NCSD not only has the added benefit of enhanced resources, but the synergy of knowledge created from the unique resources from each of the watch elements. The Federal Government's ability to limit the effects of the recent wave of worms and viruses on its networks clearly demonstrates how these collaborative relationships work and how each participant's contributions help to assess and mitigate potential damage. The NCSD has made significant progress since its inception in June 2003 by playing a central role in coordinating national efforts to deal with cyber threats and vulnerabilities. Focusing exclusively on threats (worms, viruses, etc) would force us into a reactive posture, taking action only after threat information is received, processed, and analyzed. By focusing on addressing vulnerabilities, NCSD has been successful in reducing the impact of a number of recent cyber incidents.

The NCSD is working to develop the same type of collaborative relationship with Private Sector Information Sharing Analysis Centers, State and Local Government, Law Enforcement, Academia, and Private Industry.

FedCIRC has the goal of securing the Federal Government's Cyberspace. FedCIRC, as noted in the E-Government Act of 2002, serves as the Federal Information Security Incident Center for the Federal Civilian Government. FedCIRC is the central government non-law enforcement focal point for coordination of response to attacks, promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. As such, FedCIRC must compile and analyze information about incidents that threaten information security and inform Federal agencies about current and potential information security threats and vulnerabilities.

FedCIRC demonstrated NCSD's enhanced coordination role during the recent wave of worms and viruses. (e.g. Blaster, SoBig.F). Working closely with CERT-CC and software providers, FedCIRC identified the potential impact of newly disclosed

vulnerabilities and developed corrective actions and mitigating strategies. Federal Civilian agencies were advised of the existence of these vulnerabilities, and given actionable information on reducing their exposure to the threats before attack programs were released. Patches were developed, validated and disseminated to agencies. Working closely with OMB and the Federal CIO Council, agencies were instructed to take action to address the vulnerabilities, and report their status. As a result of these measures, the Federal government was better prepared to avoid damaging impact when the exploit codes were released and the attack phase of these events occurred.

The NCSD has a number of initiatives underway to aid in threat and vulnerability reduction:

Patch Management Program: The majority of successful attacks on computing systems result from hackers exploiting the most widely-known vulnerabilities in commercial software products. The problem is not that patches to fix these vulnerabilities don't exist, but that existing patches are not quickly and correctly applied. There are several factors that contribute to this. Agencies must have a plan on how patch management is integrated into their configuration management process(es). Agencies must maintain a current inventory of assets and prioritize their assets. (e.g. mission critical, network perimeter, servers, workstations, etc). Also, with an estimated 4000 vulnerabilities being discovered each year, it is virtually impossible for most agencies to install all of the patches that are released. Therefore an organization's patching process should define a method for deciding which patches get installed first and a method for deciding which systems get patched.

FedCIRC's Patch Authentication and Dissemination Capability (PADC), a web-enabled service that provides a trusted source of validated patches and notifications on new threat and vulnerabilities is a first step. FedCIRC's vision is to build from the ability of providing validated patches to developing a more enhanced IT Configuration and Vulnerability Management program that will automate the process. By automating the process agencies will no longer have the burden of having to manually apply Patches

which will enable them more time to focus on building a more robust configuration management program which is a key part of any security strategy used to protect our critical information systems.

Data Analysis Capability: In partnership with CERT/CC, FedCIRC is piloting a study to develop real time analytical tools that may help in identifying precursors or indicators of impending attacks.

One of NCSD's goals is to have this same level of enhanced response and information sharing with the Private Sector, State and Local Government and the general Public to ensure everyone is equally prepared in our fight to prevent cyber attacks against America's Critical Infrastructures. The Federal Government has a program in place to focus on Cyber Security. State and Local Government and Private Industry must do the same to be as effective.

In addition, NCSD in its outreach and awareness function has launched its cyber security awareness initiative that includes an effort to design and lead implementation of training and awareness efforts and campaigns that use a multi-level approach to educate industry, government, and the public on the importance of their roles in National cyber security. By this effort NCSD will work with OPM and NIST to help increase the number and quality of trained cyber security professionals in the federal workforce by its efforts to facilitate and improve Cyber Corps (the scholarship-for-service program for IT security.

In closing, I would like to assure the Committee that the National Cyber Security Division is committed to building on the success that FedCIRC has achieved in helping Federal Civilian Agencies protect their information Systems from the most damaging effects of malicious code. NCSD must now translate this success to a national scale. I look forward to continuing to work with OMB and the Congress to ensure that we are successful in this important endeavor.

Mr. PUTNAM. Thank you very much Mr. Hale. I would like to welcome our distinguished ranking member and vice chair of the subcommittee as well, and we will be taking their opening statements at the conclusion of the first panel's remarks as well.

Our next witness is Norman Lorentz. Mr. Lorentz joined the Office of Management and Budget in January 2002 as Chief Technology Officer, the Chief e-Government Architect for the Federal Government. Mr. Lorentz is responsible for identifying and developing support for investments in emerging technology opportunities that will improve the Government's technical information and business architectures.

Prior to joining the Federal Government, he was senior vice president and chief technology officer for the IT career solutions provider, Dice, Inc. In this capacity he directed the development of technology strategy and infrastructure. He was also the firm's chief quality officer and a member of the executive committee. He brings to OMB extensive experience in government.

From 1998 to 2000, he was senior vice president and chief technology officer for the U.S. Postal Service. In 1998, he receive the Board of Governors Award, the U.S. Postal Service's highest recognition, and this year was named as a Federal 100 winner as well as recognition by Info World magazine as 1 of the 25 most influential CTOs in the United States. And this is your last appearance before a congressional committee as a public servant with OMB, as you will be leaving that agency and moving back into the private sector. So we appreciate your service to the government and to this subcommittee, and you are recognized.

Mr. LORENTZ. Thank you, Mr. Chairman, and good morning, members of the committee. Thank you for inviting me to discuss this important topic of worm and virus defense. My testimony today will address how the Federal Government protects its IT systems from this pervasive threat.

By design, worms and viruses can cause substantial damage and prove disruptive to normal business operations. For this reason it is important for the Federal agencies to continuously and rapidly take proactive measures to lessen the number of successful attacks. The month of August proved to be an unusually busy time for malicious code activity, beginning with Blaster and then quickly spreading the SoBig.F worm. In general, the Federal Government withstood these attacks and the impact on citizen services was minimal.

Agencies have improved their protection against malicious code by installing patches, blocking executables at the firewall and using antivirus software with automatic updates. Agencies, however, did report modest impacts associated with both worms to date. Reports from Federal civilian agencies show approximately 1,000 computers affected by each exploit. This impact ranged from a slowdown in agency e-mail to temporary unavailability of agency systems. A number of laptops proved to be susceptible to the infection since configuration management was even on these portable devices.

The Federal Government's ability to thwart worms and viruses depends on a number of interlocking management, technical and

operational controls. It is critical that these controls continue to evolve to keep pace with this increasingly sophisticated threat.

First, how were vulnerabilities discovered? DHS's Federal Computer Incident Response Center [FedCIRC], closely coordinates with a number of industry as well as government partners. These partners include Carnegie Mellon CERT, law enforcement and the Intelligence Community. These organizations routinely communicate advanced notice to DHS regarding the discovery of software vulnerabilities in the development of malicious code.

Second, how are agencies notified about these vulnerabilities? OMB and the CIO Council have developed and deployed a process to rapidly identify and respond to cyber threats and critical vulnerabilities. CIOs are advised via conference call as well as followup e-mail of specific actions necessary to protect agency systems. Agencies must then report through FedCIRC to OMB on the implementation of those required countermeasures. This emergency notification and reporting process was instituted for the Microsoft RPC vulnerability in July and as a result the agencies were able to rapidly close vulnerabilities that otherwise might have been exploited by the Blaster worm. There are mechanisms that exist for protecting systems.

The National Institute of Standard and Technology [NIST], recommends that the agencies implement a patch management program, harden all hosts appropriately, deploy antivirus software and detect and block malicious code and configure the network perimeter to deny all traffic that is not necessary. As part of the statutory responsibility under FISMA, the National Institute of Standards and Technology will publish in September draft guidelines for incident handling. The guidelines will discuss how to establish and maintain an effective incident reporting and response program with an emphasis on incident detection, analysis, prioritization and containment. The guidelines will include recommendations for handling certain types of incidents and the distribution of denial of service attacks and malicious code infections.

Last, the problems presented by the patching systems. Patch management is an essential part of any agency's information security program and requires a significant investment in time and effort. Agencies must carefully follow predefined processes in order to successfully remediate system vulnerabilities across the enterprise. A number of agencies utilize automated tools to push the patches to the desktop. The automation of the patch management process is significantly easier when the agency maintains a standardized software configuration. At the present, 47 agencies subscribe to FedCIRC's PADC capability. This service validates and quickly distributes corrective patches for known vulnerabilities.

In closing, OMB is committed to a Federal Government with resilient information systems. Worms and viruses must not be able or allowed to significantly affect agency business processes. OMB will continue to work with the agencies, Congress and GAO to ensure that appropriate countermeasures are in place to reduce the impact of malicious code.

Thank you very much.

[The prepared statement of Mr. Lorentz follows:]

STATEMENT OF
NORMAN E. LORENTZ
ACTING ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS
U.S. HOUSE OF REPRESENTATIVES
September 10, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss the important topic of worm and virus defense. My testimony today will address how the federal government protects its IT systems from this pervasive threat.

By design, worms and viruses can cause substantial damage and prove disruptive to normal business operations. For this reason, it is important that federal agencies continually and rapidly take proactive measures to lessen the number of successful attacks.

The month of August proved unusually busy for malicious code activity, beginning with the Blaster and then the quickly spreading Sobig.f worm. I am pleased to state that, in general, the federal government withstood these attacks and impact on citizen services was minimal. Agencies have improved their protection against malicious code by installing patches, blocking executables at the firewall, and using anti-virus software with automatic updates.

Agencies did, however, report modest impacts associated with the Blaster and Sobig.f worms. To date, reports from federal civilian agencies show approximately 1000 computers affected by each exploit. This impact ranged from a slowdown in agency e-mail to the temporary unavailability of internal agency systems. A number of laptops proved to be susceptible to infection since configuration management was uneven on these portable devices.

The federal government's ability to thwart worms and viruses depends on a number of interlocking management, technical and operational controls. It is critical that these controls continue to evolve to keep pace with the increasingly sophisticated threat.

How vulnerabilities are discovered

DHS' Federal Computer Incident Response Center (FedCIRC) maintains a strong relationship with a number of industry as well as government partners. These partners include commercial software vendors, Carnegie Mellon University's Computer Emergency Response Team, law enforcement, the intelligence community, and agency incident response teams. These organizations routinely communicate advance notice to DHS regarding the discovery of software vulnerabilities and the development of malicious code designed to exploit these weaknesses.

How Agencies Are Notified About Potential Vulnerabilities

The Federal Computer Incident Response Center within the Department of Homeland Security is the Federal government's focal point for coordinating response to attacks (non-law enforcement), promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. Through this role, FedCIRC notifies Federal agencies about current and potential information security threats and vulnerabilities.

OMB and the CIO Council have developed and deployed a process to rapidly counteract identified threats and vulnerabilities. CIOs are advised via conference call, as well as follow up e-mail, of specific actions needed to protect agency systems. This information is also transmitted to agency incident response centers. Agencies must then report through FedCIRC to OMB on the implementation of the required countermeasures. In particular, we track data concerning the percentage of systems patched and the time needed to complete mitigation efforts. This emergency notification and reporting process was instituted for the Microsoft RPC vulnerability in July and as a result, agencies were able to rapidly close vulnerabilities that otherwise might have been exploited by the Blaster worm.

In analyzing agency responses to earlier OMB data calls, it became apparent that the amount of time needed to implement required fixes was too long and varied widely from agency to agency. OMB asked the CIO Council's Security Liaison to sponsor a meeting so that agencies could share best practices. The meeting ensured that agency CIOs understood the urgency associated with implementing patches and were able to leverage the capabilities and ideas of other agencies.

OMB continued to discuss the Blaster and Sobig.f worms with key agency representatives. Sector specific agencies such as Treasury, Energy and Transportation provided updates on the worm's impact to the private sector and agencies participated in a discussion of lessons learned and next steps. OMB intends to hold after action meetings with federal agencies following all major cyber events so that we may continue to refine this process.

The Mechanisms that Exist for Protecting Systems

The National Institute of Standards and Technology (NIST) provides guidelines to federal agencies on securing networks, systems, and applications. NIST recommends that agencies implement a patch management program, harden all hosts appropriately, deploy antivirus software to detect and block malicious code, and configure the network perimeter to deny all traffic that is not necessary. Additional recommendations include user awareness briefings as well as training for technical staff on security standards, procedures, and sound security practices. Per longstanding OMB policy, Federal agencies are directed to follow NIST guidelines.

NIST has produced a number of recent publications that address agency security practices. These publications include: Securing the Public Web Server, Electronic Mail Security, IT Contingency Planning, Security Metrics, System Administrator Guidance for Securing Win

2000, Wireless Security, Security Patch Management, Intrusion Detection Systems, Firewall Security, and Risk Management.

As part of its statutory responsibilities under the Federal Information Security Management Act, the National Institute of Standards and Technology will publish in September draft guidelines for incident handling. The guidelines will discuss how to establish and maintain an effective incident response program with an emphasis on incident detection, analysis, prioritization and containment. The guidelines will include recommendations for handling certain types of incidents, such as distributed denial of service attacks and malicious code infections. In addition, the guidelines will include a set of sample incident scenarios that can be used to perform incident response team exercises. The guidelines will be written so they can be followed regardless of hardware platform, operating system, protocol, or application.

Another critical mechanism used to enforce protection of Federal systems is the Federal Information Security Management Act (FISMA). Under FISMA, Federal agencies are required to periodically test and evaluate the effectiveness of their information security policies, procedures and practices. The results of both the agency self assessments and the IG assessments are provided to OMB each September. OMB submits a summary report to Congress based on the agency and IG reports.

The Problems Presented by Patching Systems

Patch management is an essential part of an agency's information security program and requires a substantial investment of time and effort. Agencies must carefully follow predefined processes in order to successfully remediate system vulnerabilities across the enterprise.

These processes include: identifying all affected systems and related software revision levels, fully testing the patch before it is placed into a production environment, and prioritizing installation of the patch based on the criticality of the system. Alternative solutions such as judicious use of port blocking must be implemented if the patch cannot be installed.

A number of agencies utilize automated tools to push patches to the desktop. The automation of the patch management process is significantly easier if the agency maintains standardized software configurations.

At the present time, forty-seven agencies subscribe to FedCIRC's Patch Authentication and Dissemination Capability. This service validates and quickly distributes corrective patches for known vulnerabilities.

Federal Enterprise Architecture

Improving the federal government's response to malicious code requires that we focus on enterprise architecture and the standardized deployment of security technologies. As new technologies become available and cost effective, they must be incorporated into the IT infrastructure where they can monitor common precursors and indications of attack.

Conclusion

The Federal government is the world's largest consumer of IT systems. Because of its vast inventory and the vulnerabilities inherent in commercial software, the Federal government will, for the immediate future, continue to be impacted by the proliferation of worms and viruses. Through our oversight of agency security policies and practices, OMB will continue to work with agencies to ensure that the risks associated with malicious code are appropriately mitigated.

In addition, the federal government will continue to rely on federal, state and local law enforcement to investigate and prosecute developers of malicious code. Agencies must continue to report computer incidents and assist law enforcement investigations to the greatest extent possible. Strong cooperation was displayed between the FedCIRC community and the Secret Service, FBI and other law enforcement officials during the recent Blaster and Sobig.F incidents.

In closing, OMB is committed to a federal government with resilient information systems. Worms and viruses must not be allowed to significantly affect agency business processes. OMB will continue to work with agencies and the Congress to ensure that appropriate countermeasures are in place to reduce the impact of malicious code.

Mr. PUTNAM. Thank you very much.

Our next witness is John Malcolm. Mr. Malcolm is currently a Deputy Assistant Attorney General in the Criminal Division at the Department of Justice, where his duties include overseeing the Computer Crime and Intellectual Property Section, the Child Exploitation and Obscenity Section, the Domestic Security Section and the Office of Special Investigations. Pretty robust portfolio.

An honors graduate of Columbia College and Harvard Law School, Mr. Malcolm served as a law clerk to judges on both the U.S. District Court for the Northern District of Georgia and the 11th Circuit Court of Appeals. For 7 years Mr. Malcolm was an Assistant U.S. Attorney in Atlanta, GA, where he was assigned to the Fraud and Public Corruption Section. Mr. Malcolm also served as an Associate Independent Counsel in Washington, DC, investigating fraud and abuse at HUD.

Prior to rejoining the Department of Justice in August 2001, Mr. Malcolm was a partner at the Atlanta law firm of Malcolm & Schroeder, LLP.

Thank you for sharing your time with us and look forward to your testimony, and you are recognized for 5 minutes.

Mr. MALCOLM. Thank you for giving me this opportunity to testify about the Department of Justice's ongoing efforts to protect our Nation's critical infrastructure from the growing problem of Internet borne worms and viruses. Although computer viruses have been around for a long time, the ubiquity of Internet access and household ownership of computers in the United States have manifestly increased the deleterious impact of viruses and worms on our critical infrastructure and on our daily lives.

It seems that nearly every week we learn the name of a new computer virus or worm that exploits flaws in commonly used software and quickly spreads through the Internet. Some of these, like the Blaster worm, make the front pages of newspapers. These viruses and worms are merely the tip of the iceberg. They are just the ones that receive the most public attention. Hundreds more are released every year, posing a daily challenge to those who are responsible for protecting networks and investigating network attacks.

The effect of these viruses and worms should not be underestimated. For example, in the United States, the Slammer worm shut down the automatic teller machine system and caused significant transportation delays when electronic ticketing used for airline travel was affected. The Blaster worm and its variants have affected hundreds of thousands of computers. Moreover, since the Internet is seamless and borderless, the harmful impact of worms and viruses is not limited to our country but affects countries across the world. Clones or new variants of malicious codes continue to crop up, raising concerns that more damaging variants are right around the corner. In many cases succeeding generations of viruses and worms will build on its capabilities adding additional harmful pay loads.

The worldwide damage to computers and data as well as the productive time lost as the result of worms and viruses is measured in the millions and by some estimates in the billions of dollars. This damage has an undeniable adverse effect on important sectors

of our economy and potentially undercuts the security of our Nation's critical infrastructure.

The Department of justice has devoted significant resources to investigating and prosecuting persons who release malicious codes on the Internet. These efforts have met with some success. It bears mentioning, however, that tracking the sources of worms and viruses on the Internet is difficult and presents unique challenges to investigators because of the speed with which programs are spread and fundamental characteristics of computer networks, particularly in peer to peer network applications. It is difficult to determine precisely where an outbreak begins since simultaneous file transfers can occur in computers literally throughout the world.

Although tracking the sources of computer worms and viruses is difficult, the Department of Justice is fully committed to effectively investigating such attacks. The Criminal Division's Computer Crime and Intellectual Property Section helps coordinate investigations of computer crimes of all sorts, including virus and worm attacks. These prosecutors in turn train and work with computer hacking and intellectual property units and computer and telecommunications coordinators in each of the 93 U.S. Attorneys offices across the country. Together this network of prosecutors working with law enforcement agents from the Secret Service and the FBI and using important tools provided by the Patriot Act provide an integrated approach to addressing computer crime. Because the perpetrators of offenses may live in other countries, the investigations involve an international component that draws upon the Department's contacts with law enforcement counterparts abroad. Indeed, international cooperation is a foundation of the Department strategy for combating cyber crimes, including worms and viruses. Our efforts are rewarded whenever evidence is obtained from foreign countries that further domestic investigations or when we are able to furnish similar assistance to other countries.

In addition to international outreach, Department attorneys and agencies regularly meet with industry, trade groups and State and local law enforcement officials in order to improve communication. The Department of Justice pursues a message of a culture of security where both individual users and corporations view computer security as a key component for successful computing experience. Experience sadly teaches us that much of the damage to our computer networks is caused by teenagers and young adults armed with free hacking tools, plenty of time and too little moral teaching about how to use computers and how not to use computers. Therefore, the Department has also pursued educational programs directed to youth, their teachers and parents. We describe the program as cyber ethics. In fact, CCIPS, in an article authored by the section chief, has published an article dealing with cyber ethics in the current issue of Newsweek.

The Department of Justice continues to make progress in its battle against computer crime and intellectual property theft. Recognizing the challenges ahead, we look forward to continued success in our efforts.

Mr. Chairman, that concludes my prepared statement. I look forward to getting your questions.

[The prepared statement of Mr. Malcolm follows:]

Department of Justice

STATEMENT

OF

JOHN G. MALCOLM
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS
COMMITTEE ON GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

COMPUTER VIRUS PROTECTION

PRESENTED ON

SEPTEMBER 10, 2003

STATEMENT OF

JOHN G. MALCOLM

DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U. S. DEPARTMENT OF JUSTICE

BEFORE THE HOUSE COMMITTEE ON
GOVERNMENT REFORM, SUBCOMMITTEE
ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS
AND THE CENSUS

SEPTEMBER 10, 2003

Mr. Chairman and Members of the Subcommittee, thank you for this opportunity to testify about the Department of Justice's continuing effort to protect our nation's critical infrastructure from the growing problem of destructive Internet-borne computer "viruses" and "worms." This issue is of critical importance to our country's computer networks and its economy, and I commend the Subcommittee for holding this hearing.

In my testimony today, I would like briefly to outline the nature of the threat from malicious computer code, commonly known as viruses and worms, the Congressional response to this problem, and the Department of Justice's current efforts both to combat the effects of computer viruses and worms and to arrest and prosecute the perpetrators of these crimes.

The nature of the threat

Although computer viruses have been around for a long time, the ubiquity of Internet access and household ownership of computers in the United States have manifestly increased the deleterious impact of viruses and worms on our critical infrastructure and on our daily lives. Similarly, we have seen a significant increase in network intrusions; denial of service attacks and system damage; extortion threats involving computer systems and networks; and other criminal conduct that demonstrate that, unfortunately, criminals have taken to the Internet as eagerly as law-abiding citizens. It seems that nearly every week, we learn the name of a new computer virus or worm that exploits flaws in commonly used software and quickly spreads through the Internet. As the public relies increasingly on high-speed electronic communications, email attachments, and peer-to-peer file sharing programs, viruses and worms will continue to spread.

First, let me offer a brief explanation of what computer viruses and worms are, and how they spread from network to network. A virus is a small computer program that attaches itself to a legitimate program or file on a target machine, which is usually described as a 'host' for the virus. The virus is then copied from machine-to-machine when that infected program or file is shared. A worm is also a computer program, but unlike a virus, a worm does not need a host file. A computer worm usually has the ability to copy and spread itself to other computers on other networks. As a result, computer worms generally spread faster than computer viruses, and some have spread around the world in a matter of hours or, in some cases, minutes.

The behavior of malicious code, whether a virus or a worm, is determined by the 'payload' of the program, which is the embedded instructions that tell the virus or worm what to do once it arrives on a system. The worm or virus may be relatively benign, or it may delete essential system files, change critical data or otherwise disrupt the normal functioning of a computer system. Worms and viruses, which spread rapidly and use up available bandwidth, routinely clog networks. When this occurs, essential e-commerce and other legitimate network traffic are prevented from following their normal course.

Each year, the incidents of world-wide epidemics of computer viruses and worms increase. In recent memory, we have seen the ILOVEYOU virus in 2000; the Code Red worm and the NIMDA virus in 2001; the Klez worm in 2002; and so far in 2003, the Slammer worm; the MiMail worm; the MSBlaster worm; and SoBig.F. These viruses and worms are merely the tip of the iceberg – they are just the ones that have received the most public attention. Hundreds more are released every year, posing a daily challenge to those responsible for protecting networks and investigating network attacks.

The effect of these viruses and worms should not be underestimated. For example, in the United States, the Slammer worm shut down the automatic teller machine system and caused significant transportation delays when electronic ticketing used for airline travel was affected.

The "LovSan" or "Blaster" worm and its variants have affected hundreds of thousands of computers. The original variant of the worm shut down Maryland's Motor Vehicle Agency and other entities. The MiMail worm affected computers nationwide, including computers at U.S. government agencies, by cleverly masquerading as a message from a company's or agency's system administrator. Previous outbreaks, such as the NIMDA virus and Code Red worm, have been blamed for significant losses to businesses across the country, as servers became infected and were rendered unable to perform tasks related to banking and electronic commerce.

Since the Internet is seamless and borderless, the harmful impact of worms and viruses is not limited to our country. At the international level, news services reported that the Slammer worm was responsible for severely hampering an Asian stock market for the better part of a day, and disrupted a Canadian political party's vote for its national leader. The Blaster worm knocked nearly 20,000 Swedish Internet users offline, and harmed hundreds of thousands of home and business users around the world.

Clones, or new varieties of malicious code, continue to crop up, raising concerns that more damaging variants are right around the corner. These varieties of existing viruses and worms are developed in an underground community of creators who share emerging vulnerabilities, develop exploits directed to those vulnerabilities, and refine the malicious code. Although such "copycat" creators of viruses and worms do not always develop the original code,

their activity is no less dangerous. In many cases, succeeding generations of a virus or worm will build on its capabilities, adding additional harmful payloads or enhancing the capability of the virus to spread. For instance, the teenager in Minnesota who was just charged with creating a copycat version of the Blaster worm is alleged to have modified the original Blaster virus and caused significant additional damage.

The worldwide damage to computers and data, as well as the productive time lost, as a result of viruses and worms measures in the millions, and by some estimates, in the billions of dollars. This damage has an undeniable, adverse effect on important sectors of our economy and potentially undercuts the security of the nation's critical infrastructure. Resources are lost due to the inability of businesses and employees to use the Internet, unexpected shutdowns of computer systems in homes and offices, and time spent repairing damaged and infected systems.

Applicable legislation

Causing damage to our nation's computer networks is a federal crime, one that carries substantial penalties for those convicted. The principal federal law enforcement weapon in the battle against computer viruses and worms is the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Specifically, subsection (a)(5) makes it a federal crime to knowingly cause the transmission of a program, information, code or command, and as a result of such conduct, intentionally cause damage, without authorization, to a protected computer if the conduct caused

(or causes) --

1. a loss of at least $5,000 to one or more persons during any one-year period;
2. the impairment or modification of the medical diagnosis or treatment of one or more persons;
3. physical injury to any person;
4. a threat to public health or safety; or
5. damage to a government computer system used for the administration of justice, national defense, or national security.

The scope of the prohibition is broad and recognizes that the risk of damage from a computer virus or worm is significant, and could impact critical national or personal interests. Penalties for felony violations of the law range from 5 years in prison to 20 years for subsequent offenders, to life imprisonment for those whose knowing or reckless violations result in someone's death. We expect new sentencing guidelines to go into effect shortly that more closely correlate the sentencing structure for these crimes with their serious nature. These guidelines will provide for significant sentencing enhancements for abuse of specific skills employed in sophisticated means to facilitate the crime; the number of victims; the risk of serious bodily injury or death; and the degree of damage caused by the criminal conduct.

The Department of Justice's Response to the Problem

The Department of Justice has devoted significant resources to investigating and prosecuting persons who release malicious code on the Internet. Those efforts have met with some success. For example, in 2001, David Smith of New Jersey was sentenced to 20 months in federal prison after pleading guilty to unleashing the "Melissa" computer virus that infected untold numbers of computer networks and caused millions of dollars in damage. It bears mentioning, however, that tracking the source of viruses and worms on the Internet is difficult and presents unique challenges to investigators because of the speed with which such programs spread, and the fundamental characteristics of computer networks. Particularly in "peer-to-peer" networking applications, it is difficult to determine precisely where an outbreak began, since simultaneous file transfers can occur to other computers in far corners of the world.

Although tracking the sources of viruses and worms is difficult, the Department of Justice is committed to fully and effectively investigating such attacks. The USA PATRIOT Act has significantly enhanced the Department's ability to respond in computer crime investigations. Specifically, the reaffirmed applicability of pen register/trap and trace orders to Internet non-content traffic and the single-order pen register/trap authority afforded to the Department under this Act adds important procedural tools to investigations of computer crime.

The Criminal Division's Computer Crime and Intellectual Property Section, which I supervise, maintains a number of prosecutors who help coordinate investigations into computer crimes of all sorts, including virus and worm attacks. They, in turn, work with Computer Hacking and Intellectual Property (CHIPS) units and Computer and Telecommunications Coordinators (CTCs) in each of the 93 U.S. Attorneys' offices. Together, this network of prosecutors, working with law enforcement agencies such as the Secret Service and the FBI, provide an integrated approach to addressing computer crime.

The recent arrest by federal authorities in Minnesota of an 18-year old suspected of releasing a variant of the Blaster worm illustrates that this conduct is treated seriously and consonant with the harm that it causes. This is not the end of the Blaster worm investigation, because the original author of the worm has not yet been apprehended, and new variants of the worm appear almost daily. We will do everything we can to bring the perpetrator of the Blaster worm and copycat offenders to justice.

Because the perpetrators of these offenses may live in other countries, these investigations frequently have an international component that draws upon the Department's contacts with law enforcement counterparts abroad. Indeed, international cooperation is a foundation of the Department of Justice's strategy for combating cybercrime including viruses and worms. Department personnel, including attorneys and FBI agents, have been instrumental

in training legislators and law enforcement in foreign countries on drafting cybercrime laws and developing investigative techniques.

We worked with international partners to negotiate the Council of Europe Convention on Cybercrime, which requires parties to criminalize the use of viruses and worms to intentionally damage computers and networks. The Convention requires countries that join the Convention to have minimum procedural tools to investigate such attacks, and to facilitate international cooperation in investigating such attacks. These efforts are rewarded when evidence is obtained from foreign countries that further domestic investigations, or when we are able to furnish similar assistance to other countries.

In addition to international outreach, Department attorneys and agents regularly meet with industry, trade groups and state and local law enforcement to improve communication with federal law enforcement. The Department of Justice pursues the message of a 'culture of security' where both individual users and corporations view computer security as a key component of a successful computing experience. Preventing computer virus and worm epidemics by keeping operating system software updated and by practicing 'safe computing' will always be the first line of defense against malicious code.

The Department has also pursued educational programs directed to youth that we describe as 'cyberethics." This program delivers the message to young people that certain moral responsibilities attach to skill and knowledge about computers. We understand that some of our brightest students are attracted to the world of computing and the intellectual rigor of that course of study. However, there is a bright line between responsible intellectual inquiry and criminal conduct that hurts people and damages property.

The Department of Justice continues to make progress in the battle against computer crime and intellectual property theft. Recognizing the challenges ahead, we look forward to continued success in our efforts.

Conclusion

Mr. Chairman, I want to thank you again for this opportunity to testify about the problem of computer viruses and worms and the Department of Justice's efforts to protect critical infrastructure. Government agencies, industry, and individual citizens alike are threatened by this abuse of computing power. The Department of Justice is actively pursuing the perpetrators of these crimes and is dedicated to ensuring that they know that there are serious consequences for their actions.

Mr. Chairman, that concludes my prepared statement. I would be pleased to answer any questions that you may have at this time.

Mr. PUTNAM. Thank you very much and thank all of you for your adherence to our time restrictions. At this time I will introduce the ranking member of the subcommittee, the distinguished gentleman from Missouri, Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman, especially for calling this hearing and my thanks to the witnesses who have taken the time to be with us today and share their expertise.

Computer bugs like worms and viruses are one more example of the complexity of the world we live in. On the other hand, they are one more example of the frailty of human beings and the difficulty of legislating appropriate behavior. Many worms and viruses we have seen are nothing more than exuberance of youth experimenting with newly found freedoms and skill. As has always been the case, the pranks of youth can have consequences well beyond their capability to understand those consequences.

Last week, the FBI arrested a Minnesota high school senior and charged him with intentionally causing and attempting to cause damage to computers protected under Federal law. He faces a $250,000 fine and 10 years in prison. This young man was so naive that he built into his computer bug a direct link to his own computer. Catching him was not difficult. However, the damage done was real. The worm attack he participated in forced shutdowns of computer systems at the Federal Reserve Bank of Atlanta, the Maryland Motor Vehicle Administration, the Minnesota Department of Transportation and part of 3M facilities, including a plant in Hutchinson.

Unfortunately, most hackers are not as naive as this Minnesota teenager nor as benign. One of the earliest publicly documented cases of hacking was in 1988 at the Lawrence Berkley Lab. Cliff Stone, an astronomer turned systems manager at Lawrence Berkley Lab, was alerted to the presence of an unauthorized user in the inner system by a 75-cent accounting error. His investigations eventually uncovered a spy ring that was breaking into government computers stealing sensitive military information.

We are faced with developing public policy that recognizes both the exuberance of youth and the real threat to our government and corporations by those who seek to do us harm. One element of that public policy must be a renewed attention to preventing these attacks.

Mr. Chairman, I will not go through this entire statement, but I think you have indicated that you are working on legislation that would encourage corporate America to do a better job of securing their computers, and I look forward to working with you on that legislation.

The problems faced by corporations are much like those facing the Federal Government and we should work together to solve those problems, and I will submit the entirety of my statement in the record. Thank you.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

**STATEMENT OF THE HONORABLE WM. LACY CLAY
AT THE HEARING ON
FIGHTING THE PLAGUE OF WORMS AND VIRUSES**

SEPTEMBER 10, 2003

Thank you Mr. Chairman for calling this hearing, and my thanks to the witnesses who have taken the time to be with us today and share their expertise.

Computer bugs like worms and viruses are on more example of the complexity of the world we live in. On the other hand, they are one more example of the frailty of human beings and the difficulty of legislating appropriate behavior.

Many of worms and viruses we have seen are nothing more than the exuberance of youth experimenting with newly found freedom and skills. As has always been the case, the pranks of youth can have consequences well beyond their capability to understand those consequences.

Last week, the FBI arrested a Minnesota high school senior and charged him with intentionally causing and attempting to cause damage to computers protected under federal law. He faces a $250,000 fine and up to 10 years in prison. This young man was so naive that he built into his computer bug a direct link back to his own computer. Catching him was not difficult. However, the damage done was real. The worm attack he participated in forced shutdowns of computer systems at the Federal Reserve Bank of Atlanta, the Maryland Motor Vehicle

Administration, the Minnesota Department of Transportation and part of 3M facilities, including a plant in Hutchinson.

Unfortunately, most hackers are neither as naive as this Minnesota teenager nor as benign. One of the earliest publicly documented cases of hacking was in 1988 at the Lawrence Berkeley Lab. Cliff Stoll, an astronomer turned systems manager at Lawrence Berkeley Lab, was alerted to the presence of an unauthorized user on his system by a 75-cent accounting error. His investigations eventually uncovered a spy ring that was breaking into government computers stealing sensitive military information.

We are faced with developing public policy that recognizes both the exuberance of youth, and the real threat to our government and corporations by those who seek to do us harm. One element of that public policy must be a renewed attention to preventing these attacks.

Earlier this year, several corporations were forced to shut down operations by a worm that took advantage of a known vulnerability in the Microsoft server software. Those who had installed the patch were unaffected. Those that had not were in big trouble.

For the federal government, there are two critical actions needed to solve this problem. First, we need sustained management attention to the day-to-day routine activities of computer security. Patch management is, perhaps, one of the least glamorous jobs in computer security. However, it is one of the most critical tasks. When something like the Slammer virus

from last January hits, government managers should reward those individuals who did their job and protected the agency systems. Second, the government needs to work with industry to assure that software with fewer holes is delivered, and that those holes that do exist are fixed as quickly as possible.

Let me take a few minutes to elaborate on this idea. The government has a large market presence in computer software. Recently, OMB has suggested that the government use that leverage to lower the cost of software. I believe a better use of that leverage would be to assure safer software.

Today, the price competition in the software market, has pushed profit margins to the point where investing in safer software may well be a life and death decision for a small company. The government, however, can use its purchasing power to encourage manufacturers to put on the market a more secure product. If a system manager can choose between a product that has been extensively tested for weaknesses and one that has not, in most cases the manager will choose the safer software, even if it costs more.

The second market innovation the government can promote is an ongoing relationship between the vendor and the customer. We see that today in the home market for computer security. Vendors of virus software offer services where the software is updated regularly for protection against new viruses. There is no reason that a similar relation cannot be forged between government purchases and all computer software. We need to encourage software vendors to be in the business of continually improving software security without forcing the user to purchase

and install a new version of the software. We also must create a market where security is profitable for software companies.

Our subcommittee chairman has indicated that he is working on legislation that would encourage corporate America to do a better job of securing their computers. I look forward to working with him on that legislation. The problems faced by corporations are much like those facing the federal government. We should work together to solve those problems.

Mr. PUTNAM. Thank you, Mr. Clay, and without objection your entire statement will be included in the record. And at this time I recognize the distinguished vice chair of the subcommittee, the former Secretary of State of the great State of Michigan, Ms. Miller.

Mrs. MILLER. Thank you, Mr. Chairman, and I apologize for being late this morning. I had an opportunity to speak on the floor about the second anniversary of the horrific attacks on our Nation. I certainly appreciate you holding the hearing today and with the recent computer virus attacks on our Nation's information infrastructure the importance of this hearing is undeniable, timely and certainly appropriate. And with three panels testifying, I will be very brief in my opening statement.

The focus of today's hearing is to examine what steps are being taken to protect the information infrastructure, both the public and the private levels, from the spread of viruses. And we in the Federal Government certainly have the responsibility of protecting our citizens and ensuring that the infrastructure individuals and businesses rely on is secure. In addition, the government must protect its own systems in order to function efficiently and effectively and this dual responsibility makes the task facing the Federal Government particularly challenging.

In April of this year testimony was submitted by Robert Dacey of the GAO to the subcommittee citing a November 2002 cyber attack that affected both private and government networks and caused $900,000 in damage to computers. This is obviously a significant figure. And if a large scale cyber attack were implemented not only would the damage caused to computers be considerable but the additional financial loss and damage to the physical infrastructure could seriously affect the operations of our Nation.

And actually we in the House of Representatives have firsthand knowledge of how potentially devastating these viruses can be. The recent Blaster and the SoBig virus attacks of just a few weeks ago nearly crippled the House e-mail network by overloading service with a complex array of erroneous messages. Fortunately, the combined efforts of the House Information Resources and the systems administrators and the Members' offices limited the extent of damage that the virus creators had likely hoped for.

In fact, these attacks likely inhibited our Nation's ability to adequately respond to the vast power outage experienced by the eastern half of our Nation. I certainly shudder at the thought of what could happen to everyday businesses if a successful virus or worm crippled our Nation's power grids or financial networks, the Internet, government networks or any other infrastructure that we rely so heavily on.

Viruses are a new weapon of attack for those who wish to do harm to this great Nation. The creators of these weapons are terrorists, quite frankly, cyber terrorists who want to disrupt our way of life and to cause considerable harm to our economy and infrastructure. And as with the terrorists that we are fighting with conventional means, these cyber terrorists are using the freedoms that we hold dear against us. They can unleash an attack on our soil from anywhere in the world, and we must be prepared.

Mr. Chairman, thank you for holding this important hearing. Certainly protecting our Nation's information infrastructure must be a top priority of the Congress. Thank you.

Mr. PUTNAM. Thank you very much, Mrs. Miller. We will get to the questions.

Mr. Hale, what percentage of the Federal Government had already downloaded the patch for Blaster prior to its release?

Mr. HALE. Mr. Chairman, I don't have the exact figure with me. It is safe to say in the approximately 4 weeks between the time the vulnerability was announced by Microsoft and the advisories from FedCIRC were issued the vast majority of agencies had downloaded the patches, and I will if given the opportunity try to provide you a more measured answer in writing.

Mr. PUTNAM. What percentage of the Federal Government subscribes to FedCIRC's program?

Mr. HALE. All Federal agencies receive advisories from FedCIRC, the PADC program in specific; 47 Federal agencies are subscribing to PADC. But PADC is just one part of an agency's patch management strategy. And many agencies have other methods of getting their patches, testing them and applying them. The information the advisories provided by FedCIRC go to all agencies.

Mr. PUTNAM. So then, Mr. Lorentz, how many different options are utilized by the various agencies to handle patch management? Sounds like some contract with the private sector. Some do it internally. Some subscribe to PADC. So we've got a lot of different patches to doing that.

Mr. LORENTZ. There are different approaches. We do not dictate which method that they use. As part of our FISMA oversight, we do require them to have specific plans, risk mitigation, patch management. We are soon to get the annual FISMA reports on September 22nd on that. But the important issue here, as you can tell from the testimony of everyone here, is that the only way we're protected is if all the dots are connected, the configuration management, the patch management, the management oversight to make sure those processes are implemented as appropriate, the adherence to the information provided by FedCIRC. So there can be variation in the tools, but there cannot be variation in the expected outcome or how those dots are connected in order to mitigate the problem.

Mr. PUTNAM. Mr. Malcolm, you mentioned a number of issues about the law enforcement approach to computer security. How many people have actually served time in jail for releasing malicious code, worms and viruses?

Mr. MALCOLM. There are a couple of instances that immediately come to mind. One was Mafia Boy in the United States who was actually prosecuted in Canada. He ended up getting a sentence. There was David Smith, who was arrested and charged and successfully prosecuted for releasing the Melissa virus. I believe he got a 20-month term of imprisonment.

I would add in that regard the U.S. Sentencing Commission is reevaluating the guidelines as they apply to these sorts of offenses and we expect significant increases. There have been other perpetrators who have been identified of course. Mr. Parsons was alleged to have—he has only been charged. He is presumed to be in-

nocent. I don't know if convicted of those offenses what kind of prison term he would get. I can get back to you with a more precise answer as to that.

Mr. PUTNAM. We have heard testimony that there are hundreds of viruses per year and millions or maybe even into the billions of damage done. Is there a different attitude or is there a different approach about cyber crimes than there is about other types of crimes? Has our sentencing guidelines, our judicial system, our laws, our legislative branch not kept up with the technology that can promulgate new types of threats?

Mr. MALCOLM. In terms of keeping up with the laws obviously emerging technologies present all kinds of problems for law enforcement, and so we need to constantly reevaluate the state of our laws. And USA Patriot Act, one of the provisions provides now for nationwide service of process of pen trap orders and an explicit recognition. The pen trap orders apply to noncontent interceptions over the Internet. That is an important step in conducting these sorts of investigations.

I am not going to suggest that it is going to be the last such step that is necessary. It's certainly true that as these worms and viruses become more sophisticated and proliferate at a greater rate, the potential damage is real. I think historically there has been a perception that crimes taking place in the physical world are somehow more serious than crimes taking place over the cyber world. I believe that perception is rapidly breaking down, and I expect the prosecutions and sentences to increase.

Mr. PUTNAM. Mr. Pethia, Carnegie Mellon has done much more work on this than anyone. I would like you to comment on this different attitude. When we had conversations with the private sector when I was in Silicon Valley, the analogy is always used that people rattle their door knobs and rattle their locks thousands of times per day depending on which firm it is. Obviously you have high profile targets in the IT world and some are lower. But some are getting thousands of door rattlings per day and they choose not to report it. They don't want to give any uneasiness to shareholders or to consumers, so they just accept it as part of this Internet culture, and it results in hundreds of true viruses per year.

Is there a different attitude about the Internet and crime and consequences?

Mr. PETHIA. I don't know about different attitude, but I sense a certain complacency, that people have become so accustomed to the problem and are often so overwhelmed with the problem, so unable on their own to change some of the root causes of the problem, that they've simply chosen to live with it as best they can.

You're right, many don't report the attacks, but, again, many are so trivial and so common that if you were to report them, it's not clear what anyone would do with all of that data. In fact, separating the wheat from the chaff, the serious attacks from the trivial, has become an increasing challenge for all of us who do any kind of instant response. Buried in all of this are the serious attacks like the Blasters and the SoBigs and the people who are intent to do malicious damage.

But, I think the widespread recognition is that the problem's here and it's serious, but I think individuals don't know what they

can do above and beyond putting controls in place in their own organizations.

Mr. PUTNAM. You don't think that there's necessarily a different attitude about it?

Mr. PETHIA. I think it's more an attitude of complacency and acceptance and just frustration over not knowing what steps that they can take as individual organizations or as individuals to make a difference.

Mr. PUTNAM. Have you ever heard of something called a Black Hat convention?

Mr. PETHIA. Sure.

Mr. PUTNAM. What is that?

Mr. PETHIA. There are a number of different conferences. There are two that are typically held every year about people who talk about the Black Hat conference, or people who at one time wore black hats, they broke into and attacked computer systems. That conferences is now typically attended by white hats and not black hats, but they talk about weaknesses in software. They talk about what can be done to improve the situation. They talk about how do we exploit some of these problems so they recognize very much how widespread and serious this problem is, and in their own ways they try to take steps to get corrections out to the world.

Mr. PUTNAM. What percentage of those who are attempting to hack into computers and exploit code vulnerabilities, what percentage of them are bright, capable teenagers seeing what they can do, and what percentage of them are malicious? What percentage are based offshore, and what percentage are based domestically?

Mr. PETHIA. Those are good questions. I wish we had answers to those. You know, we all have our guesses, but I don't know of anyone who's done any detailed studies about what's called the Internet underground, what the composition of that culture is or even what the economy is. There's an underground economy that's growing, that trades in things like account names and passwords and Social Security numbers that are pirated and drivers' license numbers that are pirated, and I don't think any of us really has a good understanding of what that culture is or how big it is or how many different kinds of people play in it.

One thing that is really clear is that it is literally child's play to break into many of the systems that we have today, and when a level of skill needed to attack a system is so low, you can expect all kinds of players to come into that arena.

Mr. PUTNAM. When the conventioneers, whether they're wearing black hats or white hats, when they come together in the good of their heart, talk about ways to improve the system and draw attention to different software companies' vulnerabilities, do they ever ask for money or credit or acknowledgment or anything in exchange for disclosing that information?

Mr. PETHIA. There certainly are cases where these individuals have tried to extort money from vendors in order to not publicly disclose patches or vulnerabilities in their products. We've certainly seen cases where individuals have tried to extort organizations because they've uncovered weaknesses in their operational systems and have expected money in return not to make that public or to

exploit those vulnerabilities in some way. So there is a maliciousness there in some cases.

Mr. PUTNAM. Mr. Malcolm, do you have any other comments about the source and origin and nature of these hackers? Are they primarily international, domestic, teens, professionals?

Mr. MALCOLM. I think you can really break that down into different categories in that you have a core group of committed, highly sophisticated hackers who come up with sophisticated worms and viruses, and then unfortunately what they do frequently is there are chat rooms and Internet sites, news groups in which hackers communicate, and literally somebody who develops a very sophisticated hacking tool can put it out there so that so-called script kiddies, unsophisticated people who just happen to go to that site, can then utilize that tool.

So the level of sophistication can vary dramatically among hackers, and because these tools are made available on the Internet, lots of people can then implement them to cause damage. I think that because the Internet is borderless and seamless, and there are people who are hell-bent on destruction and technically savvy around the world, you have perpetrators who are domestic and perpetrators who are international.

Mr. PUTNAM. Thank you very much.

Mr. Clay. The Chair recognizes.

Mr. CLAY. Thank you.

Let me ask any of the three, Mr. Dacey, Hale, and Lorentz: Did the Department of Homeland Security collaborate effectively with Microsoft and the antivirus companies in the Department's effort to issue advisories? And you can start, Mr. Lorentz.

Mr. LORENTZ. In our view, the proof is in the results. The problems were, for the most part, in general, mitigated, and there was two pieces of that.

First of all was getting the information out about the remediation, which they did, and then was really following up and holding the agencies accountable on our behalf, to make sure what the implementation was and reporting that back, and we did that in a manner so that we could share what people's experiences were. So, in our view, it was in both of these incidents that we've had recently they did a find job.

Mr. PUTNAM. Thank you.

Mr. Dacey, anything to add?

Mr. DACEY. In terms of that, I'd just like to add one thing. We did do some analysis and gathered information with respect to the two vulnerabilities, the Microsoft RPC and the Cisco, and in those cases there was a fairly active discussion and reporting that took place on those two. As Mr. Lorentz indicated, for those two specifically, which were deemed critical, there were separate teleconferences and data requests that were sent out to agencies to ask, you know, what they had done and whether or not they had patched their systems in response to them.

I think that is a process which has taken place, I believe, on a few of the occasions prior to this, but I know that there is some opportunity there which would be acknowledged to improve that process, to make sure that people have been communicated to in a rapid manner by standardizing processes and procedures for that

communication to occur. But I would also defer to Mr. Hale, who could probably speak more to the specifics of those interactions.

Mr. CLAY. Great.

Mr. HALE. Yes, sir. I appreciate the remarks of my colleagues, and I just wanted to point out that those, as well as the Cisco vulnerability, the IOS vulnerability that has occurred in the past 3 months has been the major events in cyber incidents that have occurred since the formation of the national Cybersecurity Division, and so those are indicative of the kind of coordination and collaboration that this Division has started to do and intends to build on to improve not only the information-sharing among the Federal agencies, but also with the critical infrastructure protection community.

Mr. CLAY. Let me ask you, Mr. Hale, in creating the Homeland Security Department, Congress moved the Federal Computer Response Team from GSA to Homeland Security. How has this move affected that group? Did anyone leave the Agency, rather than move, as we saw with some other agencies, and did the move affect the group's ability to respond to any of the more recent attacks?

Mr. HALE. The effect was entirely positive, sir. The FedCIRC was under GSA, had a focus on the security of Federal agencies in providing a service to Federal agencies, our customer base, and thanks to the provisions of FISMA, Federal Information Security Management Act, FedCIRC was able to remain focused on that mission and continue to provide our services to our customers. We didn't lose any staff members as a result of going to the Department of Homeland Security; in fact, recruiting to fill our vacancies became increasingly easier because there were a lot of people who were very interested in becoming part of our efforts to help cybersecurity and the Federal agencies, and by joining forces with the National Infrastructure Protection Center and the other elements of NIAP, we've actually improved our ability to gather information and disseminate information to the customer base.

Mr. CLAY. Let me ask you, Mr. Malcolm, recent viruses and worms, such as Code Red, Nimbda, and Slammer, have brought large portions of the Internet to a halt, caused extensive expenses and lost revenue, and consumed the attention of tens of thousands of computer security professionals, computer network administrators and users. These are serious crimes. Have law enforcement officials found and arrested the individual responsible for these viruses and worm attacks?

Mr. MALCOLM. They've also consumed the time and attention of a lot of dedicated law enforcement agents. Of course, the Department doesn't comment about ongoing investigations; however, I think it is safe to say that with each of the worms and viruses you have identified, those are all matters of ongoing investigation in which we work cooperatively with our international counterparts. We have some successes, as with the criminal complaint that's been filed in the variant "B" of the Blaster worm, but I think it is safe to say that there is a lot more work to be done, and unfortunately, we not only have to act retroactively, but because these worms and viruses come out weekly, we have to react prospectively as well.

Mr. CLAY. Are the individuals who are responsible for these attacks, are they still at large today?

Mr. MALCOLM. Other than those who have been arrested either here or overseas by international counterparts, yes, they're still at large, unless they've died.

Mr. CLAY. And you work with international law enforcement, too?

Mr. MALCOLM. Twenty-four hours a day, 7 days a week.

Mr. CLAY. How many have you arrested out of the viruses that I named, the three that I named, Code Red, Nimbda and Slammer?

Mr. MALCOLM. I don't know the answer to that question. I believe they are all matters of ongoing investigation. I'm not sure off the top of my head of any arrests in those particular cases, but I can go back and check, and if there's anything that's a matter of public information, I'd be happy to furnish it.

Mr. CLAY. Would you share that with us?

Mr. MALCOLM. If that's public information, I certainly will.

Mr. CLAY. Thank you, Mr. Chairman. That's all.

Mr. PUTNAM. Thank you.

Mrs. Miller.

Mrs. MILLER. I thank you, Mr. Chairman. I'll just ask a couple of questions here, but I think the nature of my questions are reiterating what all the committee members are talking about here and what is really happening as far as the attitude that our Nation has and our Justice Department, our law enforcement has toward these cyberhackers.

You know, I was following here in the papers recently where the recording industry has filed all these lawsuits against the file sharers. I know 200 lawsuits or whatever. Obviously, that's not really terrorism, unless you're a recording star, you're losing all this money, right? But I was interested in the response of these college kids who are downloading all this music and are getting sued, and they certainly don't care about that. We're going to continue to down—I mean, their attitude is unbelievably cavalier, I think, to breaking the law by using electronic means to do so, and perhaps that is part of the problem we have with these cyberhackers is the attitude of our legislature, of our law enforcement; I mean, are we serious enough? And as you were mentioning, some of the—you know, is it just college kids who are doing this? Obviously not. You've got the whole realm of different kinds of people who are doing the cyberhacking.

Have you ever done a psychological profile? I mean, these people are terrorists that are trying to shut down, as I was mentioning, power grids or those kinds of things. That's not downloading music. Let me ask you first about that, as far as the Justice Department. Has there been a psychological profile? I mean, there must be some type of common trait, common element. It would be like an arsonist, right? You see the fire services do profiles of arsonists. These are people that burn buildings and stand back, and there's a whole profile about these kinds of people that perpetrate that kind of crime.

Mr. MALCOLM. I'm not aware of any psychological profile. I think that perhaps I could contrast the situation with an arson in that unless somebody wants to literally kill somebody inside a building,

arsonists tend to be motivated by one purpose, and that is collect the insurance money.

In terms of hackers, I think you run the gamut. You obviously have, perhaps, terrorists who are interested in exploiting critical infrastructure for destructive ends. You can have political "hactivists" who go on to deface Web pages of something that they are protesting. You have sophisticated hackers who take pleasure in trying to stay one step ahead of the technological development of law enforcement, who take pleasure in their ability to outwit law enforcement by masking their activities. And you also have, as I say, these script kiddies who are more or less with respect to their use of the computers who were out there on a lark. They all cause harm of varying degrees. We take them all seriously.

Mrs. MILLER. Let me just ask one other question in regard to the Patriot Act. You mention the Patriot Act, and the Patriot Act, of course, there's been a lot of consternation talked about the Patriot Act of whether or not privacy—a lot of privacy advocates are concerned about how the Patriot Act is being implemented, how you are identifying and apprehending culprits.

I'm a supporter of the Patriot Act, and I'm just wondering how that particular tool has assisted the Justice Department in our law enforcement, and are a lot of these concerns being raised by the Patriot Act impeding your ability to prosecute, apprehend people, identify them, etc.? How is the Patriot Act helping you?

Mr. MALCOLM. There are several questions in there that kind of cut across a broad swath. Let me respond to the more narrow question, then I can fill in as you would like me to.

With respect to hacking investigation, any crime that is taking place online, time is absolutely of the essence. If you can catch somebody while they are in the act or trace their communications either in real time or very shortly thereafter, your odds of catching somebody go up dramatically. Internet service providers don't retain records typically for a very long period of time, and people can very quickly cover their tracks.

There are a number of provisions in the Patriot Act that help. There is, one, the hacker trespass exception of the Patriot Act. If somebody breaks into a system, the owner of that system now can give consent to the government to go in and track the activities of that hacker while they are taking place. Certainly the ability to go and get a pen/trap order in one district and use that order to follow the communications from ISP to ISP to ISP, to get those records frozen as quickly as possible, has proven of invaluable assistance. There are other tools such as nationwide service process for search warrants, subpoenas, all of which have been instrumental in terms of these investigations.

Mrs. MILLER. Thank you.

My last question just to the panel, I suppose. Obviously, the Federal Government has their own role to play in protecting our own information and security systems and that, but I think the public needs to be educated on security, computer security, as well. I'm not sure who I'm asking this question to; any of the panelists, I suppose. Do you have a feeling that there is a role for the Federal Government to play in regards to educating the general public about security safety and how important it is?

Mr. PETHIA. I'm going to start just by saying I think that's something that I think is a strong role for the Federal Government, and it needs to happen across the country with people of all ages and all occupations. Starting at the elementary school level or where we teach students about computer skills, we need to teach them about computer ethics and the risks of working with computers and interacting in the Internet age. We teach our children how not to get into cars with strangers. We should teach them how not to get into chat rooms with strangers as well. So from there all the way up through the home user, the retired home user, all of these people are vulnerable to some kind of problems because of security or lack of security on the Internet, and I think there is a strong role for the government there to put together that kind of awareness, to put together those kind of training programs and make them broadly available.

Mr. LORENTZ. I think I would just add I think that our government has a responsibility to our citizens. As part of the management agenda, security is clearly one of the things we are looking at. It cuts across public and private-sector activity. We do have a role in clearly communicating what's acceptable, what's not, creating that common language, if you will, and it begins with exhibiting the behaviors that we would wish to see.

Mr. HALE. I would definitely endorse the statements. In fact, with home computers being connected and always on, it's nothing short of a patriotic duty to maintain the security of your home computer because it can be used to attack other computers by other people.

Mrs. MILLER. Thank you Mr. Chairman.

Mr. PUTNAM. Thank you, Mrs. Miller.

Mr. Malcolm, are there differences among nations in the laws regarding cybercrimes, and are there other nations who have particularly more effective means of enforcing them and have a greater success rate in prosecution, and are there certain countries that are more or less helpful to us in investigative work?

Mr. MALCOLM. I think the short answer to all of those questions was yes. There are a couple of things that I can say in that regard. One is we cooperated with our international counterparts throughout the world in terms of drafting the now—well, it hasn't been ratified in this country, but the now implemented accounts in the Europe Cybercrime Convention. One of the beauties of the cybercrime convention in addition to encouraging international cooperation is that it mandates signatory countries to update their substantive and procedural laws with respect to computer hacking offenses, which would include worms and viruses.

Mr. PUTNAM. Updates them to presumably a certain standard?

Mr. MALCOLM. That's right.

Mr. PUTNAM. And are we already at that standard in the United States?

Mr. MALCOLM. We're constantly retinkering, but, yes, we try to maintain the highest standard that we can. We work cooperatively with Congress in that endeavor. And I would add that the Department of Justice, although not uniquely—the Department—the State Department certainly, too—goes overseas and works with leg-

islators and law enforcement officers in other countries to try to keep their laws updated as well.

From other entities, such as the G–8, there is a high-tech unit that's called the 24/7 network in which we are able to communicate with law enforcement counterparts in these fast-breaking investigations on a moments notice, 24 hours a day, 7 days a week. There are 30 countries that are members of the high-tech 24/7 network. We're encouraging other countries to join. Some countries have better facilities, training, more money to devote to this effort than other countries, but we're encouraging all of them to stay current.

Mr. PUTNAM. But you're not aware of any one particular area of the world that is a source of more hacking attempts than another?

Mr. MALCOLM. The answer to that question, with respect to Internet piracy, with respect to hacking, I don't know the answer to that question, Congressman.

Mr. PUTNAM. Mr. Pethia, do you?

Mr. PETHIA. No, not that's been sustained over any long period of time. For a while, there were a number of viruses that for some reason came out of Bulgaria, and you see short periods of time where you'll see an increase of activity from some geographic area, but nothing that I know of that's been sustained over a long period of time.

Mr. PUTNAM. We may hear more about this in later panels. For the OMB, how long does it take, because everyone has different patch management systems—are you able to measure how long it takes for all of the computers to download the patch when a particular vulnerability is released and the patch is also then released? Do you know when everyone has taken advantage of it?

Mr. LORENTZ. I can answer the more management aspect of that and later get into the technical, because they basically act as our agent in that. But we literally are advised of the vulnerability, we call attention to the vulnerability. FedCIRC makes the agency aware of what the remediation of the patch is, and then we specifically set a time to get back to monitor the adherence to the remediation.

And it's in the last two incidents that's exactly what we did, and I would feel quite sure that FedCIRC probably has some cycle time issues that they can look at in terms of how long it actually takes, but, you know, there's two aspects to all of this. The most significant aspect is the management aspect, and that is holding people accountable once they know, and it's mutually accountable to CIOs as well. Once they know that there is an incursion, that the patch has to be applied, and that there's accountability to apply, then there's the obviously technical nature of things, and there's a number of technical capabilities that are equally effective, but I would pass it to Larry on the cycle time question.

Mr. HALE. For the 47 subscribers of patch C, we can tell when they download, but even that is—can be a misleading statistic, because one download can serve thousands of computers, and an agency may download one time and take care of their whole enterprise with that. So we've tried developing metrics with industry with the software manufacturers, and that's the constant refrain is you can't measure how many computers have been inoculated by

a single download, but it's the best thing we've got is to tell that agencies are downloading the patches.

Now, with the patch C system, agencies can also—once they've inoculated their systems, they can enter in the report and say—it requires a manual entry, but say that we've completed 90 percent or we've completed 99 percent or 100 percent of computers affected by this vulnerability, so there's a method built in for reporting back.

Mr. PUTNAM. Mr. Malcolm, if someone were to break into Coca Cola's headquarters in Atlanta and go into the office and steal the recipe for Coca Cola, what would be a ballpark estimate assuming they were arrested and convicted, what type of consequence would they face for that?

Mr. MALCOLM. Mr. Chairman, there are a lot variables that would go into answering that question.

Mr. PUTNAM. Ballpark. I'm not a judge.

Mr. MALCOLM. Well, in the interest of trademark infringement, theft, I would estimate statutory penalties at 10 years or so, depending on whether or not the person has a prior record. That would obviously affect their sentencing guidelines.

There are just too many variables for me to answer that question, without having a guideline book in front of me, but obviously the factors are what are the charges, what is the severity of the loss, what is the person's past criminal record?

Mr. PUTNAM. Well, what would it be if they hacked into Coca Cola's computer system and downloaded the secret recipe?

Mr. MALCOLM. Same answer: You would have all sorts of variables as to whether or not they abused a position of trust, what was the damage that they cased. It could obviously be, in the case of Coca Cola, a major company, a major loss, a significant period of time.

Mr. PUTNAM. Would it be significantly different than had they physically taken it?

Mr. MALCOLM. There are different guidelines factors that would take into account the fact that a computer was used, and special skills were used, and, depending on who this person was, whether or not they abused the position of trust. There are, under the sentencing guidelines—there are just too many individual case-specific factors for me to give you an accurate answer to your question. I think it is safe to say that if this was a major product and caused a serious loss, I would expect the dollar figure to be high, and that will dramatically increase the sentence since the major factor that is taken into account by the sentencing guidelines is the loss to the victim.

Mr. PUTNAM. OK. There are hundreds of viruses released every year, according to the testimony of this panel. The damages range into the billions, according to your testimony.

Mr. MALCOLM. Yes.

Mr. PUTNAM. If you could only recall two arrests, two convictions, two jail times—you mentioned David Smith and one other.

Now, I asked, what's the source of the threat? Well, we really don't know. Is it foreign or domestic? Well, we really don't know. That seems to reinforce a premise that cybercrime is treated vastly different than some other crime that caused billions in damage and

shut down power grids and shut down departments of transportation and threatened security systems within and without the government. It would suggest that there is a different approach, a different attitude, a different level of concern about cybercrime. Would you agree or disagree with that?

Mr. MALCOLM. I would reject that implication totally. There are, of course, other instances in which perpetrators had been identified; for example, the fellow in the Philippines who promulgated and released the ILOVEYOU virus. I would also say that there are—you know, the Department of Justice is well aware, as is the Department of Homeland Security, that cybervulnerabilities are among the most critical problems that we have and could have a dramatic impact in terms of protecting our critical infrastructure.

These are unusually complicated investigations in which very sophisticated people are very good at covering their tracks. To somehow suggest that just because there are fewer public arrests out there in the media, that this is not an absolutely high, high, high priority at the Department of Justice would be a completely wrong assumption to make.

Mr. PUTNAM. OK. I take it at your word.

Any other questions from the subcommittee members?

Very well. We will dismiss panel one and seat panel two as quickly as possible.

Thank you very much, gentlemen, for your input, and those of you who can, we would encourage you to stay around and listen to the private sector comments as well.

[Recess.]

Mr. PUTNAM. Very well. The subcommittee will reconvene.

I've asked panel two to rise and please be sworn in.

[Witnesses sworn.]

Mr. PUTNAM. Note, for the record, all the witnesses responded in the affirmative.

We appreciate you being seated as quickly as possible, and we will move straight to your testimony. I would ask that you be as good about maintaining our 5-minute rule as the first panel was.

Our first witness is Mr. Gerhard Eschelbeck, overseeing Qualys' engineering and operation. Gerhard Eschelbeck is responsible for protecting over 1,100 corporate networks. He's an internationally recognized security and distribution systems expert and was recently recognized as 1 of the 25 most influential CTOs by InfoWorld Media Group.

Prior to joining Qualys, Gerhard was senior vice president of engineering for security products at Network Associates; vice president of engineering of antivirus products at McAfee Associates. He was a research scientist at the University of Linz, Austria, from which he earned his Master's and Ph.D. degrees in computer science. He has authored many articles and papers and is inventor of numerous patents in the field of network security automation, and is a frequent speaker at networking and security conferences worldwide.

Welcome.

Glad to have you at the subcommittee, and you're recognized.

STATEMENTS OF GERHARD ESCHELBECK, CHIEF TECHNOLOGY OFFICER AND VICE PRESIDENT OF ENGINEERING, QUALYS, INC.; CHRISTOPHER WYSOPAL, CO-FOUNDER, ORGANIZATION FOR INTERNET SAFETY AND DIRECTOR OF RESEARCH AND DEVELOPMENT, @STAKE.INC.; AND KEN SILVA, VICE PRESIDENT, OPERATIONS AND INFRASTRUCTURE, VERISIGN, INC.

Mr. ESCHELBECK. Mr. Chairman and members of the subcommittee, thank you for the invitation to testify about my research on network vulnerabilities. The business of my company gives us a front row seat to new threats against networked computers and communications systems. Qualys provides an automated service over the Web to audit the security of networks.

I've just analyzed more than 1.2 million network vulnerabilities found by our virus scanning service during a recent 18-month period. This vast data pool demonstrates that known risks are far more prevalent than anyone has imagined. Analytical data also demonstrates a new breed of automated Internet-borne viruses and worms that mock traditional security defenses.

The source of data for my analysis was anonymous results from 1.5 million security audit scans made by organizations worldwide. We learned four themes that are called the laws of vulnerabilities. The law of half-life talks about the fact that it takes an average of about 30 days for organizations to fix 50 percent of their vulnerable systems within enterprises. The law of prevalence talks about the fact that half of the most prevalent and critical vulnerabilities are replaced by new ones each and every year. The law of persistence: Some old vulnerabilities recur due to the deployment of unpatched software as part of new rollouts. The law of exploitation, finally, talks about the fact that 80 percent of the vulnerability exploits are available within 60 days of public announcements.

Automating defenses against these threats is crucial, because human-based efforts are not working. In each case of recent damaging strikes, we've had advanced warning; weeks, even months, to prepare for known vulnerabilities, yet attackers were still able to hit hundreds of thousands of PCs and servers.

Risks to network and system security are increasing because the triggers are becoming automated, requiring no human action to deliver destructive payloads. Earlier first-generation threats are virus-type attacks, spreading with e-mail and file-sharing. They require human action to trigger, such as opening an infected file attachment. An example would be the most recent SoBig virus.

Second-generation threats comprise active worms leveraging system and application vulnerabilities. Penetration occurs without requiring user action. Replication, identification, targeting of new victims are automatic. Blended threats are common, such as incorporating viruses and Trojans.

A third generation of threats is now posing trouble. We've already seen the potential for damage. The SQL Slammer worm rapidly hit more than 75,000 homes running Microsoft SQL server, caused major damage worldwide. SQL Slammer was the fastest worm ever, infecting more than 90 percent of the vulnerable systems within 10 minutes.

A few days after Microsoft published a DCOM vulnerability in July 2003, Qualys's automated scanning service ranked this security vulnerability as the most prevalent vulnerability ever. Following the laws of vulnerability, Blaster and its derivatives appeared 3 weeks later, infecting more than 100,000 systems per hour at its peak. Urgency's now rising from a shortening discovery/attack cycle. SQL Slammer happened 6 months after discovery; Nimda was 4 months; Slapper was 6 weeks; and Blaster and Nachi came just 3 weeks after news of the vulnerability.

Public policy for network securities should strongly encourage the use of automation as an equal force response to automated tools used by attackers. Automating defense strategies include regular security audits of networks and systems, keeping antivirus software up to date, timely patch management, and the ongoing variation of security policy.

To summarize, many vulnerabilities linger, sometimes without an end. New attacks are capable of spreading faster than any possible human response effort. Protecting our networks is a continuous process of eliminating critical vulnerabilities on the regional, national and international scale.

In conclusion, public policy should demand timely detection and a rapid application of remedies providing protection from these threats.

Thank you for the opportunity to testify, and I look forward to your questions.

Mr. PUTNAM. Thank you very much, Mr. Eschelbeck.

[The prepared statement of Mr. Eschelbeck follows:]

Testimony of

Gerhard Eschelbeck, Ph.D.

Chief Technology Officer and V.P. of Engineering

Qualys, Inc.

ge@qualys.com or 408-315-4875

"Worm and Virus Defense: How Can We Protect the Nation's Computers From These Threats?"

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

House Government Reform Committee

September 10, 2003

MR. Chairman and Members of the Subcommittee: I am Gerhard Eschelbeck, Chief Technology Officer and Vice President of Engineering at Qualys, Inc. Thank you for the invitation to testify about my research on network vulnerabilities and how we can protect the nation's computers from new threats.

The business of my company gives us a front row seat to new threats against applications, networked computers and communications systems. Responding to the growing sophistication of security threats, Qualys has developed an infrastructure for automated vulnerability detection. Such automation allows us to produce security audits immediately and cost-effectively over the Web for networks of all sizes. Based on our research and experience with network vulnerabilities, we believe the development of public policy for minimizing network-based attacks requires provisions for security automation to effectively protect against a new breed of automated attack technologies.

I have just analyzed 1.24 million network vulnerabilities found by our scanning service during a recent 18-month period. This vast data pool demonstrates that known risks are far more prevalent than anyone has imagined. Analytical data also demonstrates a new breed of automated, Internet-born viruses and worms that mock traditional security defenses.

Data for my analysis were a statistically significant sample anonymously drawn from 1.5 million security audit scans made by organizations worldwide. We learned four themes that I call the "Laws of Vulnerabilities":[1]

#1 is "Half-life" – The half-life of critical vulnerabilities is 30 days and doubles with lowering degrees of severity. In other words, for even the most dangerous vulnerabilities, it still takes organizations 30 days to patch 50% of the vulnerable systems, leaving them exposed for a significant period of time.

[1] See "The Laws of Vulnerabilities" at www.qualys.com/laws.

#2 is "Prevalence" – Half of the most prevalent and critical vulnerabilities are being replaced by new vulnerabilities each year. The continuous discovery of most dangerous and widespread vulnerabilities creates an ever changing window of exposure to computers and networks.

#3 is "Persistence" – The lifespan of some vulnerabilities is unlimited. Old risks recur partly due to new deployment of PCs and servers with faulty unpatched software.

#4 is "Exploitation" – 80% of vulnerability exploits are available within 60 days of public announcements of those vulnerabilities. Such rapid availability of exploits creates a significant exposure for organizations until they patch all their vulnerable systems.

Data for the four themes document the persistent ability of attackers to gain full control of systems – including access to highly sensitive information such as financial data and intellectual property. Automating defenses against these threats is crucial because human-based efforts are not working. In each case of recent damaging strikes, we've had advance warning – weeks, even months – to prepare for known vulnerabilities. Yet attackers still were able to hit hundreds of thousands of PCs and servers, crippling vital businesses and services and causing other havoc. Internet-borne risks threaten everyone including consumers, commercial, and public organizations and local, state, and federal governments.

Automated Attacks Bring More Risk

Risks to network and system security are increasing because their triggers are becoming automatic, requiring no human action to deliver destructive payloads. Consequently, security incidents reported to the CERT Coordination Center are soaring. Incidents rose 2,099 percent from 1998 through 2002 – an average annual compounded rate of 116 percent. Incidents reported during January through June of 2003 already totaled 93 percent of incidents for all of 2002![2]

[2] See www.cert.org/stats/cert_stats.html.

The nature of these risks is changing dramatically. Earlier "First Generation" threats are virus-type attacks spread with email and file sharing. They require human action to trigger replication and spreading, such as opening an infected file attachment. Examples are the Melissa Macro virus, the LoveLetter VBScript worm, and, most recently, the SoBig virus.

"Second Generation" threats comprise active worms leveraging system and application vulnerabilities. Penetration occurs without requiring user action. Replication, identification, and targeting of new victims are automatic. Blended threats are common, such as incorporating viruses and Trojans. Recent examples are the Slapper worm (9/02), the SQL Slammer worm (1/03), and the Blaster worm (8/03).

New Challenges Posed By Risks of the Future

A "Third Generation" of threats is now posing trouble. We've already seen the potential for damage. On January 25, 2003, the SQL Slammer worm rapidly hit more than 75,000 hosts running Microsoft SQL Server, crippling Internet operations in South Korea, disabling cash machines at a major U.S. bank, disrupting 911 call center operations in Seattle, and causing other disruptions worldwide. SQL Slammer was the fastest worm ever, infecting more than 90 percent of vulnerable hosts within 10 minutes. It reached a full scanning rate of more than 55 million scans per second after just three minutes.[3] SQL Slammer, although lacking much of the potential of Third Generation Threats, demonstrated the aggressiveness of hyper-propagation.

The recent Blaster worm had many signs of a Third Generation Threat. Exploiting the Microsoft DCOM remote procedure call vulnerability, Blaster infected more than 100,000 systems per hour at its peak. Microsoft published news of the vulnerability including a patch on July 16, 2003. Within two days Qualys' automated scanning service ranked this security vulnerability in the global Top 10 list of most prevalent vulnerabilities. The DCOM vulnerability ranked #1 after just four days, making it the most prevalent vulnerability ever. Following the Laws of Vulnerabilities, Blaster

[3] See "Inside the Slammer Worm," IEEE Security & Privacy, July/August 2003 at http://computer.org/security/v1n4/j4wea.htm.

and its derivatives appeared three weeks later causing disruption and significant financial impact.

Third Generation threats contain five characteristics:

#1 – Faster Damage by Quick Propagation. By pre-compiling and cataloging vulnerable targets in advance, Third Generation threats strike faster – preventing timely intervention by security administrators. Strikes can be finished in just minutes.

#2 – Leverage Known & Unknown Vulnerabilities. New attacks continue to exploit known vulnerabilities. Pre-compiling techniques used in Third Generation attacks will also enable use of obscure vulnerabilities, including those that are unknown to the broader security community.

#3 – Employ Multiple Attack Vectors. Simultaneous targets will include new technologies lacking strong security, such as Instant Messaging, wireless network infrastructure and voice-over-IP systems. Third Generation attacks will also leverage polymorphic techniques for concealment and encryption to prevent discovery during attack.

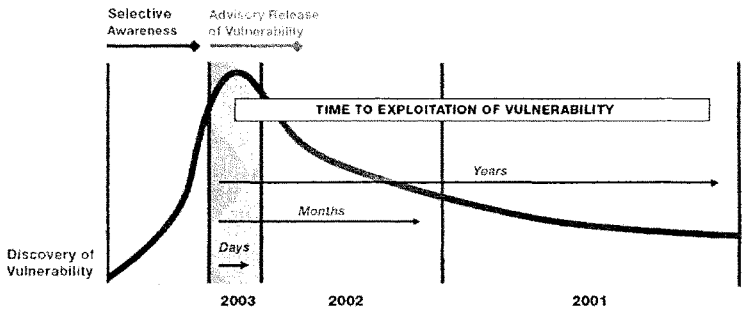
#4 – Use Active Payloads. Active payloads have specific targets such as a geographic area, an industry or a particular company. Blaster's payload was to create a distributed denial of service attack against Microsoft Corporation starting Aug. 16, 2003. Active payloads may be covert, holding back attacks for a future date or silently perform malicious actions such as modifying or deleting content on a victimized system.

#5 – Attack Inside Perimeter Defenses. Third Generation threats are shredding traditional defenses of the network perimeter. Worms like SQL Slammer and Blaster target covert channels to penetrate internal networks, such as compromising home PCs used for office connectivity and by other means.

Taking Charge With Automated Defenses

Persistence and hyper-propagation are important considerations in creating public policy for network security. In the past, the discovery/attack lifecycle was a year or more from the advent of discovering a vulnerability to widespread exploitation. Urgency is now rising from a shorter discovery/attack cycle – SQL Slammer happened six months after discovery, Nimda was four months, Slapper was six weeks, and the most recent Blaster and Nachi worms came just three weeks after news of the vulnerability.

The diagram below illustrates compression of the discovery/attack lifecycle.



Source: Qualys, as published in *SC Magazine*, July 2003

Public policy for network security should strongly encourage use of automation as an equal-force response to automated tools used by attackers. Automating defense strategies include:

- **Regular Security Audits of Networks and Systems**. New automated audit solutions identify everything susceptible to attack, identify and prioritize vulnerabilities, and match them with appropriate remedies, such as patches and new security-device configuration settings.

- **Keep Antivirus Software Up-to-Date**. Server- and client-based solutions for automatic detection and cleansing of systems provide protection only if continuously updated.
- **Timely Patch Management**. Automated audit scanners can quickly identify which systems need urgent care and facilitate a timely and consistent remediation process.
- **Ongoing Evaluation of Security Policy**. Trend analysis with automated scanning solutions provides data for ensuring that security systems help meet the ever-changing nature of attack threats; thus enabling organizations to take control of their network security, adhere to security best practices and help comply with regulatory legislations.

Conclusion

In summary, network security attacks are increasing in number and sophistication. My research demonstrates that many vulnerabilities linger, sometimes without end. New and evolving attacks are capable of spreading faster than any possible human response effort. Protecting our networks is a continuous process of eliminating critical vulnerabilities on a regional, national and international scale. Public policy for network security should demand the timely and complete detection of security vulnerabilities with automated techniques and rapid application of remedies. These measures effectively thwart new automated attacks and protect the continuity of critical network-based applications and services.

Thank you again for the opportunity to testify to the Subcommittee. I look forward to your questions.

Mr. PUTNAM. Our next witness is Chris Wysopal. Mr. Wysopal is director of research and development at @stake.Inc, managing @stake's pioneering research in application security. His primary focus is building products to assure and test software security. Working with vendors and the general public, Mr. Wysopal was also responsible for managing @stake's vulnerability research and disclosure process.

His career in the information security industry has spanned over 13 years where he has held positions in industry while also serving as regular advisor to various government agencies. Prior to joining @stake, Mr. Wysopal was senior security engineer at GTE Internetworking, formerly known as BBN, where he was the most senior engineer on the IT security staff. In addition, Mr. Wysopal is coauthor of the award-winning password-auditing program, LC3, which is used by more than 2,000 government, military and corporate organizations worldwide. And, finally, he is a founding member of the Organization for Internet Safety.

Welcome to the subcommittee. We look forward to your testimony.

Mr. WYSOPAL. Chairman Putnam and members of the committee, thank you for inviting me to testify today on the subject of protecting the Nation's computers from viruses and worms. This is a great honor for me. My company @stake consults for the Fortune 1,000, including four of the world's top software companies. We help them build more secure software and secure their infrastructures. I am also a founding member of the Organization for Internet Safety. OIS is a group of software vendors and security companies joined together to produce a process for reporting and responding to new vulnerability information safely.

Today I would like to cover three pertinent issues: The software development process, the vulnerability research process, and finally, responsible vulnerability reporting and response. Unfortunately, in less than 72 hours, if an unpatched new computer is connected to the Internet, it will be compromised. This is indicative of the software flaws that affect our information economy. My first point is on software development, the root cause of the problem is software flaws. Every virus or worm takes advantage of a security flaw in the design or implementation of a software program. The flaw can exist almost anywhere inside a program that processes data directly from a network or from a file delivered by an e-mail attachment. This means that practically every software program in the age of the Internet falls into in the category of requiring security quality processes during its development. If these processes are not in place and followed rigorously by the manufacturer, flaws will inevitably creep into the software during development, be discovered, and end up exploited.

Automatic patching is a great solution for some computers, but many environments have requirements that don't allow patches to be applied in automatic or even timely manual manner. One of the key problems with patching is the Internet or the network the computer's connected to is the distribution system. This means that a computer needs to be connected to the Internet to be patched. The irony is the Internet is the attack vector that puts the computer at risk.

As recent examples of worms demonstrate, reactive solutions are not keeping up with the speed of malicious programs. Many of the flaws found in software after it is shipped to customers are not found by the vendor. Many are found through directed research by vulnerability researchers. These are individuals who investigate the security of software for academic reasons, profit, or mere curiosity. A primary motivation of vulnerability research is altruistic. There aren't any independent or government watchdog groups looking out for the safety of the software—computer users' use. Given this vacuum, researchers feel that someone should test and find vulnerabilities. They feel that every flaw they find and report is another flaw that will be fixed before a malicious person finds and exploits it. In this way, vulnerability researchers can make all computers users more safe.

Vulnerability researchers are performing a testing function that should have been done as part of the security quality assurance process by the vendor. Vulnerability researchers think differently than traditional software testers. They think from the perspective of an attacker. The fact that there is a vast amount of software already deployed with latent undiscovered flaws means that we will be dealing with newly discovered vulnerabilities for the foreseeable future.

A process for handling new vulnerability information in a timely and safe way is required. There is some debate in the vulnerability research community as to the best way to handle vulnerability information. However, most agree that it is responsible to inform the vendor of the vulnerable product and give them time to create a patch. 4,200 vulnerabilities were tracked by CERT last year. Almost all had patches available when the information became public due to vulnerability researchers informing vendors prior to publicly disclosing.

The Organization for Internet Safety has published a process that these flaw-finders can use to report flaws to vendors and for vendors to respond to these reports, sometimes with a patch. The goal of the OIS process is to protect the computer user community as a whole. A balance was struck between the timeliness and reliability of patches and between helping sophisticated users and the majority of users who are unable to help themselves.

To conclude, software vendors face challenges building software. Vulnerability researchers can help find the flaws that vendors miss. Both need to come together to handle vulnerability safety. All I ask is a step in this direction. Viruses and worms are shutting down government offices and businesses for days. The impact grows each year. When a technology contains dangerous, unseen risks, we should have assurances that it is built properly. We need the, "electrical code for building software," and we need a way to assure that the code is followed. This will reduce the risk of insecure software at its source and strengthen the computer infrastructure for us all.

Thank you.

Mr. PUTNAM. Thank you very much. Appreciate your input.

[The prepared statement of Mr. Wysopal follows:]

Testimony for the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Hearing on "Worm and Virus Defense: How Can We Protect the Nation's Computers from These Threats?"

Christopher Wysopal

Director of Research and Development

@stake, Inc.

Introduction

Chairman Putnam and members of the Committee, thank you for inviting me to testify today on the subject of protecting the nation's computers from viruses and worms. This is a great honor for me. My company, @stake, consults for the Fortune 1000, primarily financial and telecom companies as well as independent software vendors. We enable them to build more secure software and secure their infrastructures. We also build products that automate the process of finding flaws in software. With these products and with manual methods we provide software security testing, also known as vulnerability research, for our customers. I am a founding member of the Organization for Internet Safety (OIS). OIS is a group of software vendors and security companies joined together with the goal of producing a process for reporting and responding to vulnerability information safely.

The problem of worms and viruses has plagued personal computers since their inception. The source of the problem is twofold: software that is written with time to market concerns and features as more important than safety, and computer users who don't understand that they need to take proper precautions given an increasingly risky computing environment.

A public network such as the Internet is an environment with hostile actors. The software that runs inside of critical infrastructure components such as network routers and servers, as well as desktop applications such as email and Web browsers, needs to be designed in a defensive manner. It must be built with the security quality processes of secure coding and security testing. The computer industry is slowly making progress in this direction, but the economics of software development leads to the reuse of old insecure code even in new products. Computer users are also loath to "upgrade" to new, more secure versions of software due to the cost and the resources necessary to make the change.

The current flawed computing infrastructure is not going to change for the better overnight. It will take many years of hard work. This situation leads to the need to manage newly discovered vulnerability information carefully and to apply secondary lines of defense to protect vulnerable computers until software can be created and deployed that is significantly more secure. There is no "silver bullet" secondary line of

defense. There needs to be a combination of technologies such as automated patching, antivirus products, firewalls and user education.

Vulnerabilities not detected before a software product is released are often found in the field by customers (and their security contractors), independent vulnerability researchers, and the vendors themselves. It is critical that the vulnerability information be handled properly so that a fix can be created and installed by the software user before malicious individuals take advantage of the flaw.

The Organization for Internet Safety has created a vulnerability handling process where flaw finders can easily report issues to vendors; vendors can diagnose and remedy the problem, and then release a fix. The process is a compromise between the need to produce a fix as quickly as possible yet still adequately test that the fix works and does not cause additional problems. It is also a compromise between the needs of users and security professionals to have adequate information available to protect systems, and the need to keep the details required to exploit the vulnerability away from those who would write worms or manual exploit tools.

The Root Cause of the Problem is Software Flaws

Every virus or worm takes advantage of a security flaw in the design or the implementation of a software program, whether that program is the operating system of a personal computer or network router, is running a Web or database server, or is a desktop application such as an email program or word processor. The flaws that are exploited by viruses and worms are not limited to flaws in the security *features* of these programs. The exploited flaw can exist almost anywhere inside a program that processes data directly from a network or from a file delivered by an email attachment.

Practically every software program in this modern age of the Internet falls into the category of requiring security quality processes during its development. If these processes are not in place and followed rigorously by the manufacturer, flaws will inevitably creep into the software. These unknown, latent flaws will then be shipped to the software customer. Many of these flaws will eventually be discovered during the software's lifetime.

When the details of these flaws get into the hands of the malicious individuals who write and distribute viruses and worms, many computer users suffer. The computer users affected are not only the users of the software with the flaws, but other users who share the common resources of the Internet. This is due to the fact that worms and viruses tend to clog up networks and mail servers.

Until recently, perhaps within the last 3 years, building software that was highly resistant to attack was not a top priority of software vendors. Fortunately many are now on the path to educating their software developers to build their products with a secure development process.

Securely built software has security processes added to the design, implementation, and testing phases of the software development lifecycle. Software designs need to be analyzed using threat modeling techniques to assure that the design protects against known threats. Implementation is the phase where the source code is actually written by software developers. These developers need to follow secure coding practices to avoid generating flaws such as buffer overruns. A buffer overrun is precisely the flaw that the Blaster worm exploited. Finally, security testing needs to be performed to catch any errors that the developers made that lead to security flaws.

Most software vendors have sophisticated quality testing processes where all discovered flaws ("bugs") are ranked according to severity and the likelihood a user will be affected by the flaw. The process is designed to eliminate the most serious problems while leaving many minor flaws unfixed due to time to market concerns. Security flaws can and do fit into this process. The important factor is that security flaws can have much more severe impact than a run of the mill software "bug". When security flaws are found they need to be given a high enough priority so they don't go unfixed by the time the software ships to customers.

Patches Are Not a Complete Solution

When a serious flaw is discovered in the field a software fix in the form of a patch is a necessity. If a serious flaw remains for many weeks the data shows that it will eventually be exploited. Research by the HoneyNet Project[1] showed that an unpatched Linux 6.2 system connected to the Internet would be compromised in less than 72 hours. Other operating systems had similar results. Many users think that no one is directing an attack at them so they don't need to bother with security patches. Worms and automated exploit tools don't discriminate. They make every system a target of chance.

Some argue that making patching easier and even automated is the solution. But there are problems with patching which I will outline. The only real long-term solution is to eliminate or at least drastically reduce the number of necessary patches by developing software with a secure development process.

Patches Are Often Not Applied

Automatic patching is a great solution for some computers, but many environments have requirements that don't allow patches to be applied in an automatic or even timely manual manner. Critical computers need to have acceptance testing performed on the new patches before any changes are made. Even when vendors do extensive regression testing they cannot test for all configurations. Patches have been known to cause computers to become unstable. Computer downtime and rebooting often accompany patches. When the patched computer is a critical system this requires planning and computer redundancy. If a patch fails and crashes the system it may take hours to fix.

In industrial and telecom environments, many special purpose computers are treated as appliances even though they have general purpose operating systems running inside them

[1] http://project.honeynet.org/papers/stats/

such as Windows, Solaris, or Linux. The purchaser of this equipment often does not know what software is running inside. @stake has performed audits of telecom and utility companies and found systems such as these that are years out of date with patches.

Internet Patch Distribution

Another problem with patching is *the Internet is the distribution system.* This means that a computer needs to be connected to the Internet to be easily patched. The irony is the Internet is the attack vector that puts the computer at risk. There are two timely examples that illustrate the seriousness of this problem.

The Blaster worm discovered on August 11, 2003 affected the majority of Microsoft Windows computers. It was designed to attack the Microsoft "Windows Update" Web site, which is where computer users were supposed to go to patch their systems. Fortunately the worm writer made mistakes that caused the attack to be easily disabled. Increasingly attacks are becoming more and more sophisticated. If the attack had been successful it would have been nearly impossible for most users to patch their systems.

The Cisco denial of service flaw made public on July 18, 2003 had the potential to cause parts of the Internet to fail if it was exploited. This meant that Cisco had to get the patch out to their "Tier One" customers that run critical portions of the Internet before releasing vulnerability information to all customers. If they hadn't released the patch this way there was the potential that the Internet would cease to function properly and no one could patch. Fortunately, Cisco found this problem internally, which is the best case for flaws that exist in deployed products. They were able to carefully manage the vulnerability information and patch release. If this problem had been first discovered by someone with malicious intent they could have essentially disabled the Internet and downloading a patch from Cisco's Web site would not be possible. Cisco's processes helped mitigate this fragile state of affairs.

Widespread Problems Strain Patching Resources

Most organizations have the people resources to handle patching critical infrastructure such as firewalls and routers or servers because there are a limited number of these computers. When a flaw is found that is so widespread that it affects almost every desktop or laptop, it usually takes many hours or days to patch them all. This is why for some worms you see large sophisticated organizations with computer downtime that can last days.

Reactive Solutions Not Keeping Up

The fast moving Slammer worm, which infected Microsoft SQL Servers last year, was able to compromise nearly all vulnerable systems in about 30 minutes. System administrators didn't know what hit them until it was too late. Reactive solutions such as patching computers after news of a new worm or waiting for antivirus signature updates are not keeping up with the growing sophistication of malicious code.

Preventing the Next Blaster or SoBig

Some simple design changes could have prevented the Blaster worm and the SoBig.F email virus. These changes do make using Windows computers for file sharing or email a tiny bit more difficult, but the result would be eliminating whole classes of worms or viruses. The net result would be making the Internet more reliable and eliminating the need for many users to have computer downtime due to a future Blaster-like worm or SoBig-like virus.

Blaster took advantage of a service that all Windows computers expose to the network by default. This service allows Windows computers to perform file sharing and run programs remotely on each other. The consensus of security professionals is that a service like this should never be exposed to the Internet unless necessary. The default Windows configuration should be that no services are exposed to the network by default. This is how some other current operating systems are configured out of the box. Many security savvy users configure their Windows systems either by using the Windows built-in firewall or another software firewall. By making sure services are not exposed to the network by default the Blaster worm would have been a fraction of the problem it was.

The SoBig email virus takes advantage of the fact that many users still open attachments without understanding what kind of file it is. Email viruses often try to disguise that an attachment is an executable file that will take control of their system when opened. All email programs need to be designed to not allow executable content to be sent or received. It is just too dangerous. Some newer email programs do this. Older Email programs that allow this should be considered unfit for use on the Internet and eliminated. Eradicating executable attachments from the Internet will eliminate most email viruses.

Vulnerability Researchers

Many of the vulnerabilities found in software after it is shipped to customers are not found by the vendor. Some vulnerabilities are stumbled upon by customers. Others are found through directed research by vulnerability researchers. These are individuals who investigate the security of software for academic reasons, profit, or merely curiosity. In all of these categories there are vulnerability researchers that uphold high ethical standards and those that don't.

A primary motivation of vulnerability researchers is altruistic. There currently is no independent or government watchdog group looking out for the safety needs of normal computer users the way the National Highway Traffic Safety Administration looks after the safety of car owners. Given this vacuum, vulnerability researchers feel that someone has to test and find vulnerabilities. They feel that every flaw they find and report to the vendor is another flaw that will be fixed before a malicious person finds and exploits it. In this way vulnerability researchers make all computer users safer.

At @stake, our customers rely on us to find vulnerabilities in the software they are using and report those issues to the appropriate software vendor. When the issue is fixed, all users of that software benefit.

One of the motivations of vulnerability researchers are to make a name for themselves the way an academic does publishing a paper. "Publish or perish" is certainly a way for vulnerability researchers to maintain a name for themselves in the security community and perhaps the larger information technology world. Many individuals are after credibility or fame amongst their peers. The profit motivation is there for vulnerability researchers who sell security products or services. Publishing their research is a way of demonstrating their expertise.

Whatever the motivation of researchers it is important that they handle the fruits of their labors carefully. Vulnerability information in the hands of a software vendor can allow them to fix their product. In the hands of a worm writer, some information has the potential to shut down the Internet. Most vulnerability researchers understand this power and behave ethically, but of course some don't.

There is a group of researchers that use publishing vulnerability information as a way of embarrassing vendors into cleaning up their security processes? . They want the vendor to look bad and to have the vendor's customers harmed. Five to ten years ago there was some legitimacy to this position. At that time most vendors tried to ignore researchers reporting flaws. They would not fix flaws and hoped the researcher would go away. Over time vendors have learned that their customers expect them to fix flaws in a timely way and that in many cases the stability of their customers' computing environments is at risk. Most vendors today are responsive, but mistrust remains.

There are also vulnerability researchers who fall into the malicious hacker category. They do not share their information with the vendor; they share it only with their friends. They write exploit tools that allow them and their friends to break into computers. This is a very dangerous situation because if there is no patch for the flaw the person with the exploit tool can compromise computers with impunity. It is next to impossible to detect and catch these individuals. The only solution to this is to produce software with fewer defects using a secure development process.

Why Vulnerability Researchers Succeed

There are two main reasons why vulnerability researchers succeed in finding flaws that the vendor should have found. Current development processes create an inordinate number of flaws and have limited capabilities for finding them. Much of the software developed today is not built with a secure development process. Security design flaws and insecure coding techniques are endemic in the industry. This is how the flaws get there in the first place. There are signs that many software vendors are improving. Yet even when a vendor switches to a secure development process for new code they still often include old, insecurely developed code in their new products.

Compounding this insecure development problem is inadequate security testing to find the flaws. Security testing is challenging because the testing team cannot be sure they have found all the security flaws within a fixed about of time. The complexity of modern software creates a situation where some flaws are relatively easy to find and some are more difficult and take more time to find. Even if a vendor is able to eliminate all basic flaws the chance remains someone with excess time and energy can still find a security vulnerability.

The industry needs to learn how to design and build software more securely. It also needs to learn from the techniques of vulnerability researchers how to change their quality assurance processes to include security testing.

Vulnerability researchers are essentially performing a security testing function that should have been done as part of the software quality assurance testing process by the vendor. Vulnerability researchers think differently than traditional testers. Testing applications for security flaws takes a true paradigm shift on the part of the tester; they need to begin to think of themselves not as a verifier, but as an attacker. They perform *negative testing*. Negative testing is forcing a program to perform actions on invalid or malicious data in order to reveal what the program could allow an attacker to do.

Positive testing is testing to see if a feature of a software program works. If a program is supposed to save a file to disk when save is selected from the menu, the tester will test to see if that feature works. To contrast negative testing with functional or positive testing imagine a simple financial software application that receives an account number as input and displays an account balance as output. Negative testing inputs invalid data in for the account number to ascertain how the program responds.

The simplest negative testing is to input an invalid account number and check to see that the program returns an error message. This is about the limit of negative testing that is commonly seen in a quality assurance test plan. In order to adequately test the security of an application much more extensive negative testing is required.

The goal of the security tester is to get the program to fault; to get the program to do processing it wasn't designed to do. The security tester designs tests which input data that is particularly problematic for an application to deal with. If the program produces erroneous results, the security tester hones the data in an effort to control the way the program is failing. If the tester is able to exert control over the program or is able to get the program to become unresponsive, it is a vulnerability.

Vulnerability Information Handling

The fact that flaws, or vulnerabilities, exist at all in software shipped to customers is a problem that needs to be solved. But this is a very difficult problem that will not be fixed overnight or even in a few years. The fact that there is a large amount of software already deployed with latent undiscovered flaws mean that we will be dealing with newly

discovered vulnerabilities for the foreseeable future. A process for handling vulnerability information in a timely and safe way is required.

There is some debate in the vulnerability research community as to the best way to handle vulnerability information. However, most agree that it makes sense to inform the vendor of the vulnerable product and to give them time to create a patch. If this wasn't the case there would be much more chaos on the Internet. 4,200 vulnerabilities were tracked by the CERT Coordination center last year. Almost all of them had patches available for public information release due to vulnerability researchers informing vendors.

The area where there is much debate is how much detail should be published about the vulnerability. Detailed information usually allows someone to craft a tool that exploits the flaw. Once an exploit tool is written and released, it allows a much wider audience of unskilled computer users to attack vulnerable systems. On the other hand more details can help security professionals and system administrators defend computers in ways that the vendor may not have envisioned. Many don't like the fact that they need to rely on the vendor to provide the best solution for them because there are times when this is not the case.

The problem of detail is most visible with open source software. Often the patch is distributed as a source code "diff" (for difference) file that is the ultimate detail. It shows exactly which lines of code were vulnerable and how they were changed. This sometimes leads to open source projects slipping out security fixes as part of regular releases. They don't want to notify users of the fix lest malicious individuals get the information too.

Another point of disagreement in the vulnerability research community is how to work with vendors. Many are suspicious of vendors dragging their feet and not wanting to actually fix problems. In the past many vendors did not work well with researchers. This is changing but the sense of mistrust continues.

Organization for Internet Safety Process

Introduction

The Organization for Internet Safety (OIS) was formed by a group of vendors and security companies to come up with best practices of vulnerability information handling. OIS has published a process that flaw finders can use to report flaws to vendors and for vendors to use to respond to these reports. The process, "Guidelines for Security Vulnerability Reporting and Response" (http://www.oisafety.org/reference/process.pdf) was published on July 28, 2003 after a public review period. The security companies and vendors involved intend to adopt the process themselves and promote the process to their peers.

The goal of the process was to protect the computer user community as a whole. There were times when tradeoffs needed to be made between timeliness and reliability or

between helping sophisticated users who could better protect themselves, and the majority of users who are unable to help themselves.

Participants[2]

Although additional participants may be involved in this process, the primary participants are:

- **The Finder**. The security researcher, customer, or other interested person or organization who identifies the vulnerability.
- **The Vendor**. The person, organization, or company that developed the product, or is responsible for maintaining it.
- **Coordinator**. An optional participant that serves as a proxy for the Finder and/or Vendor, assists with technical evaluations, or performs other functions to promote the effectiveness of the security response process.
- **Arbitrator**. An optional participant that adjudicates disputes between the Finder and Vendor.

Phases[3]

The basic steps of the OIS Security Vulnerability Reporting and Response Process are:

1. **Discovery**. The Finder discovers what it considers to be a security vulnerability (the Potential Flaw).
2. **Notification**. The Finder notifies the Vendor and advises it of the Potential Flaw. The Vendor confirms that it has received the notification.
3. **Investigation**. The Vendor investigates the Finder's report in an attempt to verify and validate the Finder's claims, and works collaboratively with the Finder as it does so.
4. **Resolution**. If the Potential Flaw is confirmed, the Vendor develops a remedy (typically a software change or procedure) that reduces or eliminates the vulnerability.
5. **Release**. In a coordinated fashion, the Vendor and the Finder publicly release information about the vulnerability and its remedy.

Timeline

There is no single universal timeframe for which all vulnerabilities can be investigated and remedied. Some flaws can be fixed in one line of source code. Others may require weeks of redesign and coding. Some vendors support only one version of a product that is affected and others may support dozens, compounding the problem of creating patches in a timely matter. In practice vulnerabilities take between a week and several months to remedy. The OIS process suggests 30 days as a starting point.

---

[2] Excerpted from "Guidelines for Security Vulnerability Reporting and Response" (http://www.oisafety.org/reference/process.pdf), published on July 28, 2003

[3] Excerpted from "Guidelines for Security Vulnerability Reporting and Response" (http://www.oisafety.org/reference/process.pdf), published on July 28, 2003

The guidelines prohibit publishing details that could be used to create exploits for the vulnerability until 30 days after the patch is released by the vendor. This is to allow enough time for customers to install the patch, but still allow long term researchers the information needed to better understand how vulnerabilities occur and how they can be prevented.

Conclusion

As a society we are already dependant on computers working properly for many important functions ranging from the financial system to the power grid. The types of software vulnerabilities that lead to worms and viruses such as Blaster and SoBig are well understood. Researchers now know how to build software with significantly less vulnerabilities. Instead of focusing solution efforts on lines of defense deployed by every customer, such as patching solutions and antivirus software, we should focus our nation's limited security expertise on the source of problem: the flaws in software. Software needs to be developed with a secure development process and old insecure software should be eliminated.

Viruses and worms are moving from an annoyance to shutting down government offices and businesses for days. Their impact grows each year. When a technology contains dangerous unseen risks we should have assurances that it is built properly. We need the "electrical code" for building software and we need a way to assure that the code is followed. This will reduce the risk of insecure software at its source and strengthen the computer infrastructure for us all.

Mr. PUTNAM. Our next witness is Ken Silva. As vice president for VeriSign's networking and information security, Mr. Silva oversees the mission-critical infrastructure for all network security and production IT services for VeriSign. In this role, he oversees the mission-critical network infrastructure for VeriSign's three core business units: security services, naming and directory services, and telecommunications services. His responsibilities include oversight of the technical and network security for the definitive data base of over 27 million Web addresses in dot-com and dot-net, the world's most recognizable top-level domains.

Additionally Mr. Silva coordinates the security oversight of VeriSign's Public Key Infrastructure security systems.

Mr. Silva serves on the board of directors for the Information Technology, Information Sharing and Analysis Center, and the executive board of the International Security Alliance.

He advises and participates in a number of national and international committees for organizations, and he joined VeriSign with more than 20 years' experience in the telecommunications and security industry in his portfolio.

Welcome to the subcommittee. We're delighted to have you. You're recognized.

Mr. SILVA. Thank you, Mr. Chairman and other members of the subcommittee. VeriSign's pleased to have the opportunity to provide our views on the epidemic virus and worm attacks that continue to threaten the integrity and security of information systems we've all come to depend on. VeriSign is a company that's perhaps uniquely situated to observe the continuing assaults on our information infrastructure. Our company provides industry-leading technologies in three relatively distinct yet interrelated lines of business. These include telecommunications, infrastructure services, management security, and payment processing services, directory and naming services.

Our naming services is the business dedicated to the management of the domain name system, including our operation of the A and J root servers. These are 2 of the servers out of the 13 servers that allow you to find www.house.gov. Of the hundreds of millions of machines on the Internet, it would direct you to the correct one.

In addition to that, for the last 10 years, we've managed the dot-com and dot-net top-level domains.

Since 2000, I've managed VeriSign's resources dedicated to maintaining the security of these complex technology assets.

Today I would like to make three key points. First, we should not underestimate the significance of these attacks. Although the most recent worms and viruses have been labeled by some as non-destructive, they've cost American business in excess of $3.5 billion in August alone. We can only imagine what the cost would have been had these destroyed data along their path.

Second, we should accept our shared responsibilities. Each of us has a responsibility. This includes lawmakers, government agencies, industry and private citizens. Government has a role both as a model of good security practices, as well as a thought leader in global security. Our citizens must be educated. We teach our children how to use computers in school, but do we teach them how to use them responsibly?

Third, we must resist the temptation to demonize individual participants in the network community. The finger-pointing in general is neither accurate nor helpful. It's all too easy to blame the operating systems manufacturer for flaws in their code or the network providers for not securing their networks. Many of the worms attack not only popular operating systems, but open source software as well.

Mr. Chairman, there are measures which will over time improve the security posture of our network, but there is no silver bullet that will miraculously solve our network security challenges.

VeriSign's role over past decade has led us to make significant investments in network hardware, engineering, research and development. Armed with that knowledge, we can deploy and advise others on the network how to deploy the very best configurations and maintain the stable and secure functioning of the Internet. VeriSign's unique monitoring capabilities allow us to watch as the virus propagates around the global network. As a result of VeriSign's constant vigilance, we're often among the first to recognize it, and as an attack develops—you can see our view up here shows our global constellation. I brought another slide with me, which is an example of the graphic data that we're able to monitor. This one shows a propagation of the SoBig.F virus in just a short 6-hour span on August 19.

There's another one following that, the next graphic, please, which today just happens to be the very day that this virus has decided to disarm itself. This was taken this morning.

Following the September 11 attacks, we provided some of these monitoring capabilities to both the Defense Department's NCS and the FBI's NIPC, to enable them to observe and detect anonymous traffic on the network.

Our long experience and the most recent events like Blaster worm reveal fundamental truths about our networks in the attacks. A few years ago, these things took months or weeks to propagate. Now they propagate in hours or minutes. Not only are the weapons behaving more aggressively, they're increasing their uniqueness, making selection of appropriate countermeasures difficult and uncertain. As a result of this growing risk and our growing dependency on our networks, I believe we must face up to the reality that these network attacks are every bit as threatening as physical attacks on critical infrastructures, warranting serious attention to strategies to defend against them and remedy their impact. Even when they don't bring down the network of a targeted site, the insult to the network's integrity still has observable and measurable consequences.

Another level of damage, these attacks fundamentally threaten the core assets of the Internet, including the Internet root servers and top-level domains. There are larger costs to these attacks.

I'd like to thank you for giving me the opportunity to appear before you today. Thank you.

Mr. PUTNAM. Thank you very much, Mr. Silva, and I appreciate your—all of you limiting your remarks to the 5 minutes.

[The prepared statement of Mr. Silva follows:]

Testimony of Kenneth Silva
Vice President, Networks and Security
VeriSign, Inc.

BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

COMMITTEE ON GOVERNMENTAL REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

September 10, 2003

Good morning Chairman Putnam and distinguished members of the Subcommittee. My name is Ken Silva. I am Vice President for Networks and Security of VeriSign, headquartered in Mountain View, California.

VeriSign is pleased to have the opportunity to provide our views on what we believe is one of the most important, yet poorly understood phenomena facing our nation—the epidemic of virus and worm attacks that continue to threaten the integrity and security of the information networks on which we have all come to depend.

VeriSign as a company is perhaps uniquely situated to observe the continuing assaults on our information infrastructure. Our company provides industry-leading technologies in three relatively distinct—yet interrelated -- lines of business. Each of the three serves an important role in the rapidly converging infrastructures that support communication and electronic commerce around the globe.

VeriSign's Telecommunications Services group provides the essential signaling and switching services that make today's digital telephony ----both wired and cellular—possible. This includes features like call waiting and forwarding, wireless roaming and the soon-to-be available wireless number portability.

Our Security organization provides authentication, encryption, secure credit card processing, fraud prevention and detection, managed network security services and a range of other services that enable eCommerce, eGovernment and the over-all secure Internet experience that hundreds of millions of users around the globe have come to rely on.

Our third major line of business is now known as "naming and directory services", and includes VeriSign's assets dedicated to the management of the Domain Name system of the Internet, including our stewardship of the A- and J- root servers—two of the thirteen computers around the globe that represent the top of the pyramid of the Internet's dispersed hierarchy. This is the part of the Internet's infrastructure that allows you to type in "www.house.gov" into your web

browser and immediately be directed to one unique computer from among the hundreds of millions on the network. In addition, under a contract with the Department of Commerce, VeriSign and it's predecessor subsidiary, Network Solutions have for over a decade managed the .COM and .NET top level domains that for many have come to symbolize the essence of the net. Figure 1 (attached) depicts the global distribution of these assets.

I have been privileged to serve Network Solutions and now VeriSign since 2000 as manager of the resources dedicated to maintaining the security of these complex technology assets. On behalf of VeriSign, I also serve in a number of industry capacities, including representing VeriSign on working groups of the President's National Security Telecommunications Advisory Committee—the "NSTAC", working groups of the NRIC which advises the FCC, and as a Board member of both the Internet Security Alliance and the "IT ISAC"—the IT sector's Information Sharing and Analysis Center.

I want to make three key points today that I believe are critical to how the Congress and the rest of the policy community deal with the challenges that continuing attacks against our networks pose.

First, we should not underestimate the significance of these attacks. Although the most recent worms and viruses have been labeled non-destructive, they have cost American business in excess of $3.5 Billion in August alone. We can only imagine the cost had these worms actually destroyed valuable data along their path. While it is important to maintain vigilance for state sponsored or terrorist related attacks, many of these attacks have proven to be the work of individuals barely of legal age, or younger.

Second, we must all accept our shared responsibilities. Each of us has a responsibility. This includes lawmakers, government agencies, industry, and private citizens. Government has a role both as a model of secure practices, as well as a thought leader in global security. Our citizens must be educated. We teach our children how to use computers in school, but do we teach them how to use them responsibly and safely? This responsibility for addressing the gap in security awareness is shared by government, industry and families. But at the same time, the challenge to industry of the National Strategy to Secure Cyber Space to exercise leadership in security awareness, education, assessment and practice must be taken to heart by all of us in the Internet business.

Third, we must resist the temptation to demonize software vendors and other members of the network community. The finger pointing is often misplaced and in most cases does more harm than good. It is all too easy to blame the operating system manufacturer for flaws in their code, or the network providers for not securing their networks. Many of the worms attack not only popular operating systems, but open source software and systems as well. Of greater concern to VeriSign as a security vendor are the anecdotes reported in the media; the overreactions these stories may stimulate—by well meaning legislators or others may result in inappropriately large solutions being applied to problems more readily managed narrowly—and by the marketplace.

VeriSign believes there are actions that over time will improve the overall health and well being of the Internet, but there are no magic solutions or silver bullets. Long-term health and well-being will take time and everyone's efforts. Again, this is as much a responsibility of people as it is of technology.

Because of VeriSign's obligations with respect to the A and J-ROOT servers, we have invested significant power into our infrastructure. Not only do we invest in state of the art hardware and software, we maintain a highly qualified security staff as well. This infrastructure supports not only the security of our services, but those of our security services customers as well. We are

acutely aware of what we can do, what we choose to do, and what we choose not to do. For example, we do not manufacture firewalls or anti-virus software. Instead we choose to rely on other vendors for that. We choose to select vendors that meet our high security and reliability standards and we run through real-world scenarios. Not all vendors pass this test.

We maintain laboratories where we can test security and stability functionality in the protocols and software that we rely upon. These include the protocols used to carry the Domain Name System, the Secure Sockets Layer, and the databases we select. We do this by subjecting them to various assaults and measure the response. We calculate how we can respond to them and we devise strategies for dealing with real-world scenarios. We also work very closely with respected outside sources such as the one operated by my good friend Rich Pethia from the CERT at Carnegie Mellon University. Armed with this information, we can deploy, and advise others on deploying the best configurations.

In addition to software research, VeriSign invests an enormous amount of money and resources into our monitoring capabilities. These monitors are not unlike the telemetry data carried on satellites and weapons systems. They monitor every aspect of our systems and alert us to changes within the system. They allow us to learn from failures and obtain root cause for each incident. Indeed, this monitoring has allowed us to watch some worms propagate throughout the Internet. Figure 2 (attached) depicts the spread and corresponding stress imposed on one of our key assets by the Sobig.F worm. This picture is from our monitoring system on 19 August, 2003.

Immediately following 9/11, we made some of our monitors available to the National Communications System (NCS) in the Department of Defense. We also made it available to the FBI through the National Infrastructure Protection Center (NIPC). We were somewhat surprised to learn that despite their role in protecting the infrastructure, our security agencies had no such tools at that time. Since that time however, these agencies have undergone many of their own security efforts, both through their own development as well as partnerships with industry

VeriSign's sharing of network information and tools has not been limited to the government—as I noted, we have had a long and close working relationship with the CERT at Carnegie-Mellon University and other academic security centers, and are a founding member of the IT-ISAC, and the NCS' Telecommunications ISAC—both attack information sharing bodies comprised of industry members from the IT and telecommunications sectors.

Because of this investment, we are often the first to notice significant events. On 21 October, 2002, we were the first to notice what was hailed as "the largest Distributed Denial of Service attack ever to hit the Internet". We detected this attack, devised a mitigation strategy and alerted the other ROOT operators, as well as CERT, the CIPB, NIPC, and NCS on its effects, and the countermeasures used to thwart it. Despite the fact that 8 of the 13 ROOT servers experienced some level of failure, the Internet continued to function without incident to hundreds of millions of users worldwide.

These incidents, as well as the most recent Sobig.F, Nachi, and Blaster worms reveal fundamental truths about the networks and the impacts we experience. Sobig.F for example has increased load to one of resources by as much as 35 times. We should all ask ourselves; do all of our network elements have the requisite capacity to withstand a 35-fold increase in traffic? This would of course include our mail servers, web servers, Internet backbones, etc.

We must assess our adversaries. They prey not only on the weaknesses of software and operating systems, but the predictability of human beings. Sobig did not launch itself. Someone opened it. And to this day, despite all of the press this has received, it continues to

get re-launched by unwitting individual users every day. Just a few years ago, worms used to take weeks or months to propagate. Today they take but a few hours to infect the entire world. And, as you have heard from others here today, these weapons are behaving more aggressively and they are increasing their uniqueness. This makes selection of appropriate counter-measures difficult and uncertain.

We all recognize the extent that we rely on our networks for economic activity of every flavor. This includes education, entertainment, health care and government services at every level. VeriSign believes we must all also face up to the reality that these virus and worm attacks and other "logical" assaults on our information networks are every bit as threatening as physical attacks on our critical infrastructures. These assaults warrant serious attention from every community of interest to discover the strategies needed to defend against them and remedy their impact.

To date, we continue to see the remnants of long forgotten worms such as Code Red, Nimda, and others. This is long after the patches and well-publicized fixes for these worms. In fact, the fix for Blaster (and all of its variants) was released by Microsoft several weeks ahead of the actual worm. These were well known vulnerabilities that the vendor had long since fixed. It was, and is still, the inaction of administrators and home users to remedy these vulnerabilities that these attacks were able to launch. Although technology can do a lot to help in these situations, we cannot ignore the area between the keyboard and the back of the chair. Users are still the weakest link in network security.

The impact of these worms continues to grow with each new worm. Some ISPs are still dropping packets and exhibiting degraded service because of Blaster and Sobig. The network will continue to weaken a little more with each new worm and it's remnants long after the media stops reporting on it.

But the insidious impact of these attacks is not limited to infrastructure asset compromise or network resource consumption. In point of fact, there is measurable economic harm being visited on all of the network infrastructure stewards. This harm consists not only of the episodic costs, such as the $3.5 billion cited in August of this year alone, but the long-term institutional costs as well. This harm flows downstream to all of the other key economic infrastructures that depend on the Internet.

VeriSign recognizes and believe the assertions by Chairman Greenspan and others about the enormous productivity gains in the past decade attributable to the wide deployment of Information Technology in our economy. Unfortunately, these gains have their own price, which we have not fully understood, and certainly not yet paid—in terms of obligations of appropriate use—including appropriate security practices.

We have had estimates that economy wide, the price tag of universal deployment of adequate minimum security tools across all North American users, in a perhaps three year period of effort, could reach $450 billion—roughly equivalent to the $450 billion per year value assigned to the "information economy." Clearly, we have not reckoned with who—or how—we could pay the price to make such massive network wide investments—or, indeed, who SHOULD ultimately bear this enormous unfunded societal cost.

The most important thing to remember is that securing our network assets is a shared responsibility for all of us. At the most basic level, every individual user can contribute to improve security by taking basic steps towards improved security hygiene. The prescriptions are well known and widely distributed—yet far too few actually engage even in the most simple, low cost and no-cost measures:

- Use passwords, and change them regularly;
- Use anti-virus software and update is regularly;
- Patch the operating systems;
- If you have firewall capability, use it; if you don't, get it;
- If you have an "always-on" network connection (such as DSL, or Cable modem), turn it off when you're not using it.

These simple, low cost measures are not a prescription for guaranteed network security. But they are examples of easy steps every user can take to increase their own security posture. By doing so, we improve the overall resilience of the network to attacks. Such measures will strengthen the network's weakest links, and those exploited by attackers.

When taken, these steps reduce the population of target computers a virus can successfully invade. We all benefit as the Internet becomes less hospitable to hackers, spammers or others who lurk in its murky corners. Organized crime, nuisance mongers, delinquent youths, terrorists and foreign adversaries have exploited these weaknesses in security. All of these adversaries understand our growing individual reliance and the dependence of key global infrastructures on the Internet. Many of them would exploit present vulnerabilities in order to harm America.

Undoubtedly, every operating system, every Web browser and every email client application in use today could have some additional security feature embedded that it lacked at release. But until users---major network managers at large ISPs, corporate networks and many, many Federal agencies-- demonstrate their full compliance with the version and patch management obligations of their software licenses, blaming their vendors for the extent of virus impact is misplaced and distracts us from the important work at hand.

Mr. Chairman, thank you for giving me the opportunity to appear before you today.

About VeriSign
VeriSign, Inc. (Nasdaq: VRSN), delivers critical infrastructure services that make the Internet and telecommunications networks more intelligent, reliable and secure. Every day VeriSign helps thousands of businesses and millions of consumers connect, communicate, and transact with confidence. Additional news and information about the company is available at http://www.verisign.com.

Media Relations Contacts: Brian O'Shaughnessy, VeriSign -- 650-426-5270
Jim Hock, Bite Communications -- 202-973-6616

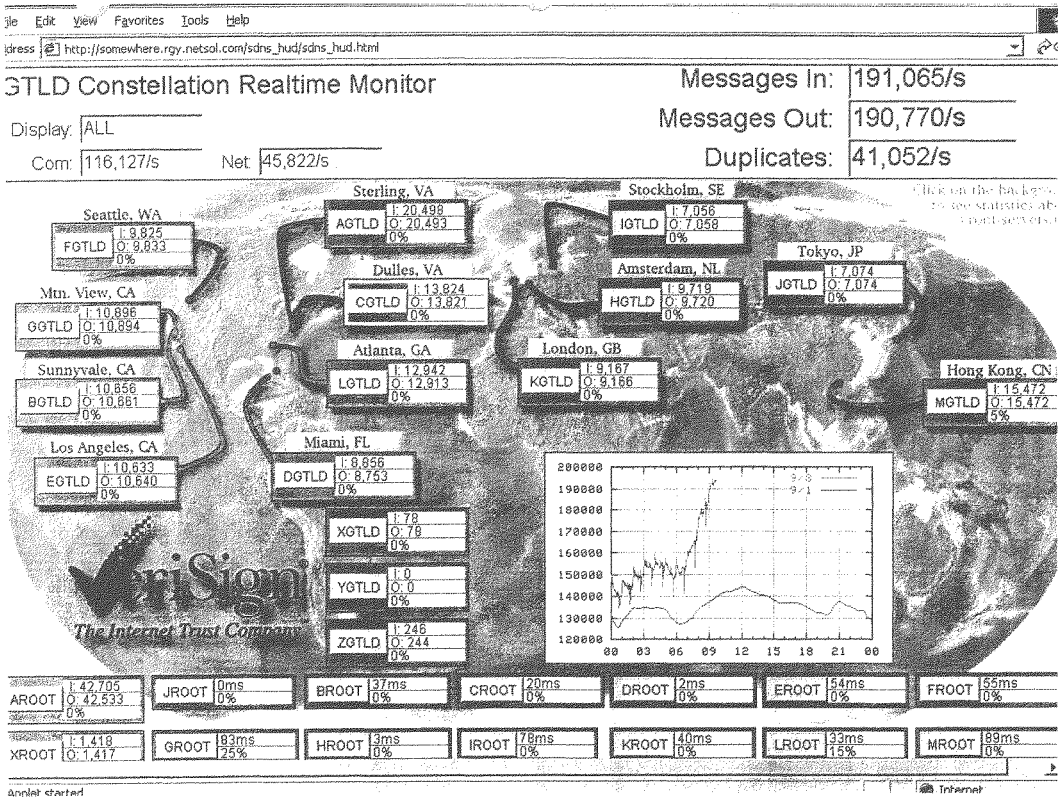

File Edit View Favorites Tools Help
Address http://somewhere.rgy.netsol.com/sdns_hud/sdns_hud.html
GTLD Constellation Realtime Monitor
Messages In: 191,065/s
Messages Out: 190,770/s
Duplicates: 41,052/s
Display: ALL
Com: 116,127/s
Net: 45,822/s
Seattle, WA
FGTLD I: 9,825 O: 9,833 0%
Mtn. View, CA
GGTLD I: 10,896 O: 10,894 0%
Sunnyvale, CA
BGTLD I: 10,656 O: 10,661 0%
Los Angeles, CA
EGTLD I: 10,533 O: 10,640 0%
Sterling, VA
AGTLD I: 20,498 O: 20,493 0%
Dulles, VA
CGTLD I: 13,824 O: 13,821 0%
Atlanta, GA
LGTLD I: 12,942 O: 12,913 0%
Miami, FL
DGTLD I: 8,856 O: 8,753 0%
XGTLD I: 78 O: 78 0%
YGTLD I: 0 O: 0 0%
ZGTLD I: 246 O: 244 0%
Stockholm, SE
IGTLD I: 7,056 O: 7,058 0%
Amsterdam, NL
HGTLD I: 9,719 O: 9,720 0%
Tokyo, JP
JGTLD I: 7,074 O: 7,074 0%
London, GB
KGTLD I: 9,167 O: 9,166 0%
Hong Kong, CN
MGTLD I: 15,472 O: 15,472 5%
VeriSign
The Internet Trust Company
200000
190000
180000
170000
160000
150000
140000
130000
120000
00 03 06 09 12 15 18 21 00
AROOT I: 42,705 O: 42,533 0%
JROOT 0ms 0%
BROOT 37ms 0%
CROOT 20ms 0%
DROOT 2ms 0%
EROOT 54ms 0%
FROOT 55ms 0%
XROOT I: 1,418 O: 1,417
GROOT 83ms 25%
HROOT 3ms 0%
IROOT 78ms 0%
KROOT 40ms 0%
LROOT 33ms 15%
MROOT 89ms 0%
Applet started
Internet

FIGURE 1

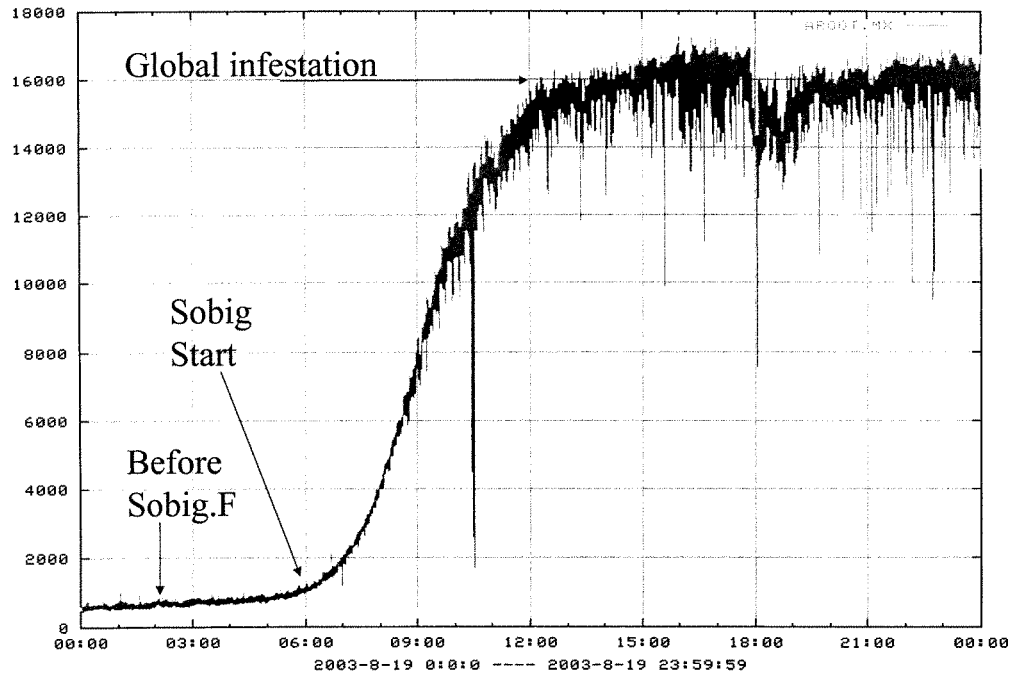

Global infestation
Sobig
Start
Before
Sobig.F
18000
16000
14000
12000
10000
8000
6000
4000
2000
0
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
00:00
2003-8-19 0:0:0 ---- 2003-8-19 23:59:59

FIGURE 2

Mr. PUTNAM. Mr. Silva, I get the impression that you had to cut yours a little bit short, so I'm going to give you the opportunity to expand on it by asking my first question about root servers. And, if you will, just take us in nontechnical terms to their role in the architecture of the Internet, and what their vulnerabilities have been in the past two viruses and worms, and what impact that could have in economic terms.

Mr. SILVA. OK. Well, Mr. Chairman, the root servers are sort of the top of the Internet naming system, if you will. There's an invisible period at the end of every domain name that people don't see, and that happens to be the root, and, then from there it goes.com; then, you know, Microsoft.com; and then www, etc. They're sort of at that very top level. No other computers can be found without the information that these provide. And then there's another layer down from that which VeriSign also operates, for dot-com and dot-net.

The SoBig.F worm in particular had a unique attack that it presented on the A root server, and that the A and B root servers were—it's where that—that worm first looked to find out where an e-mail was supposed to be sent, OK? So if they wanted to send it to, you know, anyone, it would simply look to the root server first to find out where that mail server was.

Now, in the Blaster worm, that didn't actually have an impact directly on the root servers themselves, because there was no protocol that the root servers were running or a particular name lookup that was required for that worm to spread.

Mr. PUTNAM. You mentioned and other panelists have made allusions to open source versus proprietary. Is one less vulnerable than the other, or if you would just comment a bit on the old debate between proprietary and open-source software, again, beginning with Mr. Wysopal. Let Mr. Silva think about his for a second.

Mr. WYSOPAL. The theory with open-source software is that it can be made more secure because there's more eyes. Every single user has the potential, if they have the skill set, to find flaws in that software and then correct them for themselves or notify the maintainer to correct them. With proprietary software, the user has no way really of looking deeply into the software by examining the code, but, practically, users of open-source software are not expert code reviewers and don't have the time to actually review the code, so we see vulnerabilities sort of in equal proportion in both the open-source world and in the proprietary software world.

Mr. PUTNAM. Mr. Silva.

Mr. SILVA. Yeah. I would agree mostly with what he said, except that there always has been this statement that, in the open-source world, the source code's available, and if you were running it, you could certainly look at it. I doubt seriously that you would know, 99.99 percent of the rest of the people who use it.

In addition to the people who use the software not necessarily being expert code reviewers, in many of the cases people actually writing the software are not actually expert software writers either. So it's not that it's bad software, it certainly is good software, but it's no more or less vulnerable than the software that goes through rigid configuration, management, and software review standards.

Mr. PUTNAM. Mr. Eschelbeck, would you like to weigh in?

Mr. ESCHELBECK. I do not necessarily see a relation between open source versus closed source from a vulnerability prevalence perspective. I don't think there is any analytical data that would support that.

However, I do believe strongly that software that's more popular, more widely used out there has been reviewed much more widely and is more popular, and that's one of the main reasons why I think there is more vulnerabilities known about a software that's used widely rather than a software package that's not used at all out there.

Mr. PUTNAM. What would be the impact of, in terms of improved Internet security, if any, of the next generation of Internet, IPv6? Does that in any way alter security concerns?

Mr. WYSOPAL. I don't think IPv6 really alters the security concerns. What IPv6 does is it makes many more Internet addresses available, so we can have an Internet address for, you know, your wristwatch or any small object you could have, thousands or millions of times more Internet addresses with IPv6. It doesn't really address any security issues.

Mr. SILVA. Well, actually, it does address some security issues, although probably not for the masses. There are protocols that are part of the IPv6 standard that would allow better authentication between IP addresses as they connect. Some of those capabilities have since been transferred to IPv4, such as the IP SAC, which is what many of the BPM tunnels use today, but for the general Web server, probably not.

You know, just for the average computer on the network that doesn't need to authenticate every single user, it's probably not going to offer anything new for them.

Mr. PUTNAM. Mr. Eschelbeck, do you wish to add anything?

Mr. ESCHELBECK. I would say exactly the same thing. I think there is a lot of improvements in IPv6, and it's clearly the right step in the right direction, but there is still pieces missing that we don't do in IPv6 today, like in the new protocols that are coming up. And particularly if you look from a vulnerability perspective, IPv6 is not going to address the vulnerability problem. That's really the reality why we are here today, why we're looking for vulnerabilities and how to address them. So IPv6 is certainly the way to move from an authentication, from an encryption perspective, and it would fix some of those underlying issues, but would not fix all of the security issues that we are facing today.

Mr. PUTNAM. Thank you. I will stop there and recognize the ranking member, Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman. And any one of you can attempt to answer these questions.

Let me start out by asking: What motivates people to engage in computer hacking?

I mean, let's start on this end of the table.

Mr. ESCHELBECK. I do think that there is—obviously, if you look back in history, mostly what we have seen, some of the attacks really didn't have any specific target in mind. They were mostly like who is the first who is going to launch a worm on the Internet,

and that was the results we have seen in traffic congestion, things like that. But I clearly see moving forward motives in mind.

If I look at Blaster, it was probably the biggest turning point we have seen here by Blaster introducing the ability to deliver a payload that actually does something malicious, other than just creating noise on the Internet. And in this particular case with Blaster was the denial of service attack against Microsoft, and I do see some transit that is clearly the opportunity for more active payloads coming in future worms. They were motivated by motives that we don't know and fully understand at all.

Mr. CLAY. Mr. Wysopal.

Mr. WYSOPAL. I think the main motivation is experimentation and exploration, but these people who do this experimentation don't take into account any sense of ethics, and they don't really care that their experiments cause harm to others.

Mr. CLAY. Mr. Silva, what do you think about it?

Mr. SILVA. I don't really have anything to add.

Mr. CLAY. All right. Let me ask you, there has been much discussion about information-sharing and cyber vulnerability issues between the government and the private sector, and within the private sector are there any legal or policy barriers that continue to impede information-sharing and cooperation?

Mr. Silva, we can start with you.

Mr. SILVA. Well, there are a number of issues related to antitrust, OK, that have been raised amongst companies sharing information, amongst a select group of people, that's not publicly available. More recently—or, excuse me, prior to that, one of the issues was FOIA, quite frankly, sharing information between government and industries and having, you know, the possibility that a publicly traded company with, you know, some known vulnerability that if they made that information available to the government would somehow be available through FOIA. Some action has been taken in that direction, but those are probably the two main impediments there.

Mr. WYSOPAL. I think another main impediment is companies trying to refrain from looking embarrassed basically. A lot of companies such as financial services companies banks are among the most trusted financial institutions, and people expect the highest level of assurances to protect their money, you know, their privacy, and it could be embarrassing. It could be a competitive advantage of some of their competitors to say, you know, put your money with us. You know, your privacy will really be protected with us. They say they do, but look at this, this, and this. So I think a lot of it is competition and fear of embarrassment.

Mr. CLAY. Very interesting.

Yes, Mr. Eschelbeck?

Mr. ESCHELBECK. I would actually agree with Chris's statement. I would like to add one point here. What we see as well is those areas, those sectors, in general that are—have legislation for auditing requirements, for security auditing requirements, we see a bigger sense of urgency there in comparison to some of the areas that are not legislated today.

Mr. CLAY. Going back to attacks and computer hacking, do any of you have any knowledge of foreign governments involved in

cyberattacks. How is that different from hackers attacking for the fun of it?

Let's start with you, Mr Wysopal.

Mr. WYSOPAL. It's very difficult to say where some of the malicious code, the exploit code, that's written or where some of this vulnerability research comes from. It's difficult to say whether it's a foreign government, or it's just an individual in a foreign country. When we see some malicious code, we certainly see levels of sophistication that are equal to the most sophisticated in the world coming from countries such as China. It's fairly easy to tell because of the language differences where some of this is coming from, but it's very difficult to tell whether it's actually government-sponsored or just academics or just, you know, black hats.

Mr. CLAY. Anybody else got anything to add?

Mr. Silva.

Mr. SILVA. Well, I think probably law enforcement intelligence representatives could probably answer the question as to the foreign sponsorship of the hacking probably better than any of us here could, but I have to say that I think most of these, at least from earlier testimony, have actually been caught. The few of that have actually been caught have turned out to be young adults or teenagers.

While I think we should be concerned about terrorist sponsorship or state-sponsored hacking and malicious activity, I think we should definitely not discard the fact that the vast majority of these appear to be coming from, you know, pranksters, OK, that have no political affiliation or governmental sponsorship. So, while I think it's important that we know if it is state-sponsored, I don't think that all of our efforts should be focused in that direction.

Mr. CLAY. Perhaps any one of you can take a stab at this, but can the Federal Government use its procurement power to improve the security of computer software? Anybody have a thought on that?

Mr. WYSOPAL. I think definitely. The Federal Government is probably the largest purchaser of technology, especially software, and one thing that doesn't happen when people purchase software is an acceptance test for the security of that software. Sometimes it's acceptance testing that has certain features or has a certain level of performance, but acceptance testing for security is more expensive and time-consuming, so no one really does it.

If the Federal Government was to do that, the benefits would be all the users of that software, because the Federal Government could say, you know, we spent a lot of money and tested this, and we rejected it, and we need to go back to the drawing board and build something secure. I think if that happened, the other users of software would say—or potential purchasers of the software would think twice about buying it, if the government wasn't willing to use it.

Mr. CLAY. Thank you. Thank you very much, Mr. Chairman.

Thank you very much, Mr. Chairman.

Mr. PUTNAM. Mrs. Miller.

Mrs. MILLER. Thank you, Mr. Chairman. I am going to pick up on the ranking member's question here, but I think we are all struggling with this panel, members of the committee, with this

panel on understanding what is the appropriate role of the Federal Government.

And you are in the private sector, and—I mean, I am a person that generally thinks that less government is better and less government regulation is better. But because our society is becoming so unbelievably dependent on the Internet, on computers for communication purposes and for security purposes, for everything, the term "vulnerability researcher," I guess I never really heard that before, as I listen to you say it. Now it is going to be part of my nomenclature here. But it's very descriptive, and I can understand what you're talking about there.

Do you think that the Federal Government, first of all, has an oversight role? Should we be using our purchasing power to set standards out for software? What is the fine line of the government not overregulating private industry, but certainly having consternation about some of the security problems that are inherent in software? What would your suggestion be on how far you think the government should be going here, and what is the appropriate action for the Federal Government?

I mean, we just had this huge power outage in my State of Michigan, and we are looking to the Public Service Commission to regulate an industry. And I'm trying to understand everything about the energy policy of our Nation, but I could not tell you what the proper amount for a person to pay per kilowatt hour actually is. We rely on the experts.

You are the experts in the software industry; and I think we are trying to struggle to understand what we need to do appropriately without overstepping our bounds into the private sector.

Mr. WYSOPAL. Well, one place where I think it's important for the government to regulate is when we get to issues of safety, you know, when we are talking about cars or airplanes or chemicals or things like that.

Regulation of safety is important. There used to be, you know, something that you write documents with and safety wasn't an issue. But now when we're seeing these networks being interconnected with things like the power grid actually being connected directly to the Internet, you know, through maybe a few gateways, but you know, the worms got in. You know the worms can get inside, start to get to the issue of safety. And that's a place where I think some regulation is appropriate.

You know, the software industry is a fast-moving industry and putting any regulation on it is certainly going to slow down innovation. There's no doubt about it. But maybe it's time to think about some limited safety regulations.

Mr. SILVA. I think that there's a fundamental role of our government, whether Federal Government or State government, to provide education to our people, to our citizens. If any of you happen to have a DSL or cable modem at home and would actually install a firewall on it and look at the logs, you would be shocked at the number of times penetration attempts actually hit your machine. It would just boggle your mind; it really would.

But as I said in my testimony, or in my statement, we teach our children in almost every school in the country, we teach them how to use computers, how to use a word processor, how to boot a disk,

but we don't actually teach them how to responsibly use the computers and what the consequences of their actions or inactions actually are. So I think that's a role that the Federal Government can play, as well as State government.

Mr. ESCHELBECK. I think there are two areas, looking at it. On the one side we have, obviously, existing infrastructure that we need to look at from a security perspective, and that's probably going to give us an effort for the next 5 or 10 years. And there are specific ideas how those could be handled.

However, there is the new software aspect when new software comes out, there are standards in place like common criteria that are being used to secure—to improve security software. Such standards are not existing for any commercial-type applications. I am not asking for common criteria-type certification for any type of software, but some lightweight certification would give at least a seal of approval from a security perspective as far as the new technology that is coming out there.

As far as the existing infrastructure we have in place today, I think we have to give the leadership perspective infrastructure so they can measure. The key part is, how do I measure security today. There are no tools or well-defined metrics out there. And I think we have to give the leadership and the government, and industry as well, infrastructure tools and ways to measure their security, so that they can say, I am at the level 4, I am at the level 5, and in comparison to other agencies, for example, I am at this level.

So there are ways I think those could be accomplished by putting infrastructure in place there.

Mrs. MILLER. No other questions. Just a comment.

I certainly picked up from both of the panels how important it is for education. You know, really the Internet is still relatively a new phenomenon. Ten years ago, 20 years ago, many people had not heard of the Internet or were not using it every day. The children now, of course—and perhaps it is generational—are leaping onto these computers.

I was struggling yesterday trying to download my boarding pass, and all these things keep coming up on my computer saying, upload this right now or your computer is going to blow up or something. I'm trying to understand it all.

But at any rate I certainly appreciate the testimony here today, and I think the government certainly recognizes again that society is becoming so dependent on electronic technology and how important it is for every generation to understand what the implications are of some of the cyber hacking, and how important it is for them to be able to use these tools properly and understand the ramifications of what they're up to.

Thank you.

Mr. PUTNAM. Thank you, Mrs. Miller.

Mr. Wysopal, if you would, you probably made the most extensive comments about researchers. Tell us a little bit about the category of researchers who would not be classified as altruistic, and their motivations; and I'm not asking you to psychoanalyze them, but how big a group are we talking about? Do they seek fame, seek money or simply the thrill of being able to discover the source code?

Mr. WYSOPAL. I think it's mostly the thrill of having power over computers on the Internet. Part of the way that they keep score is how many systems, you know, have you compromised—the vulnerability that you discovered and wrote exploit tools for or malicious code for, how many computers can you compromise with that.

So a bug that was exploited in a software package that was used by 100 people, no one will care about, but if you find a bug in a Microsoft piece of software which is used by millions of people, then you are looked at amongst your malicious peers as more important and a better black hat.

And this is definitely a very serious problem that people are able to find these vulnerabilities, and usually they keep them to themselves. They don't tell the vendors. They keep them to themselves or share them amongst a small group of people. So they can go into computers with impunity on the Internet and know that problem won't be patched.

And that's a very difficult problem to control. The only way to control that is to actually design the software without the flaws to begin with.

Mr. PUTNAM. And that is an impossibility, right, to have a truly foolproof code?

Mr. WYSOPAL. Yes. There's no such thing as 100 percent secure. But as a company, we do security quality testing for many different software vendors, and we see a vast difference in the number of flaws we find in a piece of software which was developed by a secure development process. Where training was given to the developers, they thought about security through the entire phase, from design implementation to test, versus software where security is really an afterthought; where after the product is shipped, people say, maybe we should think about how to configure it better.

When it isn't thought of from the very beginning, there is a big difference in the number of flaws that end up in the end product.

Mr. PUTNAM. Mr. Silva, you mentioned rule No. 2 was for everyone to accept more responsibility. You discussed the importance of education and things of that nature.

But with the prevalence of broadband, has responsibility shifted somewhat to providers or to cable operators or to telecommunications companies whose history and tradition and corporate culture would not ordinarily lead them to believe that protection against hackers or firewalls would be something of their responsibility?

Mr. SILVA. Well, as I said in my statement, it is a responsibility of everyone, and I think—we always sort of gravitate to the natural thing to do, which is to sort of look at, is this not somebody else, is the responsibility shifting from one group to another?

I don't think it's shifting; I think it's never changed. I think that ISPs, the people that we all use to connect to the Internet, have some level of responsibility. I think that the government, that industry, my company as well as all of the others, have a responsibility to do their part.

For instance, the Blaster worm has been running around the Internet now for weeks, and the network providers are carrying the traffic around it. One would think they would see that traffic mov-

ing around in the network and either deal with it or at least work with a group of people to try to figure out how to mitigate this.

At the same time, if they were to suddenly block that traffic, you know, I can assure you it will create other problems on the Internet. So I think we just have to work together and we have to find out what that magic fingerprint is.

There are a lot of these companies that are carrying this traffic that aren't in the best of financial shapes right now and probably aren't going to invest hundreds of millions of dollars into research and mitigation methods.

Mr. PUTNAM. Thank you very much.

Is there anything that you have not been asked that you wish to comment on or perhaps respond to as a result of panel one, or do you have any additional comments before we seat panel three?

Thank you all very much for your assistance and your input. With that, we dismiss panel two and seat panel three as quickly as possible. And the committee is in recess.

[Recess.]

Mr. PUTNAM. We have panel three seated, and the committee will come back together. And I would ask that you rise, please, and raise your right hands to be sworn in.

[Witnesses sworn.]

Mr. PUTNAM. Let the record show that all the witnesses have answered in the affirmative.

We will go straight to your testimony, and I would ask that you follow the examples of panels one and two and adhere to our 5-minute rule on opening statements. And I will introduce our first witness.

Greg Akers is senior vice president and chief technology officer for three strategic areas at Cisco—customer advocacy technology, corporate strategic security programs and government solutions.

Within customer advocacy technology he and his team focused on how to most effectively use technology to improve Cisco's productivity and strengthen Cisco's relationships with its valued customers. Specific initiatives include technology engineering, autonomic and adaptive networking, cross-customer advocacy research and development functions, and Internet capabilities integration.

He also leads Cisco's corporate strategic security programs with a focus on information security, intellectual property, security solution certifications, and cyber warfare.

Additionally, Mr. Akers runs a government solutions team to address the unique requirements of government. The mission of this team is to provide solutions aimed at government's core business, enabling achievements of its mission to protect its citizenry. He has dedicated teams to address global defense in space, critical infrastructure protection, U.S. homeland security challenges and a government systems unit. His primary focus will be to adapt Cisco products and services to respond to the unique requirements.

Welcome to the subcommittee. We are delighted to have you. You are recognized.

STATEMENTS OF GREG AKERS, SENIOR VICE PRESIDENT, CHIEF TECHNOLOGY OFFICER, GOVERNMENT SOLUTIONS AND CORPORATE SECURITY PROGRAMS, CISCO SYSTEMS, INC.; PHIL REITINGER, SENIOR SECURITY STRATEGIST, MICROSOFT CORP.; VINCENT GULLOTTO, VICE PRESIDENT, ANTIVIRUS EMERGENCY RESPONSE TEAM, NETWORK ASSOCIATES, INC.; AND JOHN SCHWARZ, PRESIDENT AND CHIEF OPERATING OFFICER, SYMANTEC CORP.

Mr. AKERS. Thank you. Chairman Putnam, Ranking Member Clay, thank you very much for the opportunity to testify today on this very important issue.

Cisco is a provider of networking infrastructure for the Internet and intranets of all types. We provide end-to-end network solutions, connecting people to computers and networks all over the world, and align the work-play-live-and-learn without regards to differences in time, place, or type of computer they happen to use.

Roughly 80 percent of Cisco's support transactions and 85 percent of Cisco's sales transactions are completed over our own company Web site. Therefore, we are very concerned about threats and the correct operation of the infrastructure of the Internet.

Rather than summarize the details already provided in my written testimony, in the short time today, I would like to provide recommendations to three specific groups—industry, individuals, and government—with specific actions to address some of these threats.

Vulnerabilities can never be completely eliminated, as has been previously stated. Establishing a product security response capability is a huge step toward reducing the threat. Another major improvement is gathering by setting up obvious e-mail and easy-to-use Web pages, by vendors and customers alike, so they are easily accessible, that will allow vendors to produce results for incidents as they incur.

Most vendors today neither have a team nor modification methods in place. Industry members can contribute greatly by establishing and publicizing product security processes, including taking minimum steps to establish a response team and create necessary links to facilitate incoming reports and outgoing announcements.

External reports of vulnerabilities are often accompanied with demands to publish in a short period of time, less time than the vendor needs to develop fixed software and work around and test these fixes completely. The public is generally unaware of the internal constraints influencing the vendors' schedules.

Because every vulnerability and vendor is unique, time lines should be adjusted by the vendor and the external party for each situation individually. Vendors can help by streamlining their own schedules for producing software and by establishing expectations for negotiating flexible but effective time lines with all external parties.

Many individuals and groups fail to practice confidentiality regarding vulnerabilities and fail to maintain computer and networking systems at some moderate reasonable base line and vulnerability. The consequences can be severe. Individuals should act responsibly regarding vulnerability information. We have published the security advisories and encourage others to do the same.

Some practice poor control over the need-to-know information regarding vulnerability. Some lack timeliness or otherwise detract from the overall success of the process. Numerous plans have been derailed or completely rerouted due to leaks, made more severe by late arrival of information or otherwise slowed down by lack of information or improper information.

Participants are responsible for reporting vulnerabilities promptly and solely to the appropriate recipient, protecting the confidentiality and lending assistance as they are able to. Vendor-neutral coordinating centers are valuable conduits for reporting and handling vulnerabilities. The trust placed in such organizations by the worldwide network security community for the criticality of important coordination function might be jeopardized if it becomes too dependent on funding or other centralized government control, or any one individual entity within industry or the public sector.

Government should ensure that coordinating centers are available, receive adequate funding from multiple sources and avoid dependencies that will treat any participant unevenly or in any other way unfairly. Many are aware of the issue with the "script kiddies," but not are aware of the professional "black hats" who work for a combination of organized crime, terrorists, or nation-states. An entire marketplace that exploits vulnerabilities has sprung up on the Net and has easy-to-use tools, yet it is virtually unknown to the public.

Government should increase funding and support for the development of the maturation of cyber intelligence, the advancement of information sharing, and the overall improvement of law enforcement's ability to prosecute cyber crimes. One issue is common to all the action groups: Vendors respond to customers' demands. Buyers from all of these groups wield considerable influence at purchasing time. If product security or response team are important to you, the buyer should vote with the wallet.

Specifying systems that meet the demands for more security are inevitably the ways vendors will respond, to include increased security measures in their products. Industry, individuals, and government can set effective examples for defining base line security requirements and require compliance to these simply by completion of sales.

The global nature of the Internet means that no single country or industry group can address vulnerabilities in isolation. Success in this arena requires public-private cooperation between all three of these entities.

As an example, consider the cooperation industry under the auspices of a national infrastructure assurance council, developing a vulnerability disclosure framework that should prove to be useful to all parties. The industry leaders I work with understand the roles and are willing to do their part to protect our national and economic security. The recommendations presented here would be a good starting point for improving the security posture for the entire Internet.

I want to thank you, Mr. Chairman, and the other subcommittee members for inviting me today. And I will be happy to answer any questions that you may have.

Mr. PUTNAM. Thank you very much Mr. Akers.

[The prepared statement of Mr. Akers follows:]

Testimony of Gregory Neal Akers
Senior Vice-President and Chief Technology Officer
Government Solutions Group and Corporate Security Programs
Cisco Systems, Inc.

Hearing Before the

House Committee on Government Reform

Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

September 10, 2003

Testimony of Greg Akers, September 10, 2003

Chairman Putnam, Ranking Member Clay, and other Distinguished Members: Thank you for the opportunity to testify today regarding protecting the nation's computers against the growing threats caused by worms and viruses. We are enormously dependent on the correct operation of the Internet, and recent surveys show that Americans are concerned for the safety of business conducted via the Internet.[1]

My Background

My name is Greg Akers, and I am Senior Vice-President and Chief Technology Officer for Government Solutions and Corporate Security Programs at Cisco Systems, Inc. In addition to my present executive responsibilities, I have held senior technical positions at Cisco, including network engineer and vice president of our Technical Assistance Center (the Cisco TAC). Additionally, I am a Cisco Certified Internetworking Engineer (CCIE #1037). Prior to joining Cisco, I spent fifteen years designing, building, and running large networks for "Fortune 100" companies. In 2002, I served as the President of the IT-Information Sharing and Analysis Center (IT-ISAC) and as the Vice President in 2001. Currently, I am a member of the National White-Collar Crime Board and the Board of Directors of the East Carolina Infragard.

Cisco and the Internet

Cisco Systems is the worldwide leader in networking for the Internet. Our networking solutions connect people, computing devices, and networks, and allow people to access or transfer information without regard to differences in time, place, or type of computer system.

[1] "The Internet and Emergency Preparedness: A joint survey with Federal Computer Week magazine", The Pew Internet Project, August 31, 2003, http://www.pewinternet.org/reports/toc.asp?Report=100

We provide end-to-end networking solutions that customers use to build a unified information infrastructure of their own, or to connect to someone else's network. An end-to-end networking solution is one that provides a common architecture that delivers consistent network services to all users. The broader the range of network services, the more capabilities a network can provide to its connected users.

Our core technology began with routers. Routers are what make the Internet work. They act as multi-protocol translators that tie the disparate computer networks of the world together on the Internet, in much the same way that telephone networks in different countries connect and place calls to each other.

Cisco's success is inextricably tied to the Internet. Approximately 80% of Cisco customer support calls are resolved over the Internet. In addition, we estimate that about 85% or more of sales of Cisco's products and services are completed via our website, cisco.com. Therefore, we are very concerned by worms and viruses that threaten the correct operation of the Internet. The Internet is "mission-critical" to Cisco's business.

In my brief time with you today, I will address worms, viruses, and vulnerabilities, as all three are tightly integrated. I will describe issues around vulnerabilities, how vulnerabilities are discovered, and Cisco's process for managing product security incidents, including how we disclose vulnerability and remedies to customers. I will also describe some techniques to reduce the threat of these vulnerabilities.

Vulnerabilities as Vehicles for Viruses and Worms

Viruses and worms exploit a vulnerability to propagate; therefore we will treat viruses and worms identically in this discussion. For the purpose of this testimony, we will focus on vulnerabilities, which we define as a set of conditions that leads to implicit or explicit violations of the confidentiality, integrity, or availability of an information system. Examples may include any one of the following actions performed without authorization:

- Executing commands as another user;

- Accessing data in excess of specified or expected permission;
- Posing as another user or service within a system, or:
- Causing a denial of service.

As more business is conducted using interconnected information technology, the risks of these systems to various attacks is also increasing. The type and scope of such threats can change daily. Additionally, threats are becoming more covert and intricate, which makes them harder to track, root out, and identify.

How are Vulnerabilities Discovered?

Vulnerabilities are uncovered in a variety of ways, such as by vendors during testing, in the course of normal customer use, by vendor-neutral security organizations conducting research, and by miscreants probing systems and programs.

Vendor Testing: As a vendor, Cisco regularly conducts extensive testing of its software and hardware to maintain and improve the security and stability of our products. As the latest vulnerability analysis tools become available or are developed internally, Cisco seeks to proactively identify enhancements and resolve issues, including a strong focus on security vulnerabilities. We consider a variety of factors, which can include the ease of exploitability, the critical nature of the service or protocol to the operation of networks, and the ubiquity of the equipment or application.

Customer Use: Many security vulnerabilities are discovered through customer use and are reported by way of a customer support organization. Vulnerabilities are not obvious as the root cause of a customer support case and may be difficult to identify as a true vulnerability. Customer in this context refers to any user.

Vendor-neutral Organizations: Vendor-neutral organizations, such as the Computer Emergency Response Team/Coordination Center (CERT/CC) at Carnegie Mellon University, coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and

disseminate security improvement information to the broad community. Additionally, they maintain a database to provide early warning of vulnerabilities to Department of Defense (DoD) and other government users. In some instances, affected vendors may employ the assistance of a trusted intermediary such as the CERT/CC to coordinate a multi-vendor product security incident. This can be a valuable service, but it is dependent on the impartiality of the coordination center – If the organization becomes heavily reliant upon a government or commercial organization for funding, the trust placed in it by the community might be diminished to the extent that it can not operate effectively.

Miscreants: The miscreants who uncover vulnerabilities typically range from "script kiddies" (the cyberspace equivalent of vandals and hooligans), to professional "black hats" who work for organized crime, terrorists, nation-states, or some combination. While a "first-time" exploitation of a vulnerability may require some technical expertise, almost **anyone** can make use of exploitation tools afterward. Miscreants often publish these tools widely on the Internet and elsewhere. Many successful exploits are "only" a mouse-click away; no prior experience is necessary.

Public Notification of Vulnerabilities

A key to protecting our nation's computers is effectively sharing information about cyber threats, vulnerabilities, countermeasures, and best practices. Differing opinions exist regarding the most appropriate way to disclose vulnerabilities. Nevertheless, there appears to be little dispute that vulnerabilities should be disclosed in order to reduce the risks to information systems and to minimize or halt related malicious activity.

Vulnerability disclosure is not a simple process. Affected vendors must carefully consider multiple factors in light of the nature of the vulnerability at hand. When, for example, is the appropriate time to disclose? How much information about the specific vulnerability should be revealed? Should the disclosure be made to the public all at once time, or should certain entities, such as core internet service providers, receive some advanced notification before the vulnerability is fully disclosed to the public?

If vendors disclose vulnerabilities to customers and the public before fixed software or workarounds are developed and available, customers may face the risk that a miscreant will attempt to exploit the vulnerability. If the vulnerability affects systems in widespread use within critical infrastructures, the risk to national and economic security is magnified.

It is against this daunting background that a vendor, who seeks the best way to disclose a vulnerability to the public, must carefully determine how to best minimize the risks associated with the possible exploitation of that vulnerability during and after the disclosure process.

Cisco's Vulnerability Disclosure Process: Cisco has long recognized the importance of disclosure of vulnerabilities, with a history of vulnerability disclosure dating back over a decade. In 1997, Cisco formally established its Product Security Incident Response Team ("PSIRT"), an internal, dedicated team of technical experts that handle the full scope of activities associated with handling vulnerabilities. The team members are selected carefully and are part of Customer Advocacy, Cisco's customer support organization.

When the PSIRT team receives a report of a vulnerability, it researches the exploitability and scope of the vulnerability, and then attempts to fully characterize it. The team treats reported vulnerability cases very confidentially in order to minimize the risk of accidental leaks. Once the PSIRT team has made an initial assessment that a true vulnerability exists, it contacts the Cisco development teams who are responsible for providing a fix. While the fix is in development, the team will then determine whether and what kinds of pragmatic workarounds might be devised and deployed.

Once the fix and the workarounds are developed and tested, the PSIRT team carefully documents the vulnerability. Many factors are taken into account for the published web description of the vulnerability. Enough information needs to be provided for affected customers to protect their systems; nevertheless, certain key details are often withheld to prevent miscreants from rapidly developing malicious exploits.

The PSIRT team is responsible for the time when the associated security advisory and fixed software are posted on Cisco.com. The team provides information to other Cisco organizations who respond to inquiries from customers and others about the disclosed vulnerability. After the publication of the advisory, the PSIRT team solicits feedback from affected customers and researchers to help monitor the effectiveness and viability of the fix provided. Based upon such ongoing post-disclosure monitoring, the team will continue to periodically post updates to the security on Cisco.com until the threat of an exploitation of the vulnerability has been successfully thwarted.

Mechanisms that Exist for Protecting Systems

Web traffic and mail are the two most common transport mechanisms for viruses and worms. Code Red, Slammer, Blaster, Nachi, SoBig, and most other worms and viruses entered networks through services that were specifically permitted. A typical network is expected to permit e-mail, web browsing, and news service between internal and external systems. Understanding this opportunity, attackers seek obscure ways to send their own data into the network mixed in with the normal traffic destined for web browsers, e-mail clients, and news readers.

There are many defense mechanisms designed to help protect networks and host systems from the threat of viruses, worms, and direct attack. However, such mechanisms are limited, both by their design and by the skill set of the person who configures them.

Properly configured and maintained firewalls can protect a network from an attacker trying to directly access the network from the outside. However, a firewall used alone lacks defense in depth, and cannot reliably protect against all viruses and worms. In a common scenario, a firewall administrator may inadvertently open up access to a much larger range of network traffic than suspected while trying to solve an independent network communication problem through the firewall. When such attacks are active, it

may only take moments for malicious traffic to travel past the firewall and infect vulnerable systems on the other side.

Virus Protection Programs: Virus protection programs exist for mail servers, the powerful computers which receive our mail from the Internet and sort them out for delivery to the end users. These programs regularly allow infected mail through because they have to sort through too many large messages and they can't handle the load. Even the most powerful servers depend on the e-mail administrators to keep their virus definition files up to date. For some large enterprise networks, it can take hours for the administrators to update the mail servers to catch the latest e-mail-borne virus, and that can only occur after the anti-virus vendor makes the latest definition files available.

Network Intrusion Detection Systems: Many network and system administrators rely too heavily – sometimes solely – on network Intrusion Detection Systems (network IDSes). These are devices that scan the traffic on the network and compare it against "signatures", distinctive patterns of common attacks. IDSes are very good at detecting unusual traffic, but they should be part of a larger system for securing networked resources and not relied upon as a sole means of protection. Many newer viruses and worms are better able to disguise themselves as perfectly legitimate traffic, increasing the difficulty of identifying them as malicious traffic. An IDS is a warning device, providing indication that further action needs to be taken. IDSes do not block attack traffic alone. Appropriate actions must follow to respond to the threat.

Other Network Security Tools: Other tools exist that are not yet commonly deployed that may provide some added network security protection. These include tools that monitor the "flow" of traffic that travels across the network, and which then pass such flow data to a device like those made by Arbor Networks or Riverhead Networks for further analysis. These devices look at the larger view of network traffic and report anomalous behavior such as greatly increased traffic to a specific Internet port number, a typical pattern for a new worm. In a similar vein, Cisco offers a program called CSA, Cisco Security Agent to detect inappropriate attempts to access files and other

unexpected system actions on a single computer or server. Unlike antivirus programs which wait for a specific, known virus to start attacking, these programs can alert system administrators before a new worm or virus can be identified, "fingerprinted", and announced. These host-based solutions are not yet widely deployed, but do appear promising.

Today, there is no one right solution. Vendors, end users, and system administrators can benefit from further education regarding the value of multiple tools to effectively combat these threats. Presently, the only available solutions are reactive and time-consuming. Each class of tool presented above prevents some form of attack, and new tools are constantly in development.

Keeping Systems Up to Date

The deployment and ongoing maintenance of software patches, upgrades, and workarounds incur significant time and manpower costs. A network administrator may be faced with upgrading software or implementing workarounds on thousands of devices. In many cases, the administrator can not afford to simply reboot the entire network, particularly if the resulting interruption will interfere with mission-critical services. In addition, some service providers and similar organizations may have service-level agreements (SLAs) in place with their own customers who require pre-notification of maintenance. Some "customer's customers" require maintenance to be confined to certain times of the day or strictly limit the number of maintenance events in a time period. Testing of software upgrades can be very time consuming. The demands on testing requirements have increased dramatically in the brief history of the Internet, some of it mandated by industry requirements, telecommunications regulations, and SLAs. Most network operators must contend with a myriad of testing requirements. Some testing is self-imposed because many networks are unique, and in today's competitive network services marketplace, no one can afford to deploy new software without fully testing it in their own unique environment.

Another major issue is the potential complexity arising from even the simplest of vulnerabilities. Some vulnerabilities are resolved with a "one-line" change to the source code. Others might force a near-complete redesign of the system. Such severe changes can have a dramatic impact on the confidence level of the customer, particularly in mission-critical situations. Therefore, system and network administrators are very conservative about changing a working system, particularly to defend against a vulnerability that may have not been developed into a malicious exploit.

Vendors can help. The more painless they make the upgrade, the more likely users will implement deploy it. The less impact a patch has on a working system, the more likely the customer is to trust vendor. For example, most fixed releases for Cisco products are part of the normal development cycle, and contain additional fixes for a wide variety of problems plus the addition of new features. In some cases, where it is pragmatic to do so, Cisco releases software containing **only** the exact fixes necessary to close the hole. In some cases, customers are more confident with running such software and may validate it rapidly using a reduced testing regimen. The result is that fixed code can be deployed much earlier, minimizing the customer's exposure to risk.

Vendors make every effort to release stable code, but often vulnerabilities are being fixed under severe time constraints. A miscreant might know about the problem and may be developing an exploit. At the same time, the product vendor is racing against the underground, trying to release a patch before the new exploit – possibly a new worm or virus – is released. Sometimes there's simply not enough time to test every possible combination of the new code if the vendor seeks to release the fix before the miscreants start attacking. Other times, a well intentioned researcher may indicate willingness to publish a vulnerability in a month. From the vendors view, a month might be enough time to write the fixed code, but not enough time to exhaustively test the fixed software.

The timing of vulnerability disclosure requires a fine balance of speed and quality. A blanket set of rules that define a timeline or a requirement may inappropriately force a vendor to release a fix before the software has been fully tested. If a software patch

turns out to be unstable, end users and system administrators may decide not to upgrade. Yet, by not upgrading, the networks then may become susceptible to an exploitation of the vulnerability.

Ultimately, all of these solutions depend on humans to react and respond in a timely matter. Anti-virus software is useless against newer worms and viruses if the signature database has never been updated. Anomaly-detection systems such as network-based and host-based IDSes cannot react by themselves – someone has to respond to the alarms and mitigate the purported threats. Systems are not patched if security advisories go unread, or the fixed software is not downloaded and deployed, or customers can't figure out where to find security advisories and related fixed software, or researchers and customers can't determine how, and to whom, to report a vulnerability.

Summary

Our global infrastructures are interlinked in complex, sometimes little-understood ways, and some of the dependencies are surprising.

The global nature of the Internet means that no single country or industry group can address vulnerabilities in isolation. Success in this arena requires public-private cooperation. Our common goal is to reduce vulnerabilities, mitigate risks, identify strategic objectives, and share sound information security practices.

An example of a cooperative industry effort is underway within the National Infrastructure Advisory Council (NIAC). NIAC has a current effort to develop vulnerability disclosure guidelines that should prove useful for discoverers, vendors, users, and governments. The NIAC will also make specific policy recommendations for the President. The study will be available after it has been delivered to the President in the coming months.

Testimony of Greg Akers, September 10, 2003

National and economic security are forever intertwined. The industry leaders I work with understand their role and are willing to do their part to protect our national and economic security. I would like to thank you, Mr. Chairman and other subcommittee members, for inviting me here today. I am happy to answer your questions.

Mr. PUTNAM. Our next witness is Philip Reitinger. Mr. Reitinger is a senior security strategist with Microsoft Corp.'s Trustworthy Computing security team. The Trustworthy Computing Initiative at Microsoft is a long-term, company-wide initiative to promote the values of reliability, security, privacy and business integrity.

Before joining Microsoft in January 2003, Mr. Reitinger was the Executive Director of the Department of Defense's Cyber Crime Center and the Deputy Chief of the computer crime and intellectual property section of the Criminal Division of the Department of Justice.

Mr. Reitinger is the former Chair of both the Group of Eight's High Tech Subgroup and the National Cyber Crime Training Partnership's Vision and Policy Committee.

We look forward to your testimony, Mr. Reitinger, and you are recognized for 5 minutes.

Mr. REITINGER. Good morning, Chairman Putnam, Ranking Member Clay. My name is Philip Reitinger, and I am a senior security strategist with Microsoft. I want to thank you for the opportunity to appear here today.

Before joining Microsoft, as the chairman noted, I was the Deputy Chief of the Computer Crime and Intellectual Property Section of the Department of Justice, the Executive Director of the DOD Cyber Crime Center and the Chair of the G8 Subgroup on high tech crime. Thus, for some time I have been concerned with criminal threats to people and networks and with the challenges posed by responding to cyber crime.

Responding to those challenges requires effective action on many fronts. Today, I would like to make four main points.

First, Microsoft is committed to continuing to strengthen our software to make it less vulnerable to attack. Microsoft under its Trustworthy Computing Initiative is working to create software for its customers to secure by design, secure by default, and secure in deployment. We are designing and writing software more securely, making it more secure out of the box and making it easier to keep secure.

These goals are becoming ingrained in our culture and are part of the way we value our work. Even so, there is no such thing as completely secure software. Therefore, and second, when security vulnerabilities are found, the process is to provide customers with the necessary fixes; they must be easy, fast and transparent so the customers can stay secure in deployment.

For example, we have included an automatic update feature in recent Microsoft operating systems. My written testimony describes the additional steps we are taking in more detail. Our goal is to make patch application easier so that every single customer can readily have the appropriate patches installed and have his and her information protected.

Third, as the recent past so amply demonstrates, criminals will use computer networks to launch attacks, and we must be able to respond quickly and effectively. In the case of Blaster, before the worm was released, Microsoft built, tested, and delivered a remedy for the vulnerability which Blaster exploited. We then undertook extensive measures to advise customers of the need to apply the patch immediately and how to protect their systems.

After the release of the worm, our efforts continued and expanded and included launching our Protect Your PC campaign, which included providing security information to users through publications such as the New York Times and the Washington Post.

In parallel with these public efforts, we undertook an in-depth review postmortem to understand how to reduce the likelihood of similar vulnerabilities occurring in the future. We carried out a full scrub of the subsystem that contained the vulnerability. And today we are releasing an additional patch fixing vulnerabilities we found. We know that security is a process of continuing improvement, and we are committed to that process.

Fourth, as a society, we need to devote increased resources to law enforcement personnel, training, equipment, and capabilities to prevent and investigate cyber crime. Technical and management solutions cannot prevent every cyber attack. Determined and sophisticated cyber criminals develop new means to break into systems and harm the on-line public.

In this case, Microsoft worked closely with law enforcement efforts to identify the individuals or organizations involved, and created and released Blaster interference.

But despite the best and laudable efforts of the United States and international law enforcement communities, it is still very hard to identify and prosecute cyber criminals worldwide. For example, the computer forensic challenges facing law enforcement are daunting. The amount of data that is stored electronically is growing exponentially, and law enforcement's technical capability to extract critical evidence from this massive electronic data is falling rapidly behind.

In conclusion, the Blaster worm and its variants were serious criminal attacks against the owners and users of computer networks. These attacks merited and received equally serious attention from Microsoft, the government, our customers, and our partners. In the end, a shared commitment to reducing cyber security risk and a coordinated public and private response to cyber security threats of all kinds offers the greatest hope for promoting security and fostering the growth of a vibrant, trustworthy on-line world.

Thank you.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Reitinger follows:]

Statement of Philip Reitinger

Senior Security Strategist, Microsoft Corporation

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

Hearing on "Worm and Virus Defense: How Can We Protect Our Nation's Computers from These Serious Threats?"

September 10, 2003

Chairman Putnam, Ranking Member Clay, and Members of the Subcommittee: My name is Philip Reitinger, and I am a Senior Security Strategist with Microsoft Corporation, reporting directly to our Chief Security Strategist. Before joining Microsoft, I was a Deputy Chief of the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice, the Executive Director of the Department of Defense Cyber Crime Center, and the Chair of the G8 Subgroup on High Tech Crime. For some time I have been concerned with criminal threats to people and networks in the United States and around the world, and with the challenges posed in preventing, detecting, deterring, and responding to cyber crime. Accomplishing that mission – and make no mistake about it, it is a mission – requires effective action on many fronts, including improving the security of software, developing and implementing better security policies and practices, strengthening user awareness, understanding more about the threat at a tactical and strategic level, and enhancing law enforcement's capabilities.

Therefore, I want to thank you for the opportunity to appear today to share our recent experiences with the Blaster Worm and to discuss our ongoing initiatives related to software and platform development, patch management, and computer user education that we believe will, over time and in combination with effective law enforcement action, help to reduce the number of successful attacks on computer software.

I would like to begin by providing you with a brief chronology and overview of how we responded to the Blaster Worm that was launched this summer. I will next describe our commitment to Trustworthy Computing, and how it is reflected in our software and our research and development efforts. I then want to discuss the steps under way to streamline our processes for assisting computer users to implement patches to

vulnerabilities that are discovered in software. Finally, I will discuss the importance of an effective law enforcement response in order to deter and investigate cyber crime.

Microsoft's Response to the Blaster Worm

Like many commercial software vendors, we have developed a security response program – Microsoft's is state of the art. I want to use a few moments to describe our Blaster response.

- In the Spring of 2003, a customer reported that an application was not working properly. A review by Microsoft developers revealed a buffer overrun in a core communication protocol in Windows that did not initially appear to be remotely exploitable. The bug was entered into the bug database for repair, and further review indicated that it could be remotely exploitable under certain conditions. Before the repair was made and distributed broadly, an external security researcher reported finding this buffer overrun. The Microsoft Security Response Center (MSRC) investigated this second report and concluded an immediate patch was required.
- Over the next two weeks, the MSRC led an intensive effort to build, test, and release a remedy for the vulnerability. Patches were developed for seven different versions of Windows, some in twenty-five languages. Our teams worked around the clock to ensure that the patches' quality was commensurate with their installation on millions of customers' computers worldwide.

- On July 16, we released the patches and a pair of accompanying security bulletins – one for technical audiences and one for non-technical audiences – that described the vulnerability, the risk it posed to customers' computers, and the steps they should take to protect their systems. We categorized the vulnerability as "critical" – our highest rating. Within the first week of release, well over a million customers either visited the web-hosted bulletins or received them directly via email through our free Security Notification Service.
- Because of the risk the vulnerability posed, we undertook extensive measures to advise enterprise customers of the need to apply the patch immediately. We conducted conference calls with the Information Sharing and Analysis Centers (ISACs) for several industries, collaborated on an advisory issued by the CERT Coordination Center, briefed industry analysts, and through our account teams contacted customers personally and encouraged them to take appropriate steps to secure their software. We followed up this effort by sending a community bulletin to over a million of our Microsoft Certified Professionals and partners. Throughout this process, we worked closely with partners in the intrusion detection and anti-virus communities, including the Virus Information Alliance (VIA).
- We also worked to advise the general public of the situation. In conjunction with the publication of the bulletins, we contacted reporters from major news outlets such as the Associated Press and worked with trade and business reporters from various publications. We sent an alert to every customer who

had contacted our Product Support Services unit for any reason during the previous several months, and we sent another alert to subscribers to our Virus Alert system. Finally, we collaborated with the Department of Homeland Security (DHS) on its July 24 release of an advisory.

- On July 25, an organization called XFOCUS published instructions for exploiting the vulnerability. Recognizing that the release of these instructions raised the risk of attack, we contacted our customers again and undertook a second round of outreach efforts, including collaboration with DHS on an updated DHS advisory, to both technical and non-technical audiences.
- On or before August 11, the Blaster Worm was released. The worm, which used the security vulnerability as the method by which it spread, rapidly infected computers worldwide and disrupted normal operations in many networks. In response, we immediately triggered our emergency response teams – which included Premier Support Services and Microsoft Consulting Services personnel – and mobilized our security teams from across the company.
- Over the next two weeks, thousands of our employees worked around the clock to provide customers with information about the worm (and its subsequently released variants), its effects, and the best ways to protect vulnerable computers and restore infected ones to normal operation. We published and continually updated web pages with information for non-technical audiences, and provided guidance to ISPs and hosting companies about how to protect home user and small business customers. We also

dispatched field engineers to many customer sites to provide hands-on assistance; augmented our Technical Support staff with hundreds of software engineers when customer call volumes exceeded our normal capacity; and developed tools to assist customers in identifying and protecting vulnerable computers. Throughout this period, we worked closely with anti-virus companies to share the latest and most accurate information about Blaster and its variants. In addition, we alerted leading consumer organizations and placed full-page ads in major newspapers to give consumers information about protecting their computers.

- Early in our analysis of the worm's behavior, we determined that infected computers would flood the Windows Update web site with data beginning on August 16, in an apparent effort to disrupt its operation and prevent customers from obtaining security patches. Microsoft developed a solution that provided uninterrupted support for our customers.
- Beginning with the worm's appearance, and continuing even now, Microsoft worked closely with law enforcement authorities' efforts to identify the individuals or organizations who created and released Blaster and its subsequent variants. On August 29, the FBI arrested Jeffrey Lee Parson, whom we understand is alleged to have created and released a Blaster variant. As I will discuss later, effective law enforcement is a critical element in any successful effort to protect people and networks from cyber crime.
- In the wake of Blaster, Microsoft has embarked on a proactive effort to help consumers become better protected in the future. On August 21, we launched

the Protect Your PC campaign, urging that customers take three steps to improve their security: install and/or activate an Internet firewall, stay up to date on security patches, and install an anti-virus solution and keep it up to date. We launched this campaign with a nationwide advertising campaign directing customers to the www.microsoft.com/protect web site, which serves as the focal point for the campaign.

- We also undertook an in-depth review and post-mortem, to understand how the vulnerability occurred and how to reduce the likelihood of similar vulnerabilities occurring in the future. After discovery of the vulnerability, we took steps to improve our tools, and carried out a full scrub of the subsystem that contained the vulnerability. In addition, recognizing that software development is a human process that cannot be made perfect, we also have been taking and are planning to take additional steps to improve our customers' protection against future vulnerabilities. I will discuss some of these steps below.

Microsoft's Commitment to Trustworthy Computing

The efforts I have discussed to respond to the Blaster Worm attacks and the efforts I describe below to achieve further advances in software development practices and in patch management are integral aspects of Trustworthy Computing, which is our top priority and involves every aspect of the company. The focus of Trustworthy Computing is on four core pillars: security, privacy, reliability, and business integrity.

The security pillar is most relevant for today's hearing. Under this pillar, we are working to create software and services for our customers that are Secure by Design,

Secure by Default, and Secure in Deployment, and to communicate openly about security.

- "Secure by Design" means two things: writing more secure code and architecting more secure software and services.
- "Secure by Default" means that computer software is secure out of the box, whether it is in a home environment or an IT department.
- "Secure in Deployment" means making it easier for consumers, commercial and government users, and IT professionals to maintain the security of their systems.
- "Communications" means sharing what we learn both within and outside of Microsoft, providing clear channels for people to talk to us about security issues, and addressing those issues with governments, our industry counterparts, and the public.

The Trustworthy Computing goals are real and specific, and this effort is now ingrained in our culture and is part of the way we value our work.

Although we are working hard, much remains to be done. We accept our responsibility to create ever more secure software. Part of our commitment to Trustworthy Computing is in developing innovative, new technology that will make users less vulnerable to a cyber attack. One key piece of that work is the Next-Generation Secure Computing Base (NGSCB). This is an on-going research and development effort to help to create a safer computing environment for users by giving them access to four

core hardware-based features missing in today's PCs: strong process isolation, sealed storage, a secure path to and from the user, and strong assurances of software identity. These changes, which require new PC hardware and software, can provide greater protection against malicious software attacks.

Our Efforts to Streamline the Patch Process

To be clear, the best way to streamline the patch management process is to create software that is Secure by Design and Secure by Default, thus reducing the number of vulnerabilities in code and reducing the need to patch. That said, there is no such thing as completely secure complex software, regardless of development model or platform. Therefore, when security vulnerabilities are found, the processes to provide customers with the necessary fixes must be easy, fast, and transparent, especially as we move to an environment where an increasingly smaller percentage of computers are managed by IT professionals. We are attacking this issue under the "Secure in Deployment" pillar of the Trustworthy Computing initiative.

The steps we are taking include:

- Improving our testing of patches to ensure patch quality.
- Working to ensure that each patch is uninstallable, so a rollback is possible if deployment raises an unanticipated issue, such as adversely affecting a legacy application. We are reducing the number of installers used in order to simplify the administrator's burden and make patch installation more efficient.
- Ensuring that patches register their presence on the system – and producing improved scanning tools – so a user can quickly determine if his or her machine is patched appropriately.

- Making our security patch releases more predictable. Absent a public exploit, we regularly release patches on Wednesdays, thereby allowing our customers to prepare for them.
- Avoiding reboot of the computer where practicable, as our customers are more likely to apply a patch more quickly, if server availability will not be interrupted.
- Combining patches into service packs to avoid the need for multiple downloads and installations.
- Producing specific technology, such as Software Update Services and Systems Management Server, so enterprises can download patches, test them in their unique environment, and then easily deploy them.
- Including the AutoUpdate feature in recent Microsoft operating systems, which can automatically download updates and then either install them as scheduled or request permission from the user to do so.

In sum, our goal is to make patch application easier, so that every single customer can readily have the appropriate patches installed and their information protected.

The Importance of Effective Law Enforcement

However, as I mentioned above, technical and management solutions cannot prevent every cyber attack. Determined, innovative, sophisticated hackers and cyber criminals will always develop new means to break into systems and otherwise harm the online public, just as criminals in the physical world break into cars, stores, and homes and commit other crimes such as fraud. When criminals steal or attack online, public authorities need to be able to find and punish them. Despite the best and laudable efforts

of the U.S. and international law enforcement communities, and periodic successes, it is still very hard to identify and prosecute hackers, virus writers, and cyber criminals worldwide. As a result there is insufficient deterrent to this criminal activity.

There are specific steps we can and should take.

First, we need increased funding for law enforcement personnel, training, equipment, and capabilities to prevent and investigate cyber crime. Our government's hard-working officials – including those within the Departments of Justice, Homeland Security, and Defense – are often short-staffed, under-funded, under-trained, and lack state-of-the-art technology used by cyber criminals. Increased funding is needed to give the government an edge over those whom they investigate. Additional resources may also help the government coordinate with international, state, and local law enforcement in preventing and investigating cyber crime.

Lacking these additional resources, law enforcement is trapped in a perpetual and accelerating race against hackers and virus writers, as hacker tradecraft and tools are improving faster than are law enforcement's investigative techniques. Investigations are also made considerably more difficult by the increasing scope and diversity of the Internet – the "needle in a haystack" analogy far understates the problem. And the computer forensic challenges facing law enforcement are daunting – the amount of data that is stored electronically is growing exponentially, with law enforcement's technical capability to sort through a mass of electronic data to timely find critical evidence (including clues to the location and identity of an attacker) falling rapidly behind. We must solve these problems while simultaneously ensuring that law enforcement

capabilities and investigations are tailored to intrude on the privacy of law-abiding citizens as little as possible.

Second, because cyber security is inherently an international problem with international solutions, greater cross-jurisdictional cooperation among law enforcement is needed for investigating cyber-attacks. Cyber attackers and criminals easily cross borders, as demonstrated by the many attacks, including recent worms and viruses, which were international in scope. Enhanced law enforcement assistance, collaboration, and information sharing across local, state, and international borders, along with laws in every country criminalizing cyber attacks, are vital for law enforcement to prevent and investigate cyber attacks.

Conclusion

The Blaster Worm and its variants were serious criminal attacks against the owners and users of computer networks. These attacks merited and received equally serious attention from the government and from Microsoft, as well as from our customers and our partners in the computer infrastructure and software industries. In the end, a shared commitment to reducing cyber security risks and a coordinated response to cyber security threats of all kinds — one that is based on dialogue and cooperation between the public and private sectors — offer the greatest hope for promoting security and fostering the growth of a vibrant, trustworthy online economy.

Thank you.

Mr. PUTNAM. Our next witness is Vincent Gullotto. Mr. Gullotto is the vice president of research for AVERT, the Antivirus Emergency Response Team, the antivirus research arm at Network Associates. For roughly half a decade, Mr. Gullotto has been involved in the day-to-day operations of AVERT labs. Located throughout 18 cities around the world, AVERT labs is responsible for the research and discovery of computer viruses, including Melissa, Love Letter, and Bubble Boy. Are you the ones who name them?

Mr. GULLOTTO. Yes.

Mr. PUTNAM. So Bubble Boy was your idea?

Mr. GULLOTTO. Yes.

Mr. PUTNAM. Under his leadership, the AVERT group is credited with the discovery of the first wireless virus, Phage.

Mr. Gullotto has developed the concepts and initial designs for a number of AVERT service and solution offerings, including programs such as WebImmune, the world's first Internet virus security scanner that resides on the Web, as well as the AVERT Malware Stinger, a stand-alone program designed to supplement antivirus programs.

Mr. Gullotto, we are looking forward your testimony and delighted to have you here.

Mr. GULLOTTO. Chairman Putnam, Ranking Member Clay, thank you very much for inviting me today to join the subcommittee and speak on behalf of a very serious problem we are having today, computer viruses and the evolving threat that we see going forward.

As you stated, AVERT is an antivirus research arm for Network Associates. We are a global organization working 24 hours a day, 7 days a week, discovering new viruses and naming new viruses as well. In addition to this work, we also work participatingly with 27 other companies in the antivirus discussion network [AVED], and on a day-to-day basis work closely with law enforcement as often as possible to identify and investigate cyber attacks and cyber crime.

While my written testimony submitted for the record provides a recent history of computer viruses and worms, as well as descriptions and impacts of the most well-known ones, I want to focus my testimony on three important trends and followup with three recommendations.

First, Mr. Chairman, governments and companies have become more porous. In recent years, companies have opened their enterprise to serve customers better and improve productivity of employees and suppliers. Enterprises are becoming electronic sponges. They are porous, and it's getting harder to tell the inside from the outside.

Second, reported vulnerabilities are on the rise. We have already heard the number is on the increase, and they will continue to increase as time goes on. The bad news is that this new threat, worms which exploit these vulnerabilities, can cause even greater damage than more traditional worms and viruses.

And third, the speed of cyber attacks has accelerated dramatically with a shrinking window of exposure between vulnerability and exploit. Attackers exploit a window of exposure between when the vulnerability is announced and when all the infected systems

can be patched. Today, the time is short. It's a matter of hours in some cases or a matter of weeks and days. In the future we expect it to become even shorter.

Once a vulnerability is announced, we may see an exploit within a matter of hours, and that vulnerability exploited in such a way that, within minutes perhaps, that exploit will be around the world. Denial of services like CodeRed and Nimda caused spread around the world in hours. And, of course, earlier this year we saw Slammer infect thousands of machines in just under 3 minutes.

How do we protect ourselves from computer viruses, worms, and other attacks? One key way is by moving from a traditional reactive approach to a security approach where proactive intrusive protection is used. What's required to close the window of exposure is protection in depth, including solutions that can be deployed before a new threat appears in the field, so that the threat simply bounces off the company's defenses.

Intrusion prevention looks for anomalies, and attack signatures in response, by preventing the attacks from permeating the network or system defense. An intrusion prevention system protects a network from attack while providing breathing room and response time for analysts to fix vulnerabilities.

There are other steps we can take to make a real difference. While my written testimony has recommendations for enterprising consumers, for the sake of time, I would like to share three with the policymakers today.

First, we believe policymakers should embrace Cyber First Responders. We respectfully suggest the cyber security industry, including those at the table here today, represent Cyber First Responders in our battle against the attacks on the information infrastructure. Policymakers, in addressing the threat of viruses, worms, and other attacks, should turn to these Cyber First Responders, who can provide policymakers with real-time, non-hype, accurate information about the nature of threats and the extent of the impact.

Second, policymakers should continue promoting a culture of security, a term used both in the United States and abroad, and here today as well. We believe the policymakers around the world can embrace this concept by continuing to shine a light on cyber security. Policymakers can support public awareness efforts such as the Stay Safe Online campaign; the government industry's collaborative bodies, including the Partnership for Critical Infrastructure Security; focus government leadership, such as the government's high-ranking single point of command that we hope will be announced soon; and real-time information sharing organizations, including the various vertical sector information sharing and analysis centers.

And finally, policymakers should increase support of long-term cyber security research and development.

In addressing our cyber-security challenges, research and development plays a key role in allowing us to stay ahead of the next generation of attacks. Yet many experts in industry and academia agree that we are at risk of dropping the ball on critical R&D needs.

In the area of R&D, we recommend that policymakers authorize the study of our Nation's critical infrastructure vulnerabilities, increase R&D funds to leading departments and agencies for collaborative R&D with industry and academia, refocus collaborative R&D on longer-term challenges and improve coordination amongst government-funded R&D projects.

As we commonly know in the industry, security is not a place to get to; it is an ever-evolving challenge. We urge the subcommittee and Congress to continue to put energy into addressing the cybersecurity challenge, and in return, I pledge to you our company's commitment to work with government and industry and academia to develop solutions to these urgent needs.

I thank you for the opportunity to testify this morning and look forward to your questions.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Gullotto follows:]

Testimony of Vincent Gullotto
Vice President
Anti-Virus Emergency Response Team (AVERT)
Network Associates, Inc.

Before the
House Committee on Government Reform
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

"Worm and Virus Defense: How Can We Protect the Nation's Computers From These Threats"

September 10, 2003

Chairman Putnam, Ranking Member Clay and Members of the Subcommittee, I want to thank you for inviting me to testify today on the important topic of protecting our nation's computers from the threats of viruses and worms. My name is Vincent Gullotto, and I am Vice President of the Anti-Virus Emergency Response Team (AVERT) at Network Associates, Inc. I am honored to be invited to be here today to join my distinguished colleagues from government and industry alike to discuss with this Subcommittee the current state of virus and worm attacks on our nation's computers, systems, networks and infrastructures. I also look forward to making recommendations for how we can protect ourselves from these rapidly increasing threats.

With headquarters in Santa Clara, California, Network Associates, Inc. is a leading provider of intrusion prevention solutions for network and systems security. Network Associates is comprised of three product groups: McAfee Security, which offers desktop and network anti-virus and security products; Sniffer Technologies, which provides network availability and network protection; and Magic Solutions, which develops service management solutions. In addition, we are home to Network Associates Laboratories, widely recognized as a world leader in information security research and development. Our customers range from the largest of enterprises, universities and governments, to medium and small businesses, to millions of consumers around the globe.

Network Associates is committed to working with consumers, business, academia and government to identify emerging cyber threats, risks and vulnerabilities, and to develop solutions that can be distributed rapidly and widely. As a company, we participate in a number of collaborative organizations. We are Founding Members of the Partnership for Critical Infrastructure Security, the Online Identity Theft Coalition, the Organization for Internet Safety and the National Cyber Security Alliance's Stay Safe Online campaign. We co-chair the Department of Commerce's International Outreach Subcommittee of the Communications and Information Sector Working Group. And we actively participate in the cyber-security efforts of a number of trade associations, including the Business Software Alliance, the Information Technology Association of America, the Alliance for Network Security and the Security Research Alliance. Each of these entities is devoted to building partnerships between government and industry to improve the way we prevent, identify, respond to and recover from cyber attack.

I am here today to share with you my perspectives as head of the Anti-Virus Emergency Response Team (AVERT), the anti-virus research arm of Network Associates. Located in 18 cities worldwide, AVERT is responsible for the research and discovery of computer viruses, including Melissa, LoveLetter and Bubbleboy, the first virus written that could infect a user by simply previewing an e-mail. The AVERT group is also credited with the discovery of the first wireless virus, Phage. Like its name implies, the Anti-Virus Emergency Response Team serves as a front-line in the fight against viruses and worms.

In order to fight the constantly evolving threats, AVERT cooperates with our colleagues in the anti-virus field. Three years ago, ten leading anti-virus researchers, including three from AVERT, created the Anti-Virus Emergency Discussion Network (AVED; http://www.aved.net) as an effort to thwart the rapidly spreading viruses. There are now 64 participants in this organization from 27 different anti-virus companies around the world. As you can imagine, this spirit of cooperation plays a significant role in protecting all of us from the threats from viruses, worms and other attacks.

In addition to AVERT's work with customers, partners and other researchers, we are committed to working closely with law enforcement, security and intelligence organizations to assist in their efforts to fight cybercrime worldwide. Stopping viruses and worms at their source by identifying and prosecuting their authors is a key part of our mission to help solve the computer virus problem.

Overview

Mr. Chairman, I'd like to commend you and the Members of this Subcommittee for your leadership in holding today's hearing. As the last few weeks have shown us, the impact of viruses and worms on our computer systems is rising dramatically. The computer virus infection rate has grown to speeds never before seen. And the damage caused by such attacks is escalating.

As the recent electricity blackouts in the northeastern part of the United States have shown, we as a nation are more interconnected than ever before. Our electrical systems, our telecommunications, our information technology, our financial services, our transportation and our emergency services all rely upon each other to operate effectively, and a hiccup in one can cause significant cascading effects on the others.

As we examine how to protect ourselves against malicious cyber-attacks, such as worms and viruses, it is important to view the issue not simply as an effort to avoid the annoyance of a flood of e-mails or a crashed system. The challenge must be viewed in the broader context of the potential vulnerability of our critical infrastructures. During the Slammer virus outbreak, major U.S. banks experienced widespread ATM outages, a major airline canceled or delayed flights, and a large U.S. metropolitan area lost its 911 emergency services. As a result of the more recent outbreaks, a major airline lost the use of its computer system for reservations and check-in, already cash-strapped state and municipal governments wasted numerous resources to address their network problems, and colleges and universities faced the risk of students bringing virus infected computers to school and crashing or slowing down the school's network infrastructure.

The threats are real, and the consequences of inaction or insufficient action are significant. But this is not a doomsday scenario. Attacks such as those that occurred over the last several weeks provide an important wake up call to governments, industries, and consumers. We must not be complacent; we must act. To ensure the stable, efficient and predictable operations of our critical infrastructure, we must consistently try to stay one

step ahead of the attackers, and we must implement technologies to proactively protect our systems rather than simply react as the damage is being done. The technological sophistication of the attacks may be growing, but so is the technological sophistication of the solutions. We will continue to innovate to stay one step ahead.

Viruses and Worms: Definitions and History

Before describing steps we can take to protect ourselves from worms, viruses and other attacks, I believe it would be helpful to provide a short background on the history and development of viruses and worms. With this background, I will present a series of trends that bring us to today's (and tomorrow's) security challenge.

The common belief is that anything bad happening on a computer is caused by a virus. Not so. Viruses are programs that spread. A traditional virus spreads by jumping from program to program. Worms, a term recently in vogue, generally spread from machine to machine. But a worm is a type of virus. Separately, a Trojan—as its name might imply—acts in ways that the user would not expect, but the author intended.

Deliberate exploitation of security vulnerabilities in software is increasingly common and plays a large role in recent virus and worm activity. Automated worms that spread without human interaction will usually involve such an exploit. Personal firewalls can be used to hide exploitable software from being vulnerable to the Internet. Anti-virus and intrusion prevention software can block many of the known exploits. But to really eliminate the possibility that a vulnerability will be exploited, one has to update to the latest version of the deficient software.

For most of us, paying attention to information security started out of necessity, to combat a nuisance. To see how that has changed, let me give a brief history of viruses.

Pre-1995: Boot and Com Infectors (Small-Scale Damage)

Until 1994 or earlier, viruses like Michelangelo, Brain and FORM were spread by floppy disks being passed from user to user, and were relatively easy to stop. IT staff usually had weeks or even months between the time a new virus was discovered and when it might show up on the network.

The cost of these viruses was minimal, as they were mostly produced manually as proofs of concept to expose a vulnerability while showing some proficiency of programming. The number of people who could do it, and had the motivation to do it, was fairly small.

1995 to 1998: Macro Viruses (Large-Scale Nuisance)

From 1995 to 1998, the most prevalent viruses were macro viruses, the most common being the Word macro virus. Viruses like Concept, Cap and Laroux exploited scripting languages in common applications, and were spread by users working on the same file. We started to see more costs associated with these viruses, both because of their scale and

because there were more destructive viruses being written. The justification for this was sometimes given as activism against large companies by virus writers who suggested that any kind of homogeneity bred a lack of computer security.

1999-2000: Mass Mailers (Servers Clogged by a Double Click)

In 1999, we saw the rapid rise of the e-mail-aware virus in which servers could be clogged by a double click. The first was Melissa, which hit on Friday, March 26, 1999. We have continued to see minor variations on this theme for the past couple of years, including viruses like Loveletter (i.e., the Love Bug), and a virus named after Anna Kournikova. Each of these mass mailer viruses used Visual Basic script to read the user's address book and then e-mail copies of itself to other users, who then opened the e-mail because it came from someone they knew.

This new method meant viruses started spreading more quickly than ever before. The network downtime associated with these viruses and others like them made them much more costly—at $29 billion, almost three times as expensive as the past four years and in half the time.

A variation of this type of mass mailing threat, the Bubbleboy virus, was discovered by AVERT in November 1999. In this variation, a user did not need to "click" an attachment to get infected, as the virus would launch upon the user simply opening the message itself.

2001 to Present: Worms (No User Required)

All of this was a precursor—a training ground, if you will—for the kind of threats we saw in 2001, when we began to see a new kind of virus writer and a new kind of virus: the Internet worm. Internet worms don't require a user action to spread. Once let loose, they crawl through known holes to infect new systems as fast as they can. Code Red and Nimda are two of the most severe worms to date, but our McAfee AVERT researchers have seen hundreds of examples of these worms since that time. Most significantly, with these attacks the Internet shifted from being a method for distribution to a target itself, as we saw when Code Red slowed Internet traffic by as much as a third around the globe.

Because there is no user to act as a gating factor to stop the spread of an Internet worm, the reaction time for individuals, companies or governments to protect their network has narrowed to minutes. This new threat fundamentally changed the nature of the required response to virus threats. And in response, we need to rethink the way we fight them.

Today and Tomorrow – The Compound/Unified or Blended Threat

Today, and in the months and years ahead, we face a compound/unified—or blended—threat. The term and the actual date of the first threat of this type might be argued, but what can't be argued is its ability to cause havoc.

Blended threats are designed to prey on vulnerabilities discovered in operating systems or applications. This type of attack has become prolific over the past two years, and the

threat will continue. Blended threats thrive on vulnerabilities, and there will be more vulnerabilities discovered in the months and years to come. Therefore the quest must be to find ways in which threats like CodeRed, Nimda, Klez, Slammer, and Lovsan can be stopped before they cause any damage.

Let me make one final comment on these threats and others like them. The threats listed above have many commonalities and many individual traits that have made them high impact threats throughout the past three years. They all have followed the evolution of the technology we've created to make using the Internet a faster and more convenient mode of doing business, sharing data, and communicating. Because there is common ground on which they operate, there is common ground on which we can protect each other from these and future threats.

To help understand the true workings and impact of the most well-known viruses and worms, please see **Appendix A: "Well-Known Viruses and Worms."**

Viruses and Worms: Trends

Most companies have deployed security technologies to protect their IT infrastructure. Yet, they remain vulnerable because the threats are rapidly evolving, and up until now most security technologies have been reactive rather than proactive in nature. There are several reasons why reactive response is no longer sufficient.

The speed of attacks has accelerated tremendously. Well-known "denial of service" worms like Code Red and Nimda spread around the globe in a day or less. Recently, the time required for such attacks to be felt globally has shrunk tremendously. On January 25, 2003, SQL Slammer infected over 5,000 servers around the world in UNDER THREE MINUTES. The time it takes for an attack to be created to exploit a vulnerability is shrinking. When a vulnerability is discovered in an operating system or an application, and a patch is released, it takes time to deploy the patch to vulnerable systems. Attackers exploit a "window of vulnerability" between when the vulnerability is announced, and when all affected systems can be patched. Today, the time it takes for a threat to be created to exploit a vulnerability is about three weeks. This is the time between when the vulnerability exploited by Lovsan was announced and when Lovsan itself was discovered. This timeframe is down significantly from the six months that elapsed before CodeRed took advantage of the vulnerability in Microsoft IIS. Three weeks is not a long time to prepare for something when, like many corporate information security professionals, you have the responsibility for making sure 50,000 machines are not vulnerable.

There are theories that one virus can cripple the Internet in 15 minutes. How long might it take for someone to create a multi-tiered approach that combines a mass-mailer and a DDoS (Distributed Denial of Service) attack? The future might present us with a situation

where only a few days or few hours are available for us to prepare for such an attack after a vulnerability has been announced.

Companies and governments are becoming more porous. In recent years, companies have opened their enterprises to serve their customers better and improve the productivity of employees and suppliers. They reach out to their customers to deliver service or information through web based applications. They deliver work flexibility to their employees, with wireless networks and telecommuting arrangements. And over time, we've evolved to a highly mobile, interconnected society where most professionals will have a network connection "at their fingertips" that can interact automatically with proximity networks and the corporate extranet. Enterprises are becoming electronic sponges. They are porous, and it is getting hard to tell the "inside" from the "outside."

Reported vulnerabilities are on the rise. The bad news is that the new threat—worms that exploit vulnerabilities—can cause even greater damage. One exploited hole can have major impact. In every virus wave we've seen before, we had a single application or process that was being exploited in slightly different ways – first booting from a floppy, then Word, then Outlook. In this wave of Internet-borne worms, we're seeing an explosion in activity that exploits multiple holes in multiple applications. There's no one application or process you can watch to make sure you're secure. It's about multiple layers of defense at all times.

Protecting Against Viruses and Worms: Technology and Practices

Protecting ourselves from current and new forms of threats requires both technology and improved security practices. In technology, we must look toward a new way of thinking: proactive security. In practices, we must look toward current and emerging best security practices.

Through Technology: Proactive Security

Today, IT staff is fighting a battle that appears hard to win. Attacks get in through firewalls. Systems cannot be patched fast enough to be hardened. Intrusion detection systems generate mountains of data. The result is a growing "window of vulnerability" between the appearance of a new threat and a company's ability to deploy a fix.

What's required in order to redress the balance and close the "window of vulnerability" is protection in-depth, including solutions that can be deployed before a new threat appears in the field so that the threat "bounces off" the company's defenses.

Intrusion prevention can fundamentally change the equation through precision blocking of known and unknown threats in real time. Intrusion prevention looks for anomalies and attack signatures and responds by preventing the attacks from permeating the network or system defense. An intrusion prevention system protects a network from attack, while providing breathing room and response time for analysts to fix vulnerabilities.

Intrusion prevention is about identifying threats to your business and blocking them, helping enterprises, small businesses and government agencies assure the availability and security of their desktops, application servers and web service engines.

Through Practices: Best Security Practices

In addition to technology, best security practices also play a key role in protecting ourselves from the threats of viruses, worms and other attacks. The following are a few key elements of best security practices.

First, it is important to know your critical assets. It is vital to know what they are, where they are, how critical they are to your mission, and what their vulnerabilities are.

Next, it is important to understand and assess the threats you face. What kinds of threats do you face from hackers, industrial spies or an enemy state? Where is the threat most likely to come from – Inside2Outside, Inside2Inside, or Outside2Inside? And, how severe can the impact be?

Third, it is important to know your protection needs and the defense tools–firewall, intrusion prevention, anti-virus, vulnerability assessment, access control–that help you address those needs. It is also critical to know how these tools fit in with your security strategy.

Finally, it is imperative to address the cyber threat challenges systematically. This includes:

- A layered defense with multiple methods of protection including signature based and behavioral based detection
- Integrated response to attacks
- A proactive approach that involves blocking attacks, not merely detecting them
- Well defined security policies with real enforcement

Recommendations for Action

While this testimony covers a number of areas, I respectfully would like to make a series of key recommendations. These recommendations fall into three audiences: government policymakers, enterprise users and consumer end users.

Government Policymakers

While ensuring strong cyber-security and protecting against virus and worm attacks is primarily a technology and practices issue, we believe that there is a role for government policymakers. We offer three recommendations.

1. Look to Cyber-Security Industry as "Cyber First Responders"

In Homeland Security discussions, much focus (rightfully so) is on the critical role of First Responders. We respectfully suggest that the cyber-security industry represents "Cyber First Responders" in our battle against attacks on the information infrastructure. Policymakers, in addressing the threat of viruses, worms and other attacks, should turn to these Cyber First Responders to craft public policy that embraces technology as a fundamental part of the solution. Cyber First Responders, in a collaborative partnership, can provide policymakers with real-time, non-hyped, accurate information about the nature of the threats and the extent of the impact. And in crafting potential public policy, policymakers should be cautious to do no harm to a highly innovative and responsive cyber-security industry.

2. Promote a "Culture of Security"

Policymakers and industry representatives in the U.S. and abroad have discussed the need to promote "a culture of security." We believe that policymakers around the world can embrace this concept by continuing to shine a light on cyber-security. Policymakers can support public awareness efforts (e.g., the Stay Safe Online campaign), government/industry collaborative bodies (e.g., the Partnership for Critical Infrastructure Security), focused government leadership (e.g., a high-ranking single point of command), and real-time information sharing organizations (e.g., the various vertical sector information sharing and analysis centers). Finally, policymakers can explore the business models and drivers under which industry operates. Where there are gaps between national infrastructure needs and business drivers for action, policymakers can explore "carrot" and "stick" (or incentive and requirement) approaches for industry to take action.

3. Support Cyber-Security Research & Development

In addressing our cyber-security challenges, research and development plays a key role in allowing us to stay ahead of the next generation of attacks. Yet, many of the R&D challenges go beyond ROI formulations for individual companies. Government has played and will continue to play a critical role in supporting longer-term R&D. In the area of R&D, we recommend that policymakers:

- Authorize a study of our nation's critical infrastructure vulnerabilities
- Increase R&D funds to leading departments and agencies (e.g., NIST, DARPA, HSARPA, NSA, NSF and others) for collaborative R&D with industry and academia
- Refocus collaborative R&D on longer-term challenges, realizing that true ROI may not occur until years 3 or later of a project
- Improve coordination among government-funded R&D projects

Enterprise Users (Commercial, Government and Education)

Enterprise users, whether large corporations, small or medium-sized businesses, government agencies or educational institutions, often experience the brunt of the attack from worms and viruses. While policymakers can develop an environment supportive of strong cyber-security, enterprise users can take steps to minimize risks and block attacks. We offer two recommendations.

1. Implement a Proactive Security Strategy

As discussed earlier, the traditional approach to cyber-security has been a reactive strategy, through updating virus definition files and detecting when attacks take place. Technology has evolved and now allows enterprise users to become proactive. With the delta between the discovery and the subsequent exploitation of vulnerabilities shrinking dramatically, we recommend that enterprise users embrace intrusion prevention to ensure that their networks and businesses stay up and running even when they are under attack.

2. Educate Your Users

As part of an intrusion prevention strategy, enterprises should focus resources on training and educating their internal end users. Whether acting maliciously or, more often, simply being the victims of social engineering tactics, enterprise end users can often be an organization's greatest vulnerability. With mandatory, ongoing training and education classes on cyber-security, end users—executives, employees, or students—can close the "window of vulnerability."

Consumers

Finally, consumers at home also play a key role in stopping the damage caused by viruses, worms and other attacks. Often home systems, without the support of a dedicated IT department, are the most vulnerable to these attacks. To help consumers close this hole, we make two recommendations:

1. Protect Thyself

Just as we learn to take steps to protect our physical home through locking doors and windows and screening strangers, consumers at home also should take the time to learn a couple fundamentals of cyber-security. Without requiring consumers to become cyber-security experts, we should continue to provide consumers with easy-to-understand resources on how to protect themselves through anti-virus products, personal firewalls, and other technical measures. In addition, these resources should include important best practices, such as deleting or scanning attachments and recognizing suspicious e-mail messages. The Stay Safe Online website (www.staysafeonline.info) is a good start.

2. Demand Strong Cyber-Security of Others

Consumers also can play a role through their purchasing power. We recommend that consumers prioritize security features when selecting an Internet Service Provider (ISP), even if it means paying an additional fee for extra layers of security. We also recommend that consumers inquire about the cyber-security of their online transactions, whether with banks, retailers, on-line auctions, government services, health care providers or others.

While taking steps to implement the above recommendations will not ensure total protection from viruses, worms and other attacks, these actions will have a significant effect on the impact of these attacks. Policymakers, enterprise users and consumers each can play a role in protecting ourselves and our infrastructures from cyber attack.

Conclusion

Mr. Chairman, the challenge before us today is significant. The speed of cyber attacks has accelerated dramatically. Companies and governments have become more porous. Reported vulnerabilities are on the rise. And vulnerabilities are being exploited more frequently and faster. In order to fight the challenges of tomorrow, we must not rely on the tools of today.

But there are steps we can take to make a real difference. Policymakers can embrace Cyber First Responders, support a culture of security and support critical long-term research and development. Enterprises can shift toward proactive security through intrusion prevention while educating their users in security essentials. And consumers can learn security fundamentals and demand them of those with whom they do business.

As we commonly know in the industry, security is a journey, not a destination. We urge your Subcommittee and Congress to continue putting energy into addressing the cyber-security challenge. In return, I pledge to you our company's support to continue to work with government, industry and academia to develop solutions to these urgent needs. I repeat what I said earlier, the technological sophistication of the attacks may be growing, but so is the technological sophistication of the solutions. We will continue to innovate to stay one step ahead.

I thank you again for the opportunity to testify here today, and I look forward to answering any questions the Subcommittee may have.

Appendix A: Well-Known Viruses and Worms

LoveLetter

The LoveLetter virus is noted as the most costly virus incident ever. It was the first of its kind and the most widely distributed virus making use of the .VBS extension. Much of the cost attributed to this virus is due to the virus's effect of overwriting all files bearing the extensions .vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .mp2, and .mp3.

The virus initially arrived as an e-mail with the following characteristics:

Subject: **ILOVEYOU**
Message: **kindly check the attached LOVELETTER coming from me.**
File attachment: **LOVE-LETTER-FOR-YOU.TXT.vbs**

Who could resist opening such an e-mail that played with the hearts and emotions of all? This virus is probably one of the best socially engineered viruses ever released. Social engineering, or the ability for one to craft a virus so that most anyone will open it, has become almost an art in some respects. Some social engineering messages work and some don't; a lot of the success comes down to timing and just the right amount of curiosity. The most impacted were small businesses, unable to maintain the proper backups and heavily dependent on their website operations. The combination of the wide spread of the virus and damage to files that were not backed up accounts for the exorbitant damage figure of over $8 billion worldwide.

CodeRed

CodeRed was a perfect example of a worm. It was also what is known as a file-less virus. There was nothing to click or grab on to. Thus, it moved through the Internet with relative ease, as there was almost nothing from a security software perspective that could stop it. CodeRed travels using the same networking protocol and port as normal Web traffic and took advantage of an existing vulnerability in Microsoft IIS (Internet Information Server) application both versions 4 and 5. Thus the solution to this problem was as simple as fetching the patch available from Microsoft (http://www.microsoft.com/technet/security/bulletin/MS01-044.asp) or any subsequent cumulative patch.

The damage attributed to CodeRed is much less than that of LoveLetter. Part of this is because some of the machines were subsequently taken over by Nimda, to which the cleanup cost was attributed.

Nimda

Nimda is a blended threat. It makes use of at least five different attack modes, including backdoors left by previous viruses. Coming close on the heels of other viruses, without much time for its development, we believe Nimda was created by a team of people, not just a solitary virus coder. But what Nimda demonstrated is that if we don't protect

ourselves, our own machines could be universally commandeered and used against us in a matter of hours or minutes.

An estimated quarter million to a half million machines were overcome by the virus. And many of those machines were well-known websites or mail servers for medium to large companies. In total, over 50,000 important Internet sites were infected.

SQL Slammer

Slammer is another perfect example of a worm. It exploited a vulnerability in the SQL Server Databases. This threat was responsible for knocking out ATMs and other important websites around the world that use the SQL technology. This threat —while significant—only targeted servers and did not have a major impact on Internet traffic. It did not hit home users' systems or most corporate desktops. So while its costs were high, a major portion of the machines that use the Internet were spared...at least for the time being.

SoBig

The recent SoBig virus has been the most prolific virus to date. The virus is responsible for spreading upwards of half a billion e-mail messages on the Internet. SoBig is similar to all of the other mass-mailing e-mail viruses, though it forges the sender address on its e-mails. As a result, the virus fools victims into believing it might have come from someone they know. By making it hard for friends to contact the infected party, the virus is able to reside on systems until it reaches its built-in self-termination date.

Lovsan (a.k.a Blaster)

Part of the major impact of the Blaster worm was its focus on home users. The worm attacked a port that is generally not useful to the average home user. While the impact of the worm is significant, the truly alarming lesson learned is the dramatically shortened timeframe we saw between the announcement of the vulnerability and the successful release of a worm targeting that vulnerability. How can we prevent such attacks like Blaster? A default setting that does not allow traffic on similar ports would inhibit such attacks.

Appendix B: Biography

VINCENT GULLOTTO
Vice President
AVERT (Anti-Virus Emergency Response Team)
Network Associates, Inc.

Vincent "Vinny" Gullotto is the vice president of research for AVERT (Anti-Virus Emergency Response Team), the anti-virus research arm of Network Associates. For roughly half a decade, Vinny has been intimately involved in the day-to-day operations of AVERT Labs.

Located throughout 18 cities worldwide, AVERT Labs is responsible for the research and discovery of computer viruses, including Melissa, LoveLetter, Bubbleboy, the first virus written that can infect a user by actively opening an attachment in e-mail. Under his leadership, the AVERT group is also credited with the discovery of the first wireless virus, Phage.

Vinny's creation of the AVERT research group was driven by a business model that puts customer service first. The model allows his group to focus on having the best virus detection rates in the industry. His involvement includes the design and development of McAfee's anti-virus scanning engine and virus detection technology, working round-the-clock to maintain and manage AVERT's global research capabilities.

He also works on an ongoing basis with other global members of the anti-virus community in detecting viruses. Vinny has developed the concepts and initial designs for a number of AVERT service and solution offerings. They include programs such as WebImmune (www.webimmune.net), the world's first Internet virus security scanner that resides on the Web; as well as the AVERT Malware Stinger, a stand-alone program designed to supplement anti-virus programs by going beyond traditional technology available today, serving as a test bed for components to be included in Network Associates' McAfee VirusScan engine.

When it comes to virus research and virus outbreaks, Vincent Gullotto plays an integral role in advising and alerting the public through various outlets, further enabling the public to take necessary precautions to protect themselves.

Vinny can be found giving insight regularly in technology trade publications and on technology centric Web sites. He has been instrumental in providing insight and perspective about virus events such as Melissa, LoveLetter, and CodeRed on major news networks that include CNN, ABC World News, CBS, ZD Net, CNET and IDG.

Vinny has spoken around the world, serving as a primary spokesperson for Network Associates and AVERT at press conferences, sales conferences, customer and non-customer conferences. He has also shared his vast knowledge of the anti-virus field by presenting at several security conferences, including COMDEX, Networld+Interop, the E-Security Expo , Sector 5 Security Conference and the SANS Institute conference.

Additionally, Vinny has addressed and directed a session at EICAR (European Institute for Computer Anti Virus Research), covering e-commerce and security risks associated with purchased made on the Internet.

He recently spoke at the CampIT Expo in Chicago and at the Forum ICT Conference in Rome Italy where he addressed today's threats, where they evolved from and what may be seen in the future.

Prior to AVERT, Vinny held a director and Board of Director's position at a privately held US firm that pioneered and developed cost-efficient, PC-based automated attended voice mail systems. Vinny holds a Bachelor of Science degree in Business Administration from the University of Phoenix.

Appendix C: Disclosure of Sources of Government Funding

September 8, 2003

The Honorable Adam Putnam
Chairman, Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
House of Representatives
B349-A Rayburn House Office Building
Washington, DC 20515

Chairman Putnam:

This letter serves as financial disclosure in accordance with the rules of the House of Representatives governing non-government witnesses and federal grants and contracts. I submit this disclosure in advance of my appearance before the Subcommittee on September 10, as a witness for the Subcommittee's hearing on computer viruses and worms.

The products and services of Network Associates, Inc., including McAfee Security, Sniffer Technologies and Magic Solutions, are used extensively throughout the Federal government. Network Associates has contracts with defense and civilian departments and agencies alike, including but not limited to the Departments of Defense, State, Justice, Treasury, Interior, Health and Human Services and Education as well as many independent agencies, commissions and administrations.

In addition, Network Associates Laboratories conducts federally-funded advanced security research for the following organizations:

- Defense Advanced Research Projects Agency (DARPA)
- National Science Foundation (NSF)
- National Institute of Standards and Technology (NIST)
- Army Research Labs (ARL)
- Air Force Research Labs (AFRL)
- Advanced Research & Development Activity (ARDA)

If you or a member of your staff has any questions about these sources of funding, please feel free to contact me.

Sincerely,

Vincent Gullotto
Vice President, AVERT
Network Associates, Inc.

Mr. PUTNAM. Our next witness is John Schwarz. Mr. Schwarz is president and chief operating officer of Symantec, responsible for Symantec's product development, incident response, sales, support, professional services, marketing and partner relationships.

Previously, Mr. Schwarz was president and CEO of Reciprocal, Inc., which provided comprehensive business-to-business secure e-commerce services for digital content distribution over the Internet.

Prior to taking the lead role at Reciprocal, Mr. Schwarz spent 25 years at IBM. Most recently, he was general manager of IBM's Industry Solutions Unit, a worldwide organization focused on building business applications and related services for IBM's large industry customers. He has held numerous development positions within IBM, including vice president of development for the company's Personal Software Products Division where he was responsible for IBM's OS/2 Warp and PCDOS product management systems development.

As the vice president of application development for the Software Solutions Products Group in Toronto, he was responsible for the development of worldwide product management of IBM's application development and distributed data base products business.

We look forward to your testimony, Mr. Schwarz. Welcome to the committee.

Mr. SCHWARZ. Chairman Putnam, Ranking Member Clay, thank you for the opportunity to provide testimony on this important and timely subject, and thanks for that long personal history.

Today, much of our economy depends on critical assets that are in digital form. We are a society that relies more and more on information technology; yet, we have not taken the steps to protect those assets to the same degree that we have our physical assets.

The cyber world is maturing and is a pervasive structure in organizations, as well as at home. It is also becoming more complex and vulnerable. The attacks are faster, less predictable, and more severe. The number of opportunities for exploitation also continues to grow at a rapid pace. In fact, it is estimated, on average, 250 new software vulnerabilities are discovered each month. These vulnerabilities are being exploited faster and more aggressively than ever. Again, on average, the industry is identifying 450 new viruses each month, with some very colorful names, with many reaching pretty high severity levels.

We saw the transition to "blended threats," with worms like Code Red and Nimda containing multiple attack mechanisms. These blended threats, that combine the attributes of a traditional virus and a hack attack, typically resulting in a massive denial of Internet services, are truly the biggest threat we face today in the cyber world. Leveraging the vast number of new vulnerabilities, and through the introduction of destructive payloads, rapidly propagating blended cyber attacks, represent a substantial future risk.

The next generation of attacks, known as "flash threats," have the potential to infect massive portions of corporate networks or the entire Internet within minutes or perhaps even seconds. The recent Blaster or SQL Slammer worms saw hints of these types of threats. As you've already heard, SQL Slammer infected 90 percent of the initially vulnerable systems in approximately 10 minutes.

Such threats require entirely new proactive systems to stop them. There's no reactive remedy that will ever be fast enough to protect against threats spreading at these speeds.

The interconnectivity of individuals, businesses, and government organizations is becoming ever more pervasive and continuous through always-on broadband connections. As a result, there is a vast, unmanaged computing capacity that is potentially available to the cyber criminals to launch massive denial-of-service offensives against selected targets or perhaps against the Internet as a whole.

Let me discuss some actions that we believe can improve our cyber security. First, awareness and education often mentioned today.

Educating our consumers, our businesses, the operators of critical infrastructure as well as all levels of government, on the importance of protecting our systems is essential. We need a broad awareness campaign that reaches out to all users of the Internet. At the least, all users need to be made aware of the value of firewall and automatically updated antivirus technology, like putting seat belts in cars. The remote or wireless connected worker is becoming more prevalent and can unknowingly open up an otherwise secure community network to potential vulnerabilities and attack through unprotected wireless connections in the home or in the office.

At the enterprise and organization level, the issue of IT security has for too long been left to the security administrator, or the CIO. This needs to change. Cyber security needs the top leadership of the business or government organization. As an example, the recent corporate governance legislation known as Sarbanes-Oxley significantly strengthened the rules pertaining to the financial management of all businesses. However, the legislation makes no mention of the importance of protecting the information systems that produce the data used in the financial management processes. Only when cyber security is treated with the same attention as the protection of physical and financial assets can we enable the necessary cultural change and focus enough attention and resources to truly address the cyber threat.

Second, cyber crime. We saw the arrest of Jeffrey Lee Parson for writing a variant of the Blaster worm, but we have yet to find the bigger culprits, the original authors of the recent flurry of new attacks. We need to realize that protecting the Internet is really a global issue, one that requires better international cooperation. We need more and higher quality resources for law enforcement to work on computer forensics, and we need cooperation from government and industry to assist prosecutors in building cases.

We require more harmony in cyber crime laws. Perhaps the Council of Europe's cyber crime treaty is a good starting point. Governments and industry should reach across borders when appropriate to share information on cyber crime cases, best practices, threats and vulnerabilities, in order to gain a measure of prosecution success and early warning of potential attacks.

The industry information sharing and analysis centers, the ISACs, can be a nucleus of that initiative. There should be a confidential, single point of contact in government so that the experts can communicate at a peer level at times of major cyber attacks.

And again the recently announced cyber warning information network will be a good base for this exchange.

Third, research and development; as mentioned earlier flash threats may be wreaking havoc in the near feature, and we must be more productive in our cyber security practices, focusing on behavior blocking technologies, faster threat identifications to event correlation, real-time vulnerability scanning, and automated software patch deployment.

Given the shrinking time from discovery to exploit, much new research and development needs to take place which even the combined resources of the industry cannot deliver in time. The government and academia must join this effort with incremental funding, proactive recruiting of the best talent and highly focused, jointly funded precompetitive projects.

Finally, audit and risk analysis: Security is not a static issue and, thus, requires regular assessments of systems and vigilance on the part of the IT managers, and for that matter, all users of the Internet. I commend the committee for its efforts to enact programs like FISMA, which require annual assessments of government systems and also require actions to improve the protection of those systems.

The committee's oversight in this area is invaluable. This is not just something that government should do, but all enterprises, large and small, should be encouraged to follow this example of regular security assessments. Critically, though, we need thorough and timely remediation of any audit findings. The current performance of most organizations, government and industry alike, falls well short of desired levels.

In closing, let me issue this challenge to the industry, government, and individual users. We must take cyber security more seriously and we must do it together. Aware and compliant users are the best defense against most cyber attacks. Most importantly, we all, as individual users of the Internet, need to do our part to protect cyberspace. Experience shows that effective implementations of security solutions cost in the range of 6 to 8 percent of the overall IT budgets. Few corporations or government departments have allocated adequate levels of funding to this critical need. It is time that we put our resources to work to minimize the risk of a serious disruption of our national cyber infrastructure.

Thank you and I look forward to your questions.

Mr. PUTNAM. Thank you very much, Mr. Schwarz.

[The prepared statement of Mr. Schwarz follows:]

Statement of John Schwarz
President, Symantec Corporation
House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
Hearing on Worms, Viruses and Securing Our Nation's Computers"
September 10, 2003

Chairman Putnam, Ranking Member Clay, Members of the Subcommittee, thank you for the opportunity to provide testimony on this important and timely subject: Protecting our nation's computers and our nation's critical infrastructure. A critical infrastructure that is heavily reliant on IT, and one that remains vulnerable to cyber attack.

Today, much of our economy and our critical assets are in digital form. We are a society that is becoming more and more dependent on Information Technology, yet we do not take the steps to protect those cyber assets to the same degree as we have our physical assets.

The cyber world is maturing and is pervasive in organizations as well as at home. It is also becoming more complex and vulnerable. The attacks are faster, less predictable, and more severe. The number of opportunities for exploitation also continues to grow at a rapid pace. In fact, it is estimated that on average, 70 new software or firmware vulnerabilities are discovered each week.

Last year, the number of new vulnerabilites reported was 81.5% higher than the previous year, and that number continues to rise today. We are also seeing an increase in the number of high and moderate severity vulnerabilities. They were reported as 84% higher than in 2001. These vulnerabilities are being exploited faster and more aggressively than ever. On average, we are identifying 450 new viruses each month, with many reaching high severity levels. Perhaps more alarming is the fact that once discovered, the time to exploit a vulnerability is rapidly shrinking. For example, the SQL Slammer worm in January 2003, utilized a vulnerability that was disclosed six months previously in July 2002. The recent Blaster worm utilized a vulnerability that was disclosed in July 2003 – just one month before exploit.

In the past, patch deployment was not as much of an immediate concern. Since fewer vulnerabilities were discovered, patching was less of a drain on resources. If an IT professional had to apply one new patch a quarter versus one a week, less resources, planning and potential down time was required. Additionally, it took longer for a worm or virus to propagate or spread and infect large numbers of systems, so response was much different.

In 2001, this all began to change. We saw the transition to "blended threats" with worms like Code Red, and Nimda containing multiple attack vectors. These blended threats, combine the attributes of a traditional worm and a hack attack, and are the biggest threat we face today.

This acceleration of threats, their severity and the speed of their infection, is evident in the Slammer, Bugbear, and most recently Blaster, and Sobig worms. The ability to respond to these blended threats has become more difficult. A few years ago Symantec's security response team had as much as two days to provide a solution to our customers, today that time has diminished to a matter of minutes.

By leveraging the vast number of new vulnerabilities, the potential introduction of entirely new, and more destructive forms of malicious code and cyber attacks tools represents a substantial future risk.

Looking forward the next generation of attacks, known as "Flash" threats have the potential to infect massive portions of corporate networks and even the entire Internet within minutes or even seconds The recent Blaster or SQL Slammer worms are hints of these types of threats. According to available research data, SQL Slammer infected 90% of the initially vulnerable systems in approximately 10 minutes. Such threats require entirely new proactive systems to stop them as no entirely reactive infrastructure will ever be fast enough to protect against threats spreading at these speeds.

Let me now discuss some actions that we believe can improve our cyber security.

1. Awareness and Education

Educating our consumers, our small businesses, the operators of the critical infrastructure and all levels of government on the importance of protecting our systems is essential. We need a broad awareness campaign that reaches out to all users of the Internet. The growing use of always-on broadband connections by home users and small businesses represents a significant amount of computing power, which left unprotected can be taken over and used as zombie machines to damage our networks and the hinder the commerce and services that flow through them. At the least, these home users should deploy a minimum protection of firewall and anti-virus technology. The remote or wireless-connected worker is also becoming more prevalent and can unknowingly open up a corporate network to potential vulnerabilities and attack through unprotected connections.

Enterprises and government agencies should engage their employees in security awareness programs to ensure better protection of their systems. Whether it's reminding them not to post their passwords on a yellow sticky pad on their computer, or enacting corporate best practices to change those passwords on a regular basis making them difficult to break.

At the enterprise and organizational level, the issue of IT security has for too long been an administrator or a CIO issue. This needs to change. Cyber security needs the attention of the CEO and the boardroom. Only then can we institute the necessary cultural change and focus enough attention and resources to truly address this issue.

2. Cyber crime

We saw the arrest of Jeffrey Lee Parson for writing a variant of the Blaster worm, but we have yet to find the bigger culprits, the original writer or writers of the recent flurry of worms. We need to realize that protecting the Internet is really a global issue; one that requires better international cooperation. First, we need better resources for law enforcement to work on computer forensics, and we need cooperation from industry to assist prosecutors in building cases. Second, we require better harmony in cyber crime laws, the Council of Europe's cyber crime treaty is a good starting point. Third, industry should reach across borders when appropriate, to share information on best practices, threats and vulnerabilities, in order to gain a measure of early warning of potential attacks. The Industry Information Sharing and Analysis Centers or (ISACs) can be that vehicle. Finally there should be a single point of contact in government so that those leaders can communicate at a peer level in times of major cyber attack.

3. Research and Development

Today, industry and government tends to look at the more immediate threats to our cyber infrastructure, rather than a holistic view of encompassing threats of today and tomorrow. It is a view that needs to change. As mentioned earlier, flash threats may be on us in the near future and we must be more proactive in our cyber security practices focusing on behavior blocking and better patch management, including the use of fast, safe and non-disruptive patching. Given the shrinking time from discovery to exploit, we should engage in projects like real-time vulnerability scanning, management and patching and we must do it together in partnership; industry government and academia alike.

4. Audit and Risk Analysis

Security is not a static issue and thus requires regular assessments of systems and vigilance on the part of IT mangers, and for that matter all users of the Internet. I commend the Committee for it efforts to enact programs like GISRA and FISMA, which require annual risk assessments of government systems and also require actions to improve the protection of those systems. The Committee's oversight in this area is invaluable. This is not just something that the government should do, and I would encourage enterprises, large and small to follow this example of regular security assessments.

In closing, let me issue this challenge to industry, government and the individual users: We must take cyber security more seriously and we must do it together.

The increasing prevalence of blended threats and the potential for even more fast-spreading and damaging exploits is a serious threat to our nation's information infrastructure and the economic benefits that we derive from it. We need strong leadership from industry and government to promote awareness and education on cyber security, more resources for law enforcement to investigate and prosecute cyber criminals, strong research and development partnerships to tackle the challenges of future

threats to the Internet, and more vigilance from business and governments by putting resources and support behind a proactive IT security program.

But most importantly we all as individual users of the Internet, need to do our part, to protect cyber space. Experience shows that effective implementations of security solutions cost in the range of 6-8% of overall IT budgets. Few corporations outside of the finance sector, or government departments, have allocated such levels of funding to this critical need. It is time that we put our resources to work to minimize the risk of a serious disruption of our national cyber infrastructure.

Thank you and I look forward to your questions.

Mr. PUTNAM. I appreciate the input of this entire panel, and for the record, this was the worst panel about sticking to the time lines. Usually it's the bureaucrats that go over. But all of you were very interesting with very important information, and we are delighted to have it. I would like to begin with Mr. Reitinger with Microsoft.

You have had a bad month. It has been a tough several weeks at the office. Walk us through what happens when someone, whether they have altruistic intentions, or not-so-altruistic intentions, notifies you of a vulnerability.

And walk us through the process of developing a patch, releasing it; and at what point do you notify the Federal Government, as well as your customers? Could you just walk us through that process?

Mr. REITINGER. Of course, Mr. Chairman.

Ideally, the process works with, if there's an external notification, someone contacting a software vendor, which might be Microsoft or another vendor, who then begins to develop a patch. If the notification is to the vendor, that allows the vendor to work to develop the patch in advance so that the public can be protected.

The patch is developed, and that can be a very intensive process. The Blaster patch or the patch for the vulnerability of the Blaster attack, for example, was done due to a number of different operating systems. The information associated with it had to be developed, I think, in 25 languages. And then that patch is rolled out.

In the case of Microsoft, Microsoft rolls out patches unless there's a public exploit, generally on a Wednesday for predictability purposes, so customers can know it's coming. At that point, we begin to work actively with the community, with our customers, with people in the Federal Government, including the Department of Homeland Security, to make sure that the information about the patch can get distributed as broadly as possible.

Now this next stage is the most critical stage because patch uptake, as we know, is critical. The vast majority of attacks that we have seen over time have been after a patch is released. So the key is getting patch uptake once the patch is released and available.

At some point in that process, as happened in the case at issue, there may be some exploit code that is released and perhaps eventually there is a worm or another set of attacks that are involved.

But that is the big window, to get patch uptake as broad and as deep as possible.

Mr. PUTNAM. Does the Federal Government or a particular agency of the Federal Government receive an early heads-up about a vulnerability that could have serious consequences?

Mr. REITINGER. Typically, because Microsoft's products are distributed so broadly, both within the United States and around the world, the notification is done at the same time; in other words, we released one, we released all. And the reason is, we've got customers around the world, we've got users around the world. You need to make sure you can distribute the information as broadly and as deeply as possible, and so it's generally notification to many.

Mr. PUTNAM. So a vulnerability comes to light, you develop the patch, you put it out there, and then it becomes the responsibility of the consumer to actually patch their system. And in this most recent case, despite the fact that your patch had been out there for

weeks, those who failed to download it had the system go down; and so it reflects poorly despite the fact that you had already provided the solution.

My understanding is, Microsoft is working on some better technology to make those downloads automatic. And are there legal issues, specifically the Computer Fraud and Abuse Act, that might prevent you from making it easier for consumers to patch their systems?

Mr. REITINGER. As the chairman's question indicates, there is already a future in Microsoft operating systems called Auto-Update that can automatically download and prompt the user to install patches. We are currently looking at how we can make that process easier and transparent for end-users so they can more readily have that option available to them, so that more people will in fact use and install Auto-Update.

I think your question about the Computer Fraud and Abuse Act goes to the question of whether we could basically say to our customers, you have to use Auto-Update and we install Auto-Update by default. And the answer to that question is, yes, there are legal problems. Laws like the Computer Fraud and Abuse Act and other regulations, European directives, would prohibit access to an end-user's computer without an access of authority.

We actually need consent to do that, and that is something we want to do. We want to, in fact, not overcome consumers' consent, but empower them and make their consent more effective and make it more able to control their own computer security and privacy.

Mr. PUTNAM. Mr. Akers, what's your take on the whole process of notification? And walk us through your system, if it differs from Microsoft, when you have an issue that may arise that may impact the Federal Government.

Mr. AKERS. It does differ a little bit.

We have been at this process since I have been at the company, and most notably our last restart of the process was in 1997, so it's a continuous process that we undertake. Our intent from the discovery of vulnerability, either internally or externally found, is notification to the customer and remediation so that the customer is not impacted. You also have to remember that in the case of Cisco, the fabric of the Internet itself and the intranets that deploy these patches is, in and of itself, part of the issue we have to consider as a part of the problem, too.

So, for instance, we have to be worried about our ability to distribute patches if the fabric itself does not have integrity. So when we discover vulnerability, we also begin to develop a patch. But we also, at the same time, begin to develop a plan of notification and remediation. These take different shapes depending on the nature of the vulnerability, the technologies that are involved and the issues that are at hand. In some cases, because we have to ensure that we can deploy the released information and the software itself, we may notify critical infrastructure components of the problem so that they can remediate the problem, so we can continue then to work with the rest of the constituent customer base to deploy software release and information.

We look at this on an individual case basis and use processes and policies within the company to determine how to do that, at which time we then go through the process of completing the software build, much as Microsoft indicated they do. Once that is ready, both the plan and the software, we then begin the notification process and remediation process with our customers.

We believe this process, for us, has worked well over the years and believe that it provides the best of both worlds in the context of both protecting the infrastructures themselves, our customers, and making sure that we get the information into the hands of the people that can protect themselves before the information is made available to those that might exploit it and use it for detrimental purposes.

Mr. PUTNAM. Do you have a different notification process for an agency of the Federal Government than you do for an individual customer?

Mr. AKERS. We treat the agency of the Federal Government as if it were part of the critical infrastructure, and we put them in the same structure prioritization as we would any other critical infrastructure. If we determine that a critical infrastructure asset of the Federal Government has a particular or unique circumstance, they would be prioritized accordingly within our scheme.

Mr. PUTNAM. Mr. Reitinger, in the cyber hacker world, everybody likes to pick on Microsoft. As we heard in earlier testimony, everybody gets their merit badges by messing with you all.

You have a tremendous background in law enforcement, as well, so you have seen both sides of this. Are you satisfied with the legal framework that exists today for punishing people who are hackers?

Mr. REITINGER. That is a very good question, Mr. Chairman. I think, in terms of punishing hackers, the answer is mostly yes, because Congress just last year passed an additional law raising the penalties for cyber crime and how that's going to work in practice, the sentencing guidelines associated that are now being developed.

There are two other areas, though, that require examination. One is, is the breadth of penalties enough? Have we criminalized everything we ought to criminalize as opposed to what the amount of the penalty is? And I think that can change over time as new ways to harm people on-line are created.

Secondarily, there is the question of law enforcement's ability to identify and then prosecute people, and that is the point to which my testimony related. It is actually very hard to—as your questions to Mr. Malcolm on the first panel indicated, it is very hard to identify hackers and virus writers and worm writers online, and we need to do what we can to remediate that. And perhaps the biggest way to do that is to ensure that law enforcement has the resources necessary to attack the problem, particularly with regard to training and things like forensics capabilities.

The last element I'll just mention briefly is the international piece. As Mr. Schwarz indicated, it's critical. All cybercrime—not all cybercrime, but almost all cybercrime involves an international element. Even if it's a person in the United States attacking a place in the United States, they will probably pass their attacks abroad. So you typically have an international element in cybercrime. That means that you have to have the same capabili-

ties that you have in the United States created around the world, and things like the Council of Europe Cybercrime Convention, if ratified by countries like the United States and other signatories, could go a long way toward remediating that problem.

Mr. PUTNAM. Mr. Gulloto and Mr. Schwarz, your company's mission in life is to protect your clients' systems from these worms, from these viruses, from these hackers, from malicious code. You monitor this on a 24-hour, 7-day-a-week basis. Do you notice any trends in where these threats come from? Is there a seasonality to the trends? Are there more in the summer than there are during the school year? Do they arise from Eastern Europe or Asia or North America? Could you give us some sense of the landscape of the threat environment?

Mr. SCHWARZ. Let me jump in and obviously allow my colleague to comment. We today monitor almost 1,000 customers' networks around the world and have further some 22,000 real-time scanners placed in strategic points around the Internet around the world. That level of input gives us a pretty good perspective on what is actually happening on the Internet.

First and foremost, the majority of the attacks appear to be originating in the United States, so the thought of somehow being flooded from the outside does not seem to hold true.

Second, the attacks are gaining in, if you will, virility as a result of shared technology, which is very much available in public domains on the Internet. So one of the comments I would make relative to the criminalization of this conduct, ought to think about including the publishing of exploitation methodologies and tools which can then be downloaded by people who don't necessarily have the skill to further the damage of the Internet.

We do not see any seasonality, we do not see any changes in scope as the year progresses or as various political events happen to take place around the world. What we do see is a direct correlation between the rise of always-on broadband connection and the penetration of these attacks around the world as these always-on machines are taken over and used as a base to launch massive further damage. And as my colleague from Microsoft points out, the tracing of these attacks to its origin, given today's technology, is almost impossible.

Mr. PUTNAM. Mr. Gulloto.

Mr. GULLOTO. I concur with a great deal of what Mr. Schwarz said. What I would like to address is a little bit more about the specifics of the origins of the virus-writing activity itself, specifically where viruses may or may not come from. In many cases, as we've heard previously today, and today and I will concur with that as well, it is very difficult for us to specifically state where a virus has been written or where it is originating from. As Mr. Schwarz has pointed out, there is—a majority of the traffic originates in the United States, but we are not completely convinced that the traffic that originates in the United States actually came from the United States.

I'll go to an example of a group called 29 A that exists, from what we understand and what we have researched, in Brazil and in Spain. There is a common language between the two. We have seen even in code where one virus writer will acknowledge another virus

writer for helping create some piece of code together or in such a way in which they were successfully able to take one piece of expertise from one area and the other from another area, get it to work together, and then in many cases it will get out. Now, it gets out deliberately in some cases, or they may post it to a Web site which will ask people to come to that Web site, get that—it could have come from the United States—double-clicked it when they put it on their desktop or began to simply distribute it throughout a network of friends, who then may have double-clicked on it to get it moving in the case of a mass mailer.

The worms are a little more difficult to state, meaning that I may be a virus writer that lives in Belgium—which there is a woman virus writer, her name is Gigabyte, she is 18 years old. She may have written a piece of code at her home in Belgium, but she may have taken it to France, went into an Internet cafe, put in her floppy disk, go to the program, ran it. That program immediately begins to spread. She unplugs the diskette, pays her 5 euro for the hour that she spent on the computer, and she walks out the door. It begins to spread at that particular point in time.

Mr. PUTNAM. Mr. Schwarz, you mentioned that the majority of the attacks originate in the United States. Do you distinguish between probes and attacks, or are they the same term?

Mr. SCHWARZ. We do distinguish among various categories and severities of attacks. And, yes, there are distinctions between probes where people are looking for vulnerabilities or open switches, if you will, open access points, and actual attacks that have been launched to penetrate and cause damage. We see about 175 million such events per day across the spectrum of the systems that we do monitor. Categorizing that volume of data to actually identify specific types of attacks is a bit of a daunting task. What we do with the data is correlate the information from multiple points and attempt to isolate those that have potential for being serious or those that indicate a new type of activity from which we have not been able to defend ourselves previously, and then build defenses based on that new intelligence.

Mr. PUTNAM. And do those probes also mostly originate from the United States?

Mr. SCHWARZ. The total traffic that we see—and again, I agree with Vincent's point relative to the actual pinpointing of the origin of the code, but the total traffic volume still is to some 75 or 80 percent originating in the United States. What we see is countries that have a very large prevalence of always on connections, like Korea and Japan, ranking very high, perhaps beyond the size of their population, but that may be simply spoofed addresses targeting those countries as a way to launch attacks, but not originating there.

Mr. PUTNAM. One of the concerns that we have heard, particularly with the reference to the virus that went silent today, was shut down as of today, is that it is an attempt by these code writers to learn, to explore the system for a finite period of time, and then before it could necessarily be reacted to, it goes down so that they are learning and essentially applying that knowledge toward developing the better or the perfect virus or the perfect worm. Could you comment on that? Anyone.

Mr. GULLOTO. I would agree that is certainly a possibility. We have seen behavior like this for quite some time. Approximately 3 years ago Mr. Hale, who had testified a little bit earlier, and I were on a committee, if you will, that looked at a threat called Leaves. It was an Internet worm. And at first it had looked to be rather a meek worm, but as we did more and more analysis of it, it became very complex in what it was that it did. It looked to be something that perhaps someone had created to see what would happen if they released it, what data could it gather, where could it go, what could it do so that they could then in turn go ahead and create another threat of such a nature to then have it go further. The good news was that person was actually arrested. And so I don't have any idea what happened to that person, but I know that there was an arrest in that case.

Now, we could take a look at other such threats and also concur that there is some education process. We could look at one specific factor in a threat to say this might be what they are looking to see works or doesn't work. The SoBig virus now is one that you mentioned, is one that's in its fifth to sixth generation, meaning it is multiple family members. There have been other variance of SoBig that have spread quite far as well, and the commonality amongst each variant is that it has an extension, which is PIF. And in many cases, when we see a new extension be exploited, it is an opportunity for all virus writers to learn to see if it will become successful or not, because if it is successful, others will use that same extension, knowing fair well that most computer users, which we would probably look to more toward the consumer user, but then again end users, within an environment would not understand.

We've spent a great deal of time educating people in the past couple of years about how not to click on anything that has a VBS extension. Well, we got them to understand that. Those viruses seem to have gone away. However, PIF looks a lot like JIF. JIF is not necessarily a file that can be infected. People double-click on it every single day and e-mail. No problems. They get to see something, it's great. It's a misunderstanding. Virus writers probably understand this, use it to educate themselves to see what else they can plant that will become successful.

Mr. PUTNAM. Mr. Schwarz, did you wish to add anything to that?

Mr. SCHWARZ. I think this is a very accurate description of the actual state of the technology used by the virus writers. Again, I would like to stress the importance of dealing with Web sites that actually publish this information, which are then shared among a community of people that perhaps do not have the skill to create the original varieties, but can adapt and cause additional damage.

One other thought which I would like to leave with the panel or with the committee is that many of the worms that perhaps or the viruses that are perhaps the most threatening are not those that achieve the notoriety of a SoBig. They are very visible because of the traffic they generate, but perhaps a low-profile-type worm or Trojans that have been placed in strategic points in the network in systems that are very critical to a business or the national infrastructure that can be triggered somewhere down the road with a subsequent worm or subsequent attack, causing a disruption of service or causing deletion of data, or causing, in fact, just a flow

of information to an entity that might wish to observe what is going on.

So we need to not observe just those attacks that cause the service very large volume issues, but need to be looking for low-profile, potentially, in fact, more insidious and dangerous worms than those we have seen to date.

Mr. PUTNAM. Mr. Akers and Mr. Reitinger, recognizing that there will never be a perfect code, what can software designers do to develop more secure codes, more secure systems as the abilities of the bad guys, the black hats, continue to improve? What efforts can we take to get better, more secure systems?

Mr. AKERS. I think there is actually two things that we are both doing, and we need to continue to do, as an industry. Education is a big part with our software developers. We teach our software developers that are coming out of academia today to develop software based on the function required at hand, and we don't teach them to be mindful of the issues around security that might provide vulnerabilities and subsequent exploits.

There are a number of programs out there. There are centers of excellence that are part of a program at the National Security Agency. There are a number of other venues by which we acquire information about how to do good quality, secure software engineering. And we need to continue to educate our software engineers and academia how to do those things and for those that are out in practice today, and continue to do what we are doing, which is bringing that information directly to them so that as they develop a product initially, they are mindful of the issues that we are dealing with from a security standpoint today. This is something that's going to be an ongoing process.

The second thing is continued testing. And that is something that I know that most of the vendors here and most of the vendors across the community are doing more today than we ever have. We internally have programs, we externally have programs, and we are going to continue to reinforce our ability to simply look for and test for those vulnerabilities that we might be in a position to uncover that we can then mitigate prior to the time of an exploit.

I want to kind of piggyback on the last question a little bit, too. As we look at this issue around vulnerability yielding an exploit, the other thing we can do is we could watch the testing of some of this exploit code. I can't think of a vulnerability that has been disclosed that at some point along the line somebody didn't turn the knob to see if it was more interesting than maybe the vulnerability seemed at the time the vendor talked about it. And if we start seeing these kinds of things, government and private sector should be able to identify those instances and come together to take a look at what the miscreants might actually be doing, and then start thinking about how to thwart the attempts that they may make at those particular vulnerabilities going forward.

Mr. PUTNAM. You mentioned the education and then its importance for your software designers. But these miscreants, as you've referred to them, or script kiddies are more intellectually driven; it is a game. Some people do crosswords, some people try to break into systems, and then the more malicious types. Now, don't script kiddies grow up to work for the Microsofts and Ciscos of the world?

Mr. AKERS. Not knowingly, in my case. We take a very dim view of that activity. But, no. Typically it's difficult to even distinguish between the activities of the script kiddies and the more orchestrated and well-organized, funded, and otherwise notable engagements. As a matter of fact, understand that it wouldn't be out of the realm of possibility that those more well-developed organizations and entities could take advantage of the behavior of the script kiddies to accomplish what they want to accomplish. So education of software engineers is a key part of it. And what you generally find, or at least what we generally find, is they do have a—once educated, they do maintain and have a clear understanding of the issues and want to do the right thing.

I think as was said earlier, it's almost viewed as being patriotic to make sure that when we're providing critical infrastructures, we're doing it with the highest degree of quality and security that we possibly can. And our developers take that to heart much like the rest of the developers in the community do.

Mr. PUTNAM. Mr. Reitinger.

Mr. REITINGER. Mr. Chairman, let me answer that question in two parts, first what software companies can do, and then turn to the education points.

What software companies can do is have a robust software assurance process. Conduct code reviews before software ships, use independent test teams, do threat modeling, make sure they train their developers. Use automated tools to test for security, and seek third-party certifications such as the common criteria. This is something that companies like Microsoft and other software companies do.

They need to conduct robust after-actions when vulnerabilities do occur to figure out what went wrong and how the process can be fixed going forward, because security is really a destination as opposed to an end. Or, excuse me, is really a process as opposed to an end.

Software companies need to make security easier to do so that the software's secure out of the box and it's easier to maintain going forward. So there's a whole software assurance and software support process that can ease the burden and help solve the problem.

With regard to education, there are a number of components of that. One is educating users about how they can secure their systems. That is the focus of a lot of government efforts and the Microsoft Protect Your PC Initiative.

There is also the component of the ethical outreach to kids, which was the subject of your present talk. How do we stop—how do we make young folks, if you will, not do the sorts of things that some of them are doing now, attacking systems, so that we have less chaff that we have to worry about to find the wheat. That is a really hard problem, and I think requires us to figure out how to convince young, computer-literate people that breaking into systems, if you will pardon the colloquialism, isn't cool. It doesn't build your status in a peer group. It's like burning down a building. And people really get hurt. That's something we have not all successfully done yet, and we need to continue to work on.

Mr. PUTNAM. Mr. Schwarz, Mr. Gulloto, do you all have any comments on either of those issues? Do you have any comments on the

education component, and how we can be more effective at it, and whose responsibility it is?

Mr. SCHWARZ. Let me offer one suggestion. Obviously, education is hugely important, and the more we do, the better for all of us. There is a technology solution that can be applied to partly address this problem, which is something that we call client compliance, or compliancee, as it is called in bad English. Client compliance is about ensuring that when a client is reaching out to the network to be connected, that the network has the ability to test whether that client meets some basic minimum standards of good housekeeping relative to security.

It would be great if we could come together, government and industry, and develop a joint standard for how that compliance could be achieved and then have the ability for the ISPs, for the in-house servers, to, in fact, test every client before they are given access to the network. That technology in addition to education could help us dramatically improve the level of standard, the level of security that we see today.

Mr. PUTNAM. Mr. Gulloto, any comments?

Mr. GULLOTO. With regard to the education aspect, today we face a point where we are about to probably look at the next generation of threats and how is it that we can educate primarily the home user, but to protect themselves from those threats. We have them to the point that they understand that they are probably best served by putting antivirus and updating that antivirus as often as a vendor makes it available.

Antivirus today is no longer sufficient enough to protect everyone from the threats that we are seeing such as the Internet worms, which in many cases travel at certain points in the Internet where there may not be an antivirus product that can actually support or protect them from that. Therefore, as we have spoken about today, the evolution of the threat, we have to evolve our education and how we go about having the consumer at home understand that the Internet is a big city, and that like many cities, there are good parts and there are bad parts. You should proceed with caution in both areas, and understand that what you may find in the good part is good; what you may find in the bad part might look good, but it's not necessarily good.

People that are using the Internet today to exploit children, they are looking to exploit consumers by stealing data for a financial gain, I think are slightly different than perhaps some of the script kiddies that we have spoken about today. But clearly, when we developed the stay safe on line campaign sometime back, I think we looked to find that to be an avenue in which we could teach the consumer ways in which we could have them understand as to what a bad guy looked like on the Internet and what a good guy looked like on the Internet, and perhaps what a bad guy that looked like a good guy on the Internet was.

I think funding plays a huge part of it, actually, to be able to maintain and sustain this type of education, this evolving education that we need, which is why many of us today have talked about ways in which we can find funding to further R&D, but that R&D will include education.

Mr. PUTNAM. Thank you very much.

I am told that there is a 1:30 hearing in this same room, and so we need to bring it in for a landing. Is there anything that we have not covered that any of the panelists would like to add to the discussion before we wrap up? Beginning with Mr. Akers. Do you have any final comments?

Mr. AKERS. No.

Mr. PUTNAM. Mr. Reitinger.

Mr. REITINGER. Thank you for the opportunity to testify today, Mr. Chairman.

Mr. PUTNAM. Delighted to have you. Thank you. Appreciate your insight.

Mr. Gulloto.

Mr. GUTKNECHT. No. Thank you.

Mr. PUTNAM. Dr. Schwarz.

Mr. SCHWARZ. No. Thank you.

Mr. PUTNAM. Well, thank you all very much. This has been an outstanding hearing. I do apologize for its length, but I think that it was valuable and well worth our time.

I will remind everyone we have two more hearings next week on cybersecurity as well. And, with that, the record will remain open for 2 weeks for submitted questions and answers of topics that we were unable to get to today.

The subcommittee stands adjourned.

[Whereupon, at 1:20 p.m., the subcommittee was adjourned.]

○