WHAT CAN BE DONE TO REDUCE THE THREATS POSED BY COMPUTER VIRUSES AND WORMS TO THE WORKINGS OF GOVERNMENT?

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY,
FINANCIAL MANAGEMENT AND
INTERGOVERNMENTAL RELATIONS

OF THE

COMMITTEE ON
GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

AUGUST 29, 2001

Serial No. 107–77

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
80–480 PDF WASHINGTON : 2002

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

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LaTOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, Jr., Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California

BERNARD SANDERS, Vermont (Independent)

Kevin Binger, *Staff Director*
Daniel R. Moll, *Deputy Staff Director*
James C. Wilson, *Chief Counsel*
Robert A. Briggs, *Chief Clerk*
Phil Schiliro, *Minority Staff Director*

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

STEPHEN HORN, California, *Chairman*

RON LEWIS, Kentucky
DAN MILLER, Florida
DOUG OSE, California
ADAM H. PUTNAM, Florida

JANICE D. SCHAKOWSKY, Illinois
MAJOR R. OWENS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York

Ex Officio

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. Russell George, *Staff Director and Chief Counsel*
Bonnie Heald, *Director of Communications/Professional Staff Member*
Mark Johnson, *Clerk*
David McMillen, *Minority Professional Staff Member*

CONTENTS

WHAT CAN BE DONE TO REDUCE THE THREATS POSED BY COMPUTER VIRUSES AND WORMS TO THE WORKINGS OF GOVERNMENT?

WEDNESDAY, AUGUST 29, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL
MANAGEMENT AND INTERGOVERNMENTAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
San Jose, CA.

The subcommittee met, pursuant to notice, at 10 a.m., in room 205 of the San Jose Council Chamber at 801 North First Street, San Jose, CA, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representative Horn.

Also present: Representative Honda.

Staff present: J. Russell George, staff director and chief counsel; Bonnie Heald, director of communications; Elizabeth Johnston, detailee; Scott Fagan, assistant to the subcommittee; Mark Johnson, clerk; and David McMillen, minority professional staff member.

Mr. HORN. This hearing of the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

The dramatic increase in computer use and the Internet are changing the way we communicate and conduct business. With 58 percent of Americans now having home Internet access, our Federal, State and local governments increasingly rely on the Internet to conduct business. More than 40 million Americans now perform such routine activities as filing income tax returns, health benefit claims, and renewing driver's licenses electronically.

In addition to this wealth of personal information, the government's computer systems hold information that is vital to the security and economic well-being of this Nation.

Unfortunately, these systems are increasingly vulnerable to hostile attacks that are capable of extracting unauthorized information and potentially threatening the Nation's infrastructure.

Overall, the number and sophistication of these attacks is rising dramatically according to the federally funded CERT Coordination Center. Just to explain CERT, it stands for Computer Emergency Response Team, and it's our friends at Carnegie-Mellon that have been working on this for years. The number of incidents rose from 9,859 in 1999 to 21,765 in the year 2000.

So far this year, 15,476 incidents have been recorded. An increasing number of these attacks, often in the form of viruses or worms, specifically target government systems. There are more than 48,000 known worms and viruses which enable hackers to gain access to systems and data stored on the infected computers. Some of the most destructive of these programs can delete system and application software and even destroy the hardware itself. There are nearly 110 million with Internet connections and, as we have seen, these potentially devastating viruses or worms can become an epidemic in microseconds.

In 1999, for example, the Melissa virus gained notoriety because of the speed at which it spread. The first confirmed reports of Melissa were received on Friday, March 26, 1999. By Monday, March 29, the virus had affected more than 100,000 computers.

Last year the ILOVEYOU virus created worldwide havoc in a matter of days costing an estimated almost $8 billion to fix it up. Last month, worms called Code Red I and II in Roman numerals, burrowed into nearly 1 million computer systems worldwide and affected an estimated 100 million computer users. E-mail systems went down for days. Workers were locked out of crucial computer files and some e-commerce ground to a halt. Government Web sites came under siege with the Pentagon shutting down public access to all of its Web servers. To date, the cost of Code Red worms have risen to more than $2 billion and are mushrooming to about $200 million per day.

So far, these viruses and worms have not caused irreparable damage to the Federal Government's information systems. However, as the attacks become more sophisticated, the magnitude of the potential threat is colossal.

We must do something more than just react to these attacks. There is no easy fix but governments at every level must be prepared for the next attempted invasion. Computer security must have a priority.

Today we will examine the extent of the threat to government computer systems and the need for policy changes to ensure that these systems which are vital to this Nation and its economy and its citizens are protected.

We welcome our witnesses today and we look forward to their testimony.

[The prepared statement of Hon. Stephen Horn follows:]

ONE HUNDRED SEVENTH CONGRESS

Congreſs of the United States

Houſe of Repreſentatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

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

www.house.gov/reform

"What Can be Done to Reduce the Threats Posed by Computer Viruses and Worms to the Workings of Government?"

Opening Statement
Chairman Stephen Horn
August 29, 2001

A quorum being present, this hearing of the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

The dramatic increase in computer use and the Internet are changing the way we communicate and conduct business. With 58 percent of Americans now having home Internet access, our Federal, State, and local governments increasingly rely on the Internet to conduct business. More than 40 million Americans now perform such routine activities as filing income tax returns, health benefit claims, and renewing driver's licenses electronically. In addition to this wealth of personal information, the government's computer systems hold information that is vital to the security and economic well-being of this Nation.

Unfortunately, these systems are increasingly vulnerable to hostile attacks that are capable of extracting unauthorized information and potentially threatening the Nation's infrastructure.

Overall, the number and sophistication of these attacks is rising dramatically. According to the federally funded CERT[1] Coordination Center the number of incidents rose from 9,859 in 1999 to 21,765 in 2000. So far this year, 15,476 incidents have been reported. An increasing number of these attacks, often in the form of viruses or worms, specifically target government systems.

There are more than 48,000 known worms and viruses which enable hackers to gain access to systems and data stored on the infected computers. Some of the most destructive of these programs can delete system and application software and even destroy the hardware itself.

There are nearly 110 million computers with Internet connections, and, as we have seen, these potentially devastating viruses or worms can become an epidemic in microseconds.

In 1999, for example, the Melissa virus gained notoriety because of the speed at which it spread.

[1] CERT was originally an acronym for Computer Emergency Response Team, but because there are now a number of similarly named organizations, it has been trademarked as CERT and is no longer used as an acronym.

The first confirmed reports of Melissa were received on Friday, March 26, 1999. By Monday, March 29, the virus had affected more than 100,000 computers.

Last year, the "ILOVEYOU" virus created worldwide havoc in a matter of days, costing an estimated $8.7 billion dollars to fix.

And last month, worms, called Code Red I and II, burrowed into nearly 1 million computers and affected an estimated 100 million computer users worldwide. E-mail systems went down for days. Workers were locked out of crucial computer files, and some e-commerce ground to a halt. Government web sites came under siege, with the Pentagon shutting down public access to all of its web servers. To date the costs of the Code Red worms have risen to more than $2 billion dollars and are mushrooming to about $200 million dollars per day.

So far, these viruses and worms have not caused irreparable damage to the Federal Government's information systems. However, as the attacks become more sophisticated, the magnitude of the potential threat is colossal.

We must do something more than just react to these attacks. There is no easy fix, but governments at every level must be prepared for the next attempted invasion. Computer security must become a priority.

Today, we will examine the extent of the threat to government computer systems, and the need for policy changes to ensure that those systems, which are vital to this Nation and its citizens, are protected.

We welcome our witnesses today, and look forward to their testimony.

Mr. HORN. Panel one will include Keith Rhodes, Chief Technologist, Center for Technology and Engineering, of the U.S. General Accounting Office. That is part of the legislative branch of government headed by the Controller General of the United States.

Mr. Castro, Larry Castro, is chief of defensive information operations group of the Information Assurances Directorate. General Hadon is the commanding officer of the National Security Agency, and we welcome Mr. Castro. The Information Assurance Directorate and the National Security Agency is really our No. 1 intelligence group in the United States.

Leslie G. Wiser, Jr., Section Chief, National Infrastructure Protective Center, the Federal Bureau of Investigation. They have been particularly active and very cooperative with the Congress just as the National Security Agency has cooperated with the Congress on this very difficult situation.

After Mr. Wiser, we will have Jeff Carpenter, manager of the CERT Coordination Center that I mentioned earlier with Carnegie-Mellon University and its Computer Emergency Response Team.

The fifth one is Patricia Kuhar, program manager for information technology, California State Department of Information Technology.

In addition, one of my colleagues will be here. Mr. Honda, the gentleman from California. Michael Honda is making his way to the hearing from Sacramento. I wish him well. Most of you know this because a lot of you have been before us before. But this is an investigating committee and, as such, we do administer an oath to make sure everything is done under oath. So if you will stand up and put your right hands up.

[Witnesses sworn.]

Mr. HORN. The clerk will note that all four witnesses present have taken the oath, and we can now start with Mr. Rhodes.

STATEMENT OF KEITH A. RHODES, CHIEF TECHNOLOGIST, CENTER FOR TECHNOLOGY AND ENGINEERING, GENERAL ACCOUNTING OFFICE

Mr. RHODES. Thank you, Mr. Chairman.

In keeping with the rules of the committee, I'd like to give a brief summary and have my full statement submitted for the record.

Mr. HORN. I might add that when I name each individual, that automatically under our rules their statement goes immediately into the hearing record. This is being taken down by very able people, and Mr. Rhodes knows this, and we're delighted to have a member of the U.S. General Accounting Office.

Mr. RHODES. Thank you.

Mr. Chairman and members of the subcommittee, thank you for inviting me to participate in today's hearing on the most recent rash of computer attacks. This is the third time I've testified before Congress over the past several years on specific viruses. First, the Melissa virus in April 1999 and second, the ILOVEYOU virus in May 2000. At both hearings I stressed that the next attack would likely propagate faster, do more damage, and be more difficult to detect and counter.

Again, we are having to deal with destruction are reportedly costing billions. In the past 2 months, organizations and individuals have had to contend with several particularly vexing attacks. The most notable, of course, is Code Red but potentially more damaging are Code Red II and its variants and SirCam.

Together, these attacks have infected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations. They have already caused billions of dollars of damage, and their full effects have yet to be completely assessed, partly because viruses and worms don't just go away, especially the latest Code Red II variant which seems to have been modified to enable it to reinfect the systems it attacks.

Despite some similarities, each of the recent attacks is very different in its makeup, method of attack, and potential damage. Generally, Code Red and Code Red II are both worms which are attacks that propagate themselves to networks without any user intervention of interaction. They both take advantage of a flaw in a component of versions 4.0 and 5.0 of Microsoft's Internet Information Services [IIS] Web server software.

The main point I want to make about these two worms as well as the associated virus is that in and of themselves they might not be necessarily all that interesting. The potential of the attacks, however, is what I would like to cover today in my testimony.

The worms have taken an additional step compared to what ILOVEYOU or Melissa did. Code Red itself combined a worm with a denial of service attach, and Code Red II has combined a worm with the ability for installing a back door for circumventing security services inside Web service. SirCam, on the other hand, is a virus but it's a virus that doesn't rely on, as with ILOVEYOU, the internal mail server capability of the systems it attacks. Rather, it brings its own e-mail software with it so that it can send itself out.

Some of the points that I'd like to make today are that computer security, what we need to understand from these worms and virus attacks is that computer security is indeed a full-time job. New threats and vulnerabilities are constantly being identified, and measures to address those threats and vulnerabilities are being developed and implemented.

For example, when the vulnerability exploded when Code Red was announced, a patch was also made available at the same time. This required installations using the affected software to: No. 1 keep up with the vulnerabilities associated with their software; and No. 2, install a patch to address the vulnerability. Until this announcement, most, if not all, of these installations did not know they had a problem. Considering the number of affected servers, a number of sites did not take the quick response necessary to address this new vulnerability. For example, install the available patches.

This also underscores a point that we've made to this committee as well as other committees and the Congress regarding general controls of computer security across the government. The government is not in a position to protect itself. It does not have the talent, it does not have the training, it does not have the early warning. We are constantly—in my other capacity I run a computer security test laboratory in the General Accounting Office that has done work for this and other committees, and we are always able to break in and usually we are able to break in undetected and we are not using any sophisticated techniques. So it's not surprising that Code Red, Code Red II, Code Red's latest variant, SirCam, etc., are affected.

For example, I don't know if the gentleman from Symantec, Stephen Trilling, is going to actually disassemble the Code Red software for you later, but it's not very smart code. It's not very sophisticated. Yes, it does combine denial of service attack with its ability to be a worm, but it's not very good code at all. When you look at it, it's thrown together and yet it's still extremely effective.

No. 2 the attacks are coming faster after the vulnerability is announced. About 1 month after the vulnerability was announced, an effective attack using that vulnerability was launched. Shortly after this attack was launched, another attack with far more serious consequences was launched. That's Code Red II. Code Red came out, then Code Red II came out and, as a matter of fact, we were modifying the testimony in real time over the last week because a new variant had come out.

No. 3 installing software is a complex business. In some cases, entities are installing software without actually knowing the services that are being activated. For example, we understand that some entities were installing Windows 2000 without understanding that the ISS services were being activated. Therefore, take for example, your own cell phone. You probably don't know all the services that are associated with your cell phone, and you probably don't use all of them. However, when you buy a software package now, you're getting a complete set of services, some of which you don't know that they may have vulnerability.

The initial threat associated with a given attack is difficult to assess. I think one of the reasons, Mr. Chairman, that you and I get to see one another on an annual basis is that $8 billion distributed across the entire world, sort of like the first rules of physics. If I distribute the energy across a wide enough area, nobody feels the impact. $8 billion worldwide. Nobody seems to be willing to cry uncle, either the government or industry or individual users.

Substantial financial impact. It's very hard to get anyone to say that $8 billion matters. We are now on our way to, as you pointed out, $200 million a day perhaps in impact and yet no one is willing to scream uncle. Therefore, what is the definition of critical infrastructure? If it's truly critical, someone should be crying uncle by now or somebody is in a position to not be able to cry uncle.

Affected servers. One of the additional things about the current set of worms is that the affected servers broadcast the fact that their resources can be compromised. It's not just that Code Red goes in and takes over your environment, but Code Red goes in, takes over your environment and then tells everyone else that your environment has been compromised. The vulnerability exploited by Code Red can be used to take over the server. Nefarious individuals are always looking for servers that can be compromised in this fashion.

However, rather than seeking out servers that have this vulnerability, all a person has to do is to look at their own network to see what servers are attempting to spread the Code Red worm to them. Based on this information, the individual knows that the server is vulnerable to this attack. The attacks are indeed getting worse and worse. The attacks are coming faster after vulnerabilities are being identified and have a more devastating impact.

For example, the initial version of Code Red appeared about 1 month after the vulnerability was published. Shortly after the initial release, another attack that allowed an unauthorized individual to take over the server was launched.

In the midst of all of this gloom and doom that I'm presenting, I would like to point out that there was one good thing that did come out of this legislative Code Red attacks, and that was there was very good coordination between the U.S. Government and private industry. It was, to my mind, the first time the government and industry had effectively worked together. This is the first time, in a coordinated fashion, that government and industry had worked to address a problem such as this. This is a positive step forward. However, I will say that this is the pound of cure rather than the ounce of prevention.

One of my last points. Most software is not secure. Instead of relying on the code and fix approach for software development and security, we need to build security in the software during the development process. Although this may sound simple, it often conflicts with a get to market fast development program. Users, individual, corporate and government, are more than willing to state the mantra of it's a trade-off between usability and cost and the probability of a compromise remote PC is low. In other words, the users do not want to spend the time and money to secure systems since the "other stuff" we do for a living is more important and valuable. The fallacy in this argument is that the users have not done the risk analysis that allows them to make an informed decision about their security posture.

The last point I'd like to make, Mr. Chairman, is that in going along with the pound of cure, your committee has talked time and time again that there's a dearth of management inside government and so you and others have brought about the government Information Security Reform Act. But again, that's a cure as opposed to a prevention because that requires organizations like OMB, the Inspectors General, and the General Accounting Office to come in and validate the security posture of the departments and agencies. Again, we're in a situation, as we were in Y2K, where the Congress is stepping in to pass laws to make certain that people do due diligence regarding their own security posture.

Thank you very much, Mr. Chairman. That concludes my testimony, and I would entertain any questions from you or committee members.

[The prepared statement of Mr. Rhodes follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, House of Representatives

For Release
on Delivery
Expected at 10 a.m., PDT
Wednesday
August 29, 2001

INFORMATION SECURITY

Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures

Statement of Keith A. Rhodes
Chief Technologist

GAO
Accountability * Integrity * Reliability

GAO-01-1073T

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on the most recent rash of computer attacks. This is the third time I've testified before Congress over the past several years on specific viruses—first, the "Melissa" virus in April 1999 and second, the "ILOVEYOU" virus in May 2000. At both hearings, I stressed that the next attack would likely propagate faster, do more damage, and be more difficult to detect and counter.

Again, we are having to deal with destructive attacks that are reportedly costing billions. In the past 2 months, organizations and individuals have had to contend with several particularly vexing attacks. The most notable, of course, is Code Red but potentially more damaging are Code Red II and SirCam. Together, these attacks have infected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations. They have already caused billions of dollars of damage and their full effects have yet to be completely assessed.

Today, I would like to discuss the makeup and potential threat that each of these viruses pose as well as reported damages. I would also like to talk about progress being made to protect federal operations and assets from these types of attacks and the substantial challenges still ahead.

The Attacks

Despite some similarities, each of the recent attacks is very different in its makeup, method of attack, and potential damage. Generally, Code Red and Code Red II are both "worms," which are attacks that propagate themselves through networks without any user intervention or interaction. They both take advantage of a flaw in a component of versions 4.0 and 5.0 of Microsoft's Internet Information Services (IIS) Web server software.

Code Red originally sought to do damage by defacing Web pages and by denying access to a specific Web site by sending it massive amounts of data, which essentially would shut it down. This is known as a denial-of-service (DoS) attack. Code Red II is much more discreet and potentially more damaging. Other than sharing the name of the original worm, the only similarity Code Red II has with Code Red is that it exploits the same IIS vulnerability to propagate itself. Code Red II installs "backdoors" on infected Web servers, making them vulnerable to hijacking by any attacker who knows how to exploit the backdoor. It also spreads faster than Code Red. Both attacks have the potential to decrease the speed of the Internet and cause service disruptions. More importantly, these worms broadcast to the Internet the servers that are vulnerable to this flaw, which allows others to attack the servers and perform other actions that are not related to Code Red.

SirCam is a malicious computer virus that spreads primarily through E-mail. Once activated on an infected computer, the virus searches through a select folder and mails user files acting as a "Trojan horse" to E-mail addresses in the user's address book. A Trojan horse, or Trojan, is a program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. If the user's files are sensitive in nature, then SirCam not only succeeds in compromising the user's computer, but also succeeds in breaching the data's confidentiality. In addition to spreading, the virus can attempt to delete a victim's hard drive or fill the remaining free space on the hard drive making it impossible to perform common tasks such as saving files or printing. This form of attack is extremely serious since it is one from which it is very difficult to recover.

SirCam is much more stealthy than the Melissa and ILOVEYOU viruses because it does not need to use the victim's E-mail program to replicate. It has its own internal capabilities to mail itself to other computers. SirCam also can spread through another method. It can copy itself to other unsuspecting computers connected through a Windows network (commonly referred to as Windows network computers) that has granted read/write access to the infected computer. Like Code Red and Code Red II, SirCam can slow the Internet. However, SirCam poses a greater threat to the home PC user than that of the Code Red worms.

Table 1 provides a high-level comparison of the attacks. The attachment to this testimony answers the questions in the table in greater detail.

Table 1: High-level Comparison of the Attacks

	What is it?	How does it spread?	Who is at risk?	What damage can it do?
Code Red	Code Red is a worm, which is a computer attack that propagates through networks without user intervention. This particular worm makes use of a vulnerability in Microsoft's Internet Information Services (IIS) Web server software—specifically, a buffer overflow.	The worm scans the Internet, identifies vulnerable systems, and infects these systems by installing itself. Each newly installed worm joins all the others, causing the rate of scanning to grow rapidly.	Users with Microsoft IIS server installed with Windows NT version 4.0 or Windows 2000.	The program can deface Web sites, and was designed to perform a DoS attack against the www.whitehouse.gov Web site. It can also decrease the speed of the Internet.
Code Red II	Code Red II is also a worm that exploits the same IIS vulnerability. However, the worm also opens a backdoor on an infected server that allows any follow-on remote attacker to execute arbitrary commands.	Code Red II spreads like Code Red; however, in doing so, it selects Internet addresses that are in the same network range as the infected computer to increase the likelihood of finding susceptible victims.	Users with Microsoft IIS Web server software installed with Windows 2000.	Like Code Red, Code Red II can decrease the speed of the Internet. Unlike Code Red, it also leaves the infected system open to any attacker who can alter or destroy files and create a denial of service. It does not deface Web pages.
SirCam	SirCam is a malicious computer virus that spreads through E-mail and potentially through unprotected network connections. Once the malicious code has been executed on a system, it may reveal or delete sensitive information.	This mass-mailing virus attempts to send itself to E-mail addresses found in the Windows Address Book and addresses found in cached browser files. It also attempts to copy itself to specific Windows networked computers.	Any E-mail user or user of a computer with unprotected Windows network connections to the infected computer.	SirCam can publicly release sensitive information and delete files and folders. It can also fill the remaining free space on the computer's hard drive. Furthermore, it can lead to a decrease in the speed of the Internet.

Systems infected by Code Red and SirCam can be fixed relatively easily. A patch made available by Microsoft can remove the vulnerability exploited by Code Red and rebooting the infected computer removes the worm itself. Updating and using antivirus software can help detect and partially recover from SirCam. Patching and rebooting an infected server is not enough when a system is hit by Code Red II. Instead, the system's hard drive should be reformatted, and all software should be reinstalled to ensure that the system is free of other backdoor vulnerabilities.

Of course, there are a number of other immediate actions organizations can take to ward off attacks. These include:

- using strong passwords,
- verifying software security settings,

- installing firewalls,
- backing up files early and often,
- ensuring that known software vulnerabilities are reduced by promptly implementing software patches available from vendors,
- ensuring that policies and controls already implemented are operating as intended,
- using scanners that automatically search for system vulnerabilities,
- using password-cracking tools to assess the password strength of the audited users,
- using network monitoring tools to identify suspicious network activity, and
- developing and distributing lists of the most common types of vulnerabilities and suggested corrective actions.

Impact of the Attacks

Reports from various media and computer security experts indicate that the impact of these viruses has been extensive. On July 19, the Code Red worm infected more than 250,000 systems in just 9 hours, according to the National Infrastructure Protection Center (NIPC). An estimated 975,000 servers have been infected in total, according to Computer Economics, Inc. Code Red and Code Red II have also reportedly disrupted both government and business operations, principally by slowing Internet service and forcing some organizations to disconnect themselves from the Internet.

For example, reports have noted that (1) the White House had to change the numerical Internet address that identifies its Web site to the public, and (2) the Department of Defense was forced to briefly shut down its public Web sites. Treasury's Financial Management Service was infected and also had to disconnect itself from the Internet. Code Red worms also reportedly hit Microsoft's popular free E-mail service, Hotmail; caused outages for users of Qwest's high-speed Internet service nationwide; and caused delays in package deliveries by infecting systems belonging to FedEx Corp. There are also numerous reports of infections in other countries.

The economic costs resulting from Code Red attacks are already estimated to be over $2.4 billion.[1] These involve costs associated with cleaning infected systems and returning them to normal service, inspecting servers

[1] Estimate was developed by Computer Economics Inc.

to determine the need for software patches, patching and testing services as well as the negative impact on the productivity of system users and technical staff.

Although Code Red's reported costs have not yet surpassed damages estimated for last year's ILOVEYOU virus, which is now estimated to be more than $8 billion[2], the Code Red attacks are reportedly more costly than 1988's Morris worm. This particular worm exploited a flaw in the Unix operating system and affected VAX computers from Digital Equipment Corp. and Sun 3 computers from Sun Microsystems, Inc. It was intended to only infect each computer once, but a bug allowed it to replicate hundreds of times, crashing computers in the process. Approximately 10 percent of the U.S. computers connected to the Internet effectively stopped at the same time. At that time, the network had grown to more than 88,000 computers and was a primary means of communication among computer security experts.[3]

SirCam has also reportedly caused some havoc. It is allegedly responsible for the leaking of secret documents from the government of Ukraine. And it reportedly infected a computer at the Federal Bureau of Investigation (FBI) late last month and sent some private, but not sensitive or classified, documents out in an E-mail. There are reports that SirCam has surfaced in more than 100 countries.

Attacks Underscore Challenges Involved in Protecting Systems

GAO has identified information security as a governmentwide high risk issue since 1997. As these incidents continue, the federal government continues to face formidable challenges in protecting its information systems assets and sensitive data. These include not only an ever changing and growing sophistication in the nature of attacks but also an urgent need to strengthen agency security controls as well as a need for a more concerted and effective governmentwide coordination, guidance, and oversight. Today, I would like to briefly discuss these challenges. I would also like to discuss progress that has been made in addressing them, including improvements in agency controls, actions to strengthen warning and crisis management capabilities, and new legislation to provide a comprehensive framework for establishing and ensuring effectiveness of information security controls over information resources that support

[2] Computer Economics, Inc.

[3] http://www.cert.org/encyc_article/tocencyc.html.

federal government operations and assets. These are positive steps toward taking a proactive stand in protecting sensitive data and assets.

First, these latest incidents again show that computer attack tools and techniques are becoming increasingly sophisticated. The Code Red attack was more sophisticated than those experienced in the past because the attack combined a worm with a denial-of-service attack. Further, with some reprogramming, each variant of Code Red got smarter in terms of identifying vulnerable systems. Code Red II exploited the same vulnerability to spread itself as the original Code Red. However instead of launching a DoS attack against a specific victim, it gives an attacker complete control over the infected system, thereby letting the attacker perform any number of undesirable actions. SirCam was a more sophisticated version of the ILOVEYOU virus, no longer needing the victim's E-mail program to spread.

In the long run, it is likely that hackers will find ways to attack more critical components of the Internet, such as routers and network equipment, rather than just Web site servers or individual computers. Further, it is likely that viruses will continue to spread faster as a result of the increasing connectivity of today's networks and the growing use of commercial-off-the-shelf (COTS) products, which, once a vulnerability is discovered, can be easily exploited for attack by all their users because of the widespread use of the products.

Second, the recent attacks foreshadow much more devastating Internet threats to come. According to official estimates, over 100 countries already have or are developing computer attack capabilities. Further, the National Security Agency has determined that potential adversaries are developing a body of knowledge about U.S. systems and methods to attack them. Meanwhile, our government and our nation have become increasingly reliant on interconnected computer systems to support critical operations and infrastructures, including telecommunications, finance, power distribution, emergency services, law enforcement, national defense, and other government services. As a result, there is a growing risk that terrorists or hostile foreign states could severely damage or disrupt national defense or vital public operations through computer-based attacks on the nation's critical infrastructures.

Third, agencies do not have an effective information security program to prevent and respond to attacks—both external attacks, like Code Red, Code Red II, and SirCam, and internal attempts to manipulate or damage systems and data. More specifically, we continue to find that poor security planning and management are the rule rather than the exception. Most agencies do not develop security plans for major systems based on risk, have not formally documented security policies, and have not implemented programs for testing and evaluating the effectiveness of the controls they rely on.

Agencies also often lack effective access controls to their computer resources and consequently cannot protect these assets against unauthorized modification, loss, and disclosure. Moreover, application software development and change controls are weak; policies and procedures governing segregation of duties are ineffective; and access to the powerful programs and sensitive files associated with a computer systems operation is not well-protected. In fact, over the past several years, our analyses as well as those of the Inspectors General have found that virtually all of the largest federal agencies have significant computer security weaknesses that place critical federal operations and assets at risk to computer-based attacks.

In recognition of these serious security weaknesses, we and the Inspectors General have made recommendations to agencies regarding specific steps they should take to make their security programs effective.[4] Also, in 2001, we again reported information security as a high-risk area across government, as we did in our 1997 and 1999 high-risk series.[5]

Fourth, the government still lacks robust analysis, warning, and response capabilities. Often, for instance, reporting on incidents has been ineffective—with information coming too late for agencies to take proactive measures to mitigate damage. This was especially evident in the Melissa and ILOVEYOU attacks. There is also a lack of strategic analysis to determine the potential broader implications of individual incidents. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance.

[4] See, for example, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

[5] *High-Risk Series: An Update* (GAO-01-263, January 2001).

Further, as we recently reported,[6] the ability to issue prompt warnings about attacks is impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks, (2) a shortage of skilled staff, (3) the need to ensure that undue alarm is not raised for insignificant incidents, and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway. Lastly, government entities have not developed fully productive information-sharing and cooperative relationships. We recently made a variety of recommendations to the Assistant to the President for National Security Affairs and the Attorney General regarding the need to more fully define the role and responsibilities of the NIPC, develop plans for establishing analysis and warning capabilities, and formalize information-sharing relationships with the private sector and federal entities.[7]

Fifth, most of the nation's critical infrastructure is owned by the private sector. Solutions, therefore, need to be developed and implemented in concert with the private sector, and they must be tailored sector by sector; through consultation about vulnerabilities, threats, and possible response strategies. Putting together effective partnerships with the private sector is difficult, however. Disparate interests between the private sector and the government can lead to profoundly different views and perceptions about threats, vulnerabilities, and risks, and they can affect the level of risk each party is willing to accept and the costs each is willing to bear. Moreover, industry has raised concerns that it could potential face antitrust violations for sharing information. Lastly, there is a concern that an inadvertent release of confidential business material, such as trade secrets or proprietary information, could damage reputations, lower consumer confidence, hurt competitiveness, and decrease market shares of firms.

[6] *Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities* (GAO-01-1005T, July 25, 2001).

[7] The NIPC agreed with generally agreed with our findings and stated that the NIPC considers it of the utmost urgency to address the shortcomings we identified. However, the NIPC did not comment on several key recommendations, including the need to improve cooperative relationships with other federal entities, such as Defense and the Secret Service. See *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities* (GAO-01-323, April 25, 2001).

Fortunately, we are beginning to see improvements that should help agencies ward off attacks. We reported earlier this year[8] that several agencies have taken significant steps to redesign and strengthen their information security programs. For example, the Internal Revenue Service (IRS) has made notable progress in improving computer security at its facilities, corrected a significant number of identified weaknesses, and established a service-wide computer security management program. Similarly, the Environmental Protection Agency has moved aggressively to reduce the exposure of its systems and data and to correct weaknesses we identified in February 2000.

Moreover, the Federal Computer Incident Response Center (FedCIRC) and the NIPC have both expanded their efforts to issue warnings of potential computer intrusions and to assist in responding to computer security incidents. In responding to the Code Red and Code Red II attacks, FedCIRC and NIPC worked together with Carnegie Mellon's CERT Coordination Center, the Internet Security Alliance, the National Coordinating Center for Telecommunications, the Systems Administrators and Network Security (SANS) Institute, and other private companies and security organizations to warn the public and encourage system administrators and home users to voluntarily update their software.

We also recently reported on a number of other positive actions taken by NIPC to develop analysis, warning, and response capabilities. For example, since its establishment, the NIPC has issued a variety of analytical products to support computer security investigations. It has established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. It has developed crisis management capabilities to support a multi-agency response to the most serious incidents from FBI's Washington, D.C., Strategic Information Operations Center.

The administration is currently reviewing the federal strategy for critical infrastructure protection that was originally outlined in Presidential Decision Directive (PDD) 63, including provisions related to developing analytical and warning capabilities that are currently assigned to the NIPC. On May 9, 2001, the White House issued a statement saying that it was working with federal agencies and private industry to prepare a new version of the "national plan for cyberspace security and critical

[8] *High-Risk Series: An Update* (GAO-01-263, January 2001).

infrastructure protection" and reviewing how the government is organized to deal with information security issues.

Lastly, the Congress recently enacted legislation to provide a comprehensive framework for establishing and ensuring the effectiveness of information security controls over information resources that support federal government operations and assets. This legislation[9]—known as Government Information Security Reform (GISR)—requires agencies to implement an agencywide information security program that is founded on a continuing risk management cycle. GISR also added an important new requirement by calling for an independent evaluation of the information security program and practices of an agency. These evaluations are to be used by OMB as the primary basis for its summary report to the Congress on governmentwide information security.

In conclusion, the attacks we are dealing with now are smarter and more threatening than the ones we were dealing with last year and the year before. But I believe we are still just witnessing warning shots of potentially much more damaging and devastating attacks on the nation's critical infrastructures. To that end, it's vital that federal agencies and the government as a whole become proactive rather than reactive in their efforts to protect sensitive data and assets. In particular, as we have recommended in many reports and testimonies,[10] agencies need more robust security planning, training, and oversight. The government as a whole needs to fully develop the capability to strategically analyze cyber threats and warn agencies in time for them to avert damage. It also needs to continue building on private-public partnerships—not just to detect and warn about attacks—but to prevent them in the first place. Most of all, trust needs to be established among a broad range of stakeholders, roles and responsibilities need to be clarified, and technical expertise needs to be developed. Lastly, becoming truly proactive will require stronger

[9] Floyd D. Spence, National Defense Authorization Act for Fiscal Year 2001, P.L. 106-398, Title X, Subtitle G, 114 Stat. 1654, 1654A-265 (2000).

[10] See, for example, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000); *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999); *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection* (GAO/T-AIMD-00-72, February 1, 2000) and *Critical Infrastructure Protection: Challenges to Building A Comprehensive Strategy for Information Sharing and Coordination* (GAO/T-AIMD-00-268, July 26, 2000).

leadership by the federal government to develop a comprehensive strategy for critical infrastructure protection, work through concerns and barriers to sharing information, and institute the basic management framework needed to make the federal government a model of critical infrastructure protection.

Mr. Chairman and Members of the Subcommittee, this concludes my statement. I would be pleased to answer any questions that you or Members of the Subcommittee may have.

Contacts and Acknowledgment

For further information, please contact Keith Rhodes at (202) 512-6412. Individuals making key contributions to this testimony included Cristina Chaplain, Edward Alexander, Jr., Tracy Pierson, Penny Pickett, and Chris Martin.

Attachment I: Details on the Attacks

Code Red

Question	Answer
What is it?	Code Red is a worm, which is a computer attack that propagates through networks without user intervention. This particular worm makes use of a vulnerability in Microsoft's Internet Information Services (IIS) Web server software—specifically, a buffer overflow.[a] The worm looks for systems running IIS (versions 4.0 and 5.0) that have not patched the unchecked vulnerability, and exploits the vulnerability to infect those systems. Code Red was initially written to deface the infected computer's Web site and to perform a distributed denial of service (DDoS) attack against the numerical Internet address used by www.whitehouse.gov. Two subsequent versions of Code Red do not deface Web pages but still launch the DDoS attack. Code Red was first reported on July 17, 2001. The worm is believed to have started at a university in Guangdong, China.
How does it spread?	The worm scans the Internet, identifies vulnerable systems, and infects these systems by installing itself. Each newly installed worm joins all the others causing the rate of scanning to grow rapidly. The first version of Code Red created a randomly generated list of Internet addresses to infect. However, the algorithm used to generate the list was flawed, and infected systems ended up reinfecting each other. The subsequent versions target victims a bit differently, increasing the rate of infection.
Who is at risk?	Users with a Microsoft IIS server installed with Windows NT version 4.0 and Windows 2000.
What damage can it do?	The original variant of Code Red (CRv1) can deface the infected computer's Web site and used the infected computer to perform a DDoS attack against the Internet address of the www.whitehouse.gov Web site. Subsequent variants of Code Red (CRv2a and CRv2b) no longer defaced the infected computer's Web site making detection of the worm harder. These subsequent variants continued to target the www.whitehouse.gov Web site and used smarter methods to target new computers for infection. The uncontrolled growth in scanning can also decrease the speed of the Internet and cause sporadic but widespread outages among all types of systems. Specifically, • Although the initial version, CRv1, defaces the Web site, the primary impact to the server is performance degradation as a result of the scanning activity of this worm. This degradation can become quite severe since it is possible for a worm to infect the same machine multiple times. • Other entities, even those that are not vulnerable to Code Red, are impacted because servers infected by Code Red scan their systems and networks. Depending on the number of servers performing this scan, these entities may experience network denial of service. This was especially true with the implementation of CRv1 since a "flaw" in the random number generator essentially targeted the same servers. As noted above, this behavior is not found in the later variants. However, the end result may be the same since CRv2a and CRv2b use improved randomization techniques that facilitate more prolific scanning.
What can you do if you're infected?	Install a patch made available by Microsoft and reboot the system. (The patch should also be installed as a preventative measure).

Question	Answer
Technical Details on How the Code Red Worm Operates	
The Code Red worm has three phases – discovery and propagation, attack, and dormancy. Execution of these phases is based upon the day of the month.	
Phase 1: Discovery and Propagation	Between day 1 and day 19 of any month, Code Red performs its discovery and propagation function. It does this by generating 100 subprograms on an infected server. All but one of these subprograms has the task of identifying and infecting other vulnerable Web servers by scanning a generated list of Internet addresses. Once a target system is identified, Code Red uses standard Web server communication to exploit the flaw and send itself to the vulnerable server. Once a new server is infected, the process continues. CRv1 created a randomly generated list of Internet addresses to infect. However, the algorithm used to generate the random number list was "flawed", and infected systems ended up re-infecting each other because the random list that each computer generated was the same. CRv2a and CRv2b were modified to generate actual random lists of Internet addresses that were more effective at identifying potential servers that had not already been attacked. Therefore, these versions can ultimately infect greater numbers of unprotected servers. CRv1 also defaced the target system's Web site. This was done by replacing site's actual Web page with the message, "HELLO! Welcome to http://www.worm.com! Hacked by Chinese!"[b] This message enabled system administrators to easily identify when their servers had been infected. CRv2a and CRv2b modified the functionality so it would no longer deface Web pages, forcing system administrators to be proactive in determining infection. Descriptions of the variants are listed below. • CRv1: Web site defacement and "random" target selection for additional attacks. • CRv2a: No Web defacement and modified random target selection • CRv2b: No Web defacement and better target selection by optimizing the random number generation process, i.e., better target addresses are generated. Due to the target optimization, systems infected with version 2b are able to infect new systems at a faster rate than version 2a.
Phase 2: Attack	Between day 20 and day 27 of any month is Code Red's attack phase. Once Code Red determines the date to be within this designated attack date range, each infected server participates in a DDoS attack by sending massive amounts of data to its intended target, the numeric Internet address of the White House Web site. Since all infected servers are set to attack the same target on the same set of dates, the large amount of Internet traffic is expected to flood the Internet with data and bombard a numeric address used by www.whitehouse.gov with more data than it can handle. This flooding of data would cause the Web server to stop responding to all Web server requests, including legitimate users surfing the White House Web site.
Phase 3: Dormancy	From day 28 to the end of the month, the Code Red worm lays dormant, going into an infinite sleep phase. Although the worm remains in the computer's memory until the system is rebooted, Code Red will not propagate or initiate any attacks once it enters dormancy. According to testing performed by Internet Security Systems, Carnegie Mellon's CERT Coordination Center (CERT/CC), and the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC), the dormant worm cannot be awakened to restart the process.

Code Red II

Question	Answer
What is it?	Code Red II is also a worm that makes use of a buffer overflow vulnerability in Microsoft's IIS Web server software. Except for using the buffer overflow injection mechanism, the worm is very different than the original Code Red and its variants. In fact, it is more dangerous because it opens backdoors on infected servers that allow any follow-on remote attackers to execute arbitrary commands. There is no DDoS attack function in Code Red II. Code Red II was reported on August 4, 2001, by industry analysts.
How does it spread?	Like Code Red, the worm scans the Internet, identifies vulnerable systems, and infects these systems by installing itself. Each newly installed worm joins all the others causing the rate of scanning to grow. Code Red II, however, mostly selects Internet addresses in the same range as the infected computer to increase the likelihood of finding susceptible victims.
Who is at risk?	Users with Microsoft IIS Web server software (versions 4.0 and 5.0) installed with Windows 2000.
What damage can it do?	Like Code Red, Code Red II can decrease the speed of the Internet and service disruptions. Unlike Code Red, it also leaves the infected system open to any attacker who can alter or destrc files and create a denial of service attack. Specifically, • Because of the worm's preference to target its closest neighbors, combined with the enormous amount of scanning traffic generated by the numerous subprograms running in parallel, a large amount of broadcast request traffic is generated on the infected system's network. If several machines on a local network segment are infected, then the resulting attempt to propagate the infection to their neighbors simultaneously can generate broadcast requests at "flooding" rates. Systems on the receiving end of an effective "broadcast flood" may experience the effects of a DoS attack. • Code Red II allows remote attackers and intruders to execute arbitrary commands on infected Windows 2000 systems. Compromised systems are then subject to files being altered or destroyed. This adversely entities that may be relying on the altered or destroyed files. Furthermore, compromised systems are also at high risk for being exploited to generate other types of attacks against other servers.
What do you do if you're infected?	Several anti-virus software vendors have created tools that remove the harmful effects of the worm and reverse the changes made by the worm. This fix, however, is useless if the infected computer had been accessed by an attacker who installed other backdoors on the system that would be unaffected by the Code Red II patch tool. According to FedCIRC (Federal Computer Incident Response Center), due to the malicious actions of this worm, patching and rebooting an infected server will not solve the problem. The system's hard drive should be reformatted and all software should be reinstalled.

Technical Details of the Code Red II Worm

The Code Red II worm also has three phases – preparation, propagation, and Trojan insertion. Based upon current analysis, Code Red II only affects Web servers running on the Microsoft Windows 2000 operating system platform.

Phase 1: Preparation	During the preparation phase, the worm checks the current date to determine whether it will run at all. If the date is later than October 1, 2001, then the worm will cease to function and will remain infinitely dormant. If the date is before October 1, 2001, then all functions will be

Question	Answer
	performed. Although this discovery may bring hope that after October 1, 2001, this worm will no longer be a threat, this date constraint can be easily changed in a variant. The other activities conducted during the preparation phase include: • The functionality of Code Red II is dependent on both the system's environment and the current date. Code Red II checks the default system's language, e.g., English, Chinese, etc., and stores that information. • The worm also checks if the system has been previously infected, by searching for the existence of a specific file. If the file exists, then Code Red II becomes dormant and does not re-infect the system.[c] If the file does not exist, Code Red II creates the file and continues the process. • Preparation is finalized when the worm disables the capability of the Windows 2000 operating system to repair itself if it discovers that one of its required system files has been modified in any way. This becomes important during the Trojan Insertion function. Once the worm has completed the preparation phase, it immediately starts the propagation and Trojan insertion phases to complete infection.
Phase 2: Propagation	Code Red II creates hundreds of subprograms to propagate itself. The number of subprograms created depends upon the default language that the worm identified in the Preparation phsse. If the system's default language is Chinese, then 600 subprograms are created. If the default language is not Chinese, then 300 subprograms are generated. The propagation phase is unique because Code Red II seeks to copy itself to computers that are mostly near the infected system. The algorithm uses the infected system's own Internet address to generate a list of random Internet addresses. The generated list is comprised of Internet addresses that are closely related to the infected system. The rationale is that similar systems should reside in the "neighborhood" of the infected system, resulting in an increased chance of infection. Each of the subprograms is tasked with scanning one of the randomly generated Internet addresses to identify and infect another vulnerable system. Like Code Red, this worm uses the buffer overflow vulnerability to infect its target. Once a new target is infected, the process continues.
Phase 3: Trojan Insertion	Code Red II is more malicious than the Code Red worm discussed earlier, due to the existence of the Trojan horse backdoor programs that Code Red II leaves behind on the infected computer. The basic process follows: • Initially, executable files are copied to specific locations on the Web server, which by necessity, are accessible by any remote user. These executable files can run commands sent by a remote attacker to the server through the use of well-crafted Web commands. • A Trojan horse program is planted on the server that allows further exploit of the infected computer. The Trojan horse program is named after a required system program that executes when the next user logs into the system. It is also placed in a location that ensures that the Trojan horse program will be run instead of the required system program. Upon execution, the Trojan horse changes certain system settings that grant remote attackers read, write, and execute privileges on the Web server. • Twenty-four to forty-eight hours after the preparation function is initiated, Code Red II forces the infected system to reboot itself. Although the reboot eliminates the memory resident worm, the backdoor and the Trojan horse programs are left in place since they are stored on the system's disks. The reboot also restarts the IIS software, which, in turn, ensures that the Web server uses the newly compromised system settings. Since the Trojan horse will always be executed each time a user logs on, Code Red II

Question	Answer
	guarantees that remote attackers will always have access to the infected system. This is important, since even if the executable files copied at the beginning of the Trojan Insertion phase are deleted, the excessive privileges the Trojan sets at reboot are still in place. Therefore, the Trojan enables a remote attacker to perform similar exploits using these excessive privileges.

SirCam

Question	Answer
What is it?	SirCam is a malicious computer virus that spreads through E-mail and potentially through unprotected Windows network connections. What makes SirCam stealthy is that it does not rely on the E-mail capabilities of the infected system to replicate. Other viruses, such as Melissa and ILOVEYOU, used the host machine's E-mail program while SirCam contains its own mailing capability. Once the malicious code has been executed on a system, it may reveal or delete sensitive information. SirCam was first detected on July 17, 2001.
How does it spread?	This mass-mailing virus attempts to send itself to E-mail addresses found in the Windows Address Book and addresses found in cached files. It may be received in an E-mail message saying "Hi! How are you?" and requesting help with an attached file. The same message could be received in Spanish. Since the file is sent from a computer whose owner is familiar enough with the recipient to have their E-mail address in their address book, there is a high probability that the recipient will trust the attachment as coming from a known sender. This helps ensure the virus's success in the wild and is similar to the social engineering approach used by Melissa and ILOVEYOU. The E-mail message will contain an attachment that will launch the code when opened. When installed on a victim machine, SirCam installs a copy of itself in two files. It then "steals" one of the target system's files and attempts to mail that file with itself as a Trojan, that is, a file with desirable features, to every recipient in the affected system's address book. It can also get E-mail addresses from the Web browser. SirCam can also spread to other computers on the same Windows network without the use of E-mail. If the infected computer has read/write access to specific Windows network computers, SirCam copies itself to those computers, infecting the other computer.
Who is at risk?	Any E-mail user or any user of a PC with unprotected Windows network connections that is on the same Windows network as an infected computer.
What damage can it do?	SirCam can publicly release sensitive information and delete files and folders. It can also completely fill the hard drive of the infected computer. Furthermore, it can also lead to a decrease in the speed of the Internet. Specifically, • It can cause security breaches by attaching randomly chosen documents to itself and then E-mailing them to other parties. This allows the worm to cause unauthorized disclosure of

Question	Answer
	confidential information. • It can also delete files and folders. There is a one in twenty chance that an infected computer will have its hard drive erased or a one in fifty chance that the hard drive will be completely filled with garbage on October 16. • It can create a file named C:\Recycled\sircam.sys which consumes all free space on the C: drive. A full hard drive prevents users from saving files to that drive, and in certain configurations impedes system-level tasks, such as saving files and printing. It can result in a denial of service attack by flooding E-mail systems with useless E-mail containing attachments of various sizes.
What do you do if you're infected?	Most anti-virus software vendors have released updated information, tools, or virus databases to help detect and partially recover from SirCam.
Technical Details of the SirCam Virus	
Actions performed once the user executes the attachment	• SirCam detaches itself from the E-mail attachment and attempts to execute its program file on the target machine. • It copies itself to several directories on the target system. • It then "steals" one of the target system's files and attempts to mail that file with itself as a Trojan to every recipient in the affected system's address book. It can also get E-mail addresses from the Web browser. The subject line and the attachment's name differ from E-mail to E-mail. The attached file is where the virus' malice lies: the infected E-mail's attachment has a name that matches the subject line and two extensions, the second being .exe, .bat, .com, .pif, or .lnk. For example, a Word file called SAMPLE.DOC could be attached to the E-mail as SAMPLE.DOC.EXE. • It can also delete files and folders. There's a one in twenty chance that an infected computer will have its hard drive erased and a on in fifty chance that its hard drive will be completely filled with garbage on October 16. In addition to E-mail propagation, SirCam can copy itself to other systems on the Windows network that have write-able access. SirCam will copy itself to those systems and rename itself to be a system file that will be executed upon the next system reboot.

[a] Buffer overflows occur when programs do not adequately check input for appropriate length. Thus, any unexpected input "overflows" onto another portion of the central processing unit's executions stack. If this input is chosen judiciously by a rogue programmer, it can be used to launch code of the programmer's choice.

[b] http://www.cert.org/advisories/CA-2001-19.html.

[c] A reported variant of Code Red II does reinfect the server.

Mr. HORN. Yes. We will have all the presenters and get it all on the table and then we'll go to questions.

We now have Larry Castro, Chief Defensive Information Operations Group of the Information Assurance Directorate of what is probably our greatest national intelligence agency, the National Security Agency. Thank you, Mr. Castro, for coming.

STATEMENT OF LAWRENCE CASTRO, CHIEF, DEFENSIVE INFORMATION OPERATIONS GROUP, INFORMATION ASSURANCE DIRECTORATE, NATIONAL SECURITY AGENCY

Mr. CASTRO. Thank you, sir. Good morning. Thank you for that kind introduction. On behalf of our Director, Lieutenant General Mike Hadon, I am pleased to respond to the subcommittee's invitation to discuss NSA's view of the threats posed by malicious computer code, particularly viruses and worms.

My name is Larry Castro. I lead the Defensive Information Operations Group within NSA's Information Assurance Directorate. I'm accompanied today by Mr. Steve Ryan, a senior technical director in our group. We have submitted to the committee a formal statement for the record, and what I'd like to do is just summarize some of the key points of that as well as refer you to a few graphics that we put together.

As the chairman has most kindly pointed out, NSA is probably most well known for its signals intelligence or SIGINT mission which provides critical information about a wide range of foreign intelligence topics. Our Information Assurance mission to protect national security related information is an equally vital part of NSA's 50 year history and it's in this capacity of representing NSA's information assurance capability that I appear before you today.

What I'd first like to do in the next chart is to share with you the larger context with which we approach our information assurance mission and that is we seek in our products and the services that we provide to our customers within the national security community to provide products and services that emphasize these five attributes. We are, of course, most well known for historically providing very high-grade encryption products, but as the world of networking has evolved, we have branched out and our products now seek to help ensure the availability of communications, to protect data integrity, and to ensure the ability to authenticate and have non-repudiation among users.

Even with these within the even larger framework, we operate our entire information assurance mission, and that is to say again we seek to work across a wide spectrum with regard to computer and cyber incidents ranging from providing the technology to protect to engaging in services in cooperation with the U.S. Space Command and Joint Task Force on Computer Network Operations to detect and report on incidents in cyber space and then finally in support of the Defense Information System Agency to react to those incidents.

What the chart seeks to depict is to say that to do all of this you need to have that mix among technology, operations and personnel. The technology needs to be robust and the people, as has been pointed out in Mr. Rhodes' testimony, need to be well-trained to do the job. And then finally, you have to implement a sound information assurance policy.

I'd like to share with you all our view of the environment in which we're operating. Here, this is not a piece of modern art. It, in fact, is a result of work done by Doctor Bill Cheswick at Lumina wherein he has developed a capability of scanning the Internet. This is a scan of some 80,000 Internet routers. Each of those dots, should they be capable of being resolved, is one such router and the connections between the routers are color-coded to show the state of conductivity.

Within NSA and within our Information Assurance Defensive Operations Group we have a number of customers who correspond to one or more of those dots, and our job is to provide the situation awareness of what's going on among that whole milieu of dots, in particular, looking for the routers associated with bad actors. And I will try to describe some of the techniques that we use to do that. The sort of take way though is that the impression that you're given and the reason I like to use this chart is that this is an exploding environment. It's continuing to grow and branch out and that there are no boundaries in that chart up there. We don't see any State boundaries within the U.S. Department of Defense. We don't see any boundaries between U.S. Space Command, U.S. Central Command. And this is the message that we take, that the vulnerability of one leads to the vulnerability of all.

Going now to discuss a little bit about the threat. It's clearly one that has many, many dimensions and, from our perspective at NSA, we see folks in each of those clouds playing in cyber space. They have varying motives. Some are just in it for ego, quite frankly. Others are there for financial gain and occasionally we detect those who are there for serious data mining, possibly even espionage.

In the next chart we attempt to define the classes of attacks that we are contemplating. Starting from the left and then working to the right, we would simply alert the committee that there is a credible threat actually even in the distribution of software. The ability to implant this malicious code as the software is put into shrink wrap does exist and, of course, there are many who are concerned about this and are reacting to it.

Then with regard to the actual communication structures within the Internet itself, as shown there, there are both passive and active means of monitoring those structures, of inserting one's self in for less than good purposes. Of course, the main thrust of this presentation and this committee's work is the active remote attack that we show there in the bottom and that is surely one for which and through which we see the majority of incidents that we work on today.

And then getting actually into the enclave that we seek to defend. There are those who would simply stand off just outside this enclave, perhaps just outside this window, attempting to influence the cyber environment and then, quite frankly, sir, the thing that we're most concerned about within the Department of Defense, and it's been borne out over the last several years, is the insider threat. Again, the insider, either cooperating with outsiders or on its own, can do quite a bit of damage.

The other thing that needs to be noted is more and more we see the appearance of bulletin boards, chat rooms and other fora allowing hackers and those who would attempt to do harm in cyber space to exchange information. What this chart attempts to depict is that freeware that allows someone to become a scrip kitty and perhaps even become more extensive is readily available, is increasing in complexity and simply allows more efficient work on behalf of the hacker.

Now I'd like to turn to an examination that we completed within the Department of Defense looking at incidents over the last quarter. That would be to say the last 3 months preceding this one. What we did was to look at the apparent origin of the incidents that we are recording in the Department of Defense in the Joint Task Force on Computer Network Operations. Interestingly, as you can see, for that particular quarter and for a number of different reasons having to do with lots of things going on in the world, China was the country of apparent origin for over 20 percent of the incidents recorded within the Department of Defense. The others in the top 10 are shown there.

I do have to make one clarification with regard to apparent origin. As many know, the apparent origin is simply the last place that we see an attack coming from. As the chart here shows, the actual perpetrator could be located anywhere behind that apparent origin location. However, I still think it's useful to show which countries are being implicated, either wittingly or unwittingly, in these kind of attacks and intrusion attempts.

As has been discussed over the last 3 months, there have been a number of different worms and viruses and attacks that have shown up. One that impressed us most was the one referred to as the W32 Leaves worm or just the Leaves worm. Without going into the details—time doesn't allow—simply to say that this was a very, very complex attack. What impressed us most was the fact that when it was all said and done, the intruder down there in the lower right had the capability, estimates say, to control with one single set of commands about 24,000 zombies that he had established in his network. He did it in a very, very sophisticated way, a way that involved from time to time using encryption of his commands and, as I said before, he was able in the end to setup a command and control mechanism that did not require him to communicate individually with each of the computers under his control, but rather he used an Internet relay chat channel to provide both updates to his zombies and to provide commands.

We actually saw no harmful activity that came from this attempt to setup this distributed computing network, but I think it is indicative of the sophistication that we can expect to see in the future.

Now with regard to what we would suggest are the ways ahead, and they have already been very well covered by Mr. Rhodes so I will only seek to reiterate one more time. There's clearly a very, very strong component of education and awareness, not only for the practitioners but, we would submit, for the Nation at large. We would commend the committee. We think that having this hearing involving both government entities, academia, and the industry is a very, very important way of getting that message out.

We would also like to share with the committee the fact that within NSA, trying to get to the point again raised by Mr. Rhodes with regard to having sufficient folks well-trained, we have established an Academic Centers of Excellence Program that uses community-accepted criteria for validating the curricula of universities who engage in information assurance-related education.

Within California, of the 23 universities that have been so designated, U.C. Davis, Stanford University and the Naval Post-Graduate School of Monterey have been designated as Academic Centers of Excellence for information assurance education.

The second point is that giving increasing emphasis on anticipatory defensive measures. Specifically by this, we mean the fact that, again, as has already been pointed out, every one of the vulnerabilities that are being exploited by those who would do harm in cyber space are known beforehand and are anticipated by the hacker before the defense community makes the necessary patch.

To give you an idea of how we are always behind the power curve, last year within the Department of Defense, there were on the order of 24,000 what we would describe as incidents. Our definition of incidents is different from those used by the Search CC, so the numbers aren't quite the same.

But the important take away is that we estimate that at least 80 percent of the those 24,000 incidents could have been prevented had the patch to close the particular vulnerability in question been in place in a proper amount of time. And that's not to say that the department doesn't give high visibility to making these patches, but it is, quite frankly, a resource issue. The same system administrator who's charged with making that patch is also charged with keeping that computer system up and supporting his commander and, of course, that's usually what takes the priority.

And then finally, as was mentioned again previously, the kind of interaction between governmental entities and between the government and industry that we saw so well carried out during the Code Red campaign is in fact what we would suggest be the model for the future. If we have that kind of continued cooperation, if we have the mechanisms in place, both mechanical mechanisms and, quite frankly, emotional and thought process mechanisms, we believe we can go a long way in getting ahead of the power curve.

That concludes my testimony, sir, and we'd be glad to take questions at the appropriate time.

[The prepared statement of Mr. Castro follows:]

STATEMENT OF MR. LAWRENCE CASTRO
CHIEF, DEFENSIVE INFORMATION OPERATIONS GROUP
INFORMATION ASSURANCE DIRECTORATE
NATIONAL SECURITY AGENCY
Before the
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

August 29, 2001

Good morning, Mr. Chairman and distinguished Members of the Committee. On behalf of Lt Gen Michael Hayden, Director of the National Security Agency (NSA), I am pleased to accept the Subcommittee's invitation to discuss NSA's view of the threats posed by malicious computer code, particularly viruses and worms. My name is Larry Castro, and I lead the Defensive Information Operations Group within NSA's Information Assurance Directorate. I am accompanied today by Mr. Steve Ryan, a senior technical director in our group. NSA is most well known for its Signals Intelligence or SIGINT mission which provides critical information about a wide range of foreign intelligence topics. Our Information Assurance mission to protect national security related information is another vital part of our fifty-year history. It is in this capacity of representing NSA's Information Assurance capability that I appear before you today. NSA's responsibilities and authorities in the area of Information Assurance are specified in or derived from a variety of Public Laws, Executive Orders, Presidential Directives, and Department of Defense Instructions and Directives. Chief among them is the July 1990 "National Policy for Security of National Security Telecommunications and Information Systems" (NSD-42). This National Security Directive designates the Secretary of Defense as the Executive Agent for National Security Telecommunications and Information Systems Security (NSTISS), and further designates the Director of NSA as the "National Manager" for NSTISS. The Directive assigns the Director, NSA, broad responsibilities for national security systems including:

- Evaluating system vulnerabilities
- Acting as the focal point for U.S. Government cryptography and Information Assurance
- Conducting research and development in this area
- Reviewing and approving Information Assurance standards
- Conducting foreign liaison
- Operating printing and fabrication facilities for cryptographic keying material
- Assessing overall security posture
- Prescribing minimum standards for cryptographic materials

I think it is very important that the Committee Members have a clear understanding of the responsibilities and scope of NSA in the area of Information Assurance. At this point, I would like to briefly outline some of the forces and recent history that have shaped the situation we find ourselves in today and which point to some of the fundamental issues that need resolution in the near future.

BACKGROUND

When I began working at NSA some 36 years ago, the "security" business we were in was called Communications Security, or COMSEC. It dealt almost exclusively with providing protection for classified information against disclosure to unauthorized parties when that information was being transmitted or broadcast from point to point. We accomplished this by building the most secure "black boxes" that could be made, employing high-grade encryption to protect the information. In the late 1970s, and especially in the early 1980s with the advent of the personal computer, a new discipline we called Computer Security, or COMPUSEC, developed. It was still focused on protecting information from unauthorized disclosure, but brought with it some additional challenges and threats, e.g., the injection of malicious code, or the theft of large amounts of data on magnetic media. With the rapid convergence of communications and computing technologies, we soon realized that dealing separately with COMSEC on the one hand, and COMPUSEC on the other, was no longer feasible; and so the business we were in became a blend of the two, which we called Information Systems Security, or INFOSEC. The fundamental thrust of INFOSEC continued to be providing protection against unauthorized disclosure, or **confidentiality**, but confidentiality was no longer the exclusive point of interest. The biggest change came about when these computer systems started to be interconnected into local and wide area networks, and eventually to Internet Protocol Networks, both classified and unclassified. We realized that in addition to confidentiality, we needed to provide protection against unauthorized modification of information, or data **integrity**. We also needed to protect against denial-of-service attacks and to ensure data **availability**. Positive identification, or authentication, of parties to an electronic transaction had been an important security feature since the earliest days of COMSEC, but with the emergence of large computer networks, data and transaction **authenticity** became an even more important and challenging requirement. Finally, in many types of network transactions it became very important that parties to a transaction could not deny their participation, so that data or transaction **non-repudiation** joined the growing list of security services often needed on networks. Because the term "security" had been so closely associated, for so long, with providing confidentiality to information, within the Department of Defense we adopted the term **Information Assurance**, or IA, to encompass the five security services of confidentiality, integrity, availability, authenticity and non-repudiation. I should emphasize here that not every IA application requires all five security services, although most IA applications for national security systems – and all applications involving classified information – continue to require high levels of confidentiality.

Much of the work of Information Assurance in providing an appropriate mix of security services is not operational or time-sensitive, i.e., education and training, threat and vulnerability analysis, research and development, assessments and evaluations, and tool development and deployment. However, in an age of constant probes and attacks of on-line networks, an increasingly important element of protection deals with operational responsiveness in terms of **detecting** and **reacting** to these time-sensitive events. This defensive operational capability is closely allied with and synergistic with traditional Information Assurance activities, but in recognition of its operational nature is generally described as **Defensive Information Operations**, or DIO. The organization I lead, the Defensive Information Operations (DIO) Group, provides the following services to assist our customers:

- **Operational Readiness and Assessments** – This service establishes a customer's IA readiness level. Operational Security (OPSEC) Assessments and Information Security (INFOSEC) Assessments are services available to customers needing expert and experienced vulnerability and risk analysis support for their operational systems. OPSEC examines in totality the operation being evaluated to identify any associated information that could be exploited by known or potential adversaries. The Inter-agency OPSEC Support Staff (IOSS) provides this support to a wide range of customers. The INFOSEC Assessments Office provides customers with an IA analysis focused on the identification of their missions, identification of information critical to the performance of those missions, identification of potential vulnerabilities of the systems which process, store and transmit critical information, and recommendations for elimination or mitigation of identified vulnerabilities. We also have a "Red Team" which provides authorized readiness support to customers through active cyber intrusion activities to their computer networks based on very specific customer requirements. In this role, NSA operates much as an adversarial cyber intruder without causing any damage to the systems "attacked." The results of these Red Team operations are then shared with the customer to assist in improving their network security.
- **IA Monitoring** – Information Assurance monitoring is conducted by the Joint COMSEC Monitoring Activity (JCMA) under a Joint Chiefs of Staff charter. It is performed by a mix of civilian and military personnel deployed worldwide who monitor customer communications systems, including encrypted and unencrypted communications, for force protection and for exercises. This activity is strictly controlled in conformity with procedures approved by the Attorney General pursuant to the Electronic Communications Privacy Act with authorization from the customer receiving the monitoring support. Detected disclosures of sensitive or classified information over monitored systems are reported directly to the customer for appropriate action.
- **National Security Incident Response Center** – The defense of both the National Information Infrastructure (NII) and the Defense Information Infrastructure (DII) requires a robust and time-sensitive approach. To help meet this challenge, NSA's National Security Incident Response Center (NSIRC) provides near real-time reporting of cyber attack incidents, cyber attack analysis, and threat reporting relevant to information systems. Through round-the-clock, seven-days-a-week operations, the NSIRC provides the Departments of Defense, the Intelligence Community, Federal Law

Enforcement and other Government organizations with information valuable in assessing current threats or defining recent cyber intrusions.

THE THREAT

Clearly the threat to computer networks is real and growing worldwide, from nation states, non-state groups, and individuals. These sources have a wide variety of motives ranging from revenge or ego to profit, influence, or intelligence collection. Factors such as expanding network connectivity and the subsequent ease of access to systems, coupled with growing worldwide computer literacy, facilitate attacks against computer systems. The explosion in the number of computer bulletin boards and newsgroups has led to the wide and instantaneous dissemination of attack tools and techniques. Not only are intruders becoming more sophisticated, but the development of automated tools makes it easier for less skilled intruders to inflict more damage. A single hacker could potentially cause damage in cyberspace normally only considered within the means of a nation state.

I believe it would be useful to review of the results of a recent examination of cyber incidents that have been encountered on DoD networks during the second quarter of this year. This summary provides a macro picture of the larger cyber environment against which the most recent worm activity may be viewed.

Not surprisingly, among the findings of this examination is that China is the largest **apparent origin** of cyber incident activity targeting DoD systems, comprising 20% of the examined activity. The limitations of the term "apparent origin" must be noted. This term is used because source Internet Protocol (IP) addresses identified in cyber incident reports can also be compromised systems. Therefore, the apparent origin countries may or may not be the host nation from which the intrusion or probe attempts actually originated. Nevertheless, the apparent source listing is informative because it portrays a listed country's involvement (either wittingly or unwittingly) in malicious cyber activity or in precursor probing in preparation for such activity. As the DoD examination describes, the rest of the "top ten" list (in descending order) is: South Korea, Germany, United States, Canada, France, Taiwan, United Kingdom, Italy, and Japan.

The bulk of source IP addresses, U.S. as well as foreign, resolve to university or Internet service provided (ISP) systems. These systems often assign dynamic IP addresses to users, which may account for the fact that very few IP addresses were seen more than once as the apparent source of incident activity in this quarter. Additionally, university and ISP systems usually encompass a large number of computers available for exploitation. This, combined with the fact that the security practices of universities in general are commonly more relaxed, make them attractive targets for use as hop-points.

Automated probing of Internet addresses and scanning for vulnerable ports makes up the majority of reported incident activity. This type of activity, while legal, is often a precursor to intrusion attempts or malicious activity and should therefore be treated by network administrators as suspicious. In almost all cases, following probing and scanning, intruders gain their unauthorized access by exploiting known vulnerabilities in operating systems. Having gained such access, the intruder then inserts and activates a malicious code payload intended to extend the intruders reach to additional systems. One of the most serious examples of malicious codes we have seen, SubSeven 2.2, surfaced during the last quarter.

The SubSeven 2.2 is a Trojan Horse that exploits vulnerabilities associated with computers operating with Windows 9X, Windows 2000, Windows ME, and Windows NT 4.0. The code provides the capabilities that give the intruder access to cached passwords, the system registry, and other information on the infected computer. These capabilities provide the means for connection to a secure network using a compromised computer via cable or DSL modem causing serious concern. The code also enables the intruder to break into additional systems disguised as trusted personnel by redirecting the port and port scanner. At this point, the intruder has an army of computers at his disposal. Thus, a zombie network controlled by a Distributed Denial of Service (DDoS) tool can block or degrade network resources on an extremely large scale.

Such DDoS tools have become easier to use, offering more types of attacking techniques, better control of the zombie network, and better anonymity for the attacker. For these reasons, DDoS attacks are becoming more common, more complex, and more powerful. There are many barriers to a comprehensive solution to the problem posed by DDoS activity, including systems without basic security, the frequent international nature of the activity, and the lack of preparedness of victims.

COUNTERING THE THREAT

The threat is wide ranging, and the potential for damage to global e-commerce has already been demonstrated by cyber events of the past year. Additionally, while not yet demonstrated, the possibility of a well-coordinated cyber attack that could inflict significant damage to one or more of our Nation's critical infrastructures must be anticipated. Within NSA, our Defensive Information Operations mission to counter this threat is primarily directed toward assisting in the protection of national security and national security-related systems. In this regard, the National Security Incident Response Center (NSIRC) works in support of the U.S. Space Command and its subordinate Joint Task Force for Computer Network Operations (which has responsibility for the protection of Department of Defense networks) and the FBI's National Infrastructure Protection Center. This cooperation and interaction includes the posting of NSIRC analysts to both organizations for the purpose of coordinating our joint effort. We are not defenseless, and there are many significant efforts underway to respond to the cyber threat. Key factors in mitigating the damage from cyber attacks include:

- Education and Awareness
- Anticipatory Defensive Measures
- Responsible Exchange of Actionable Cyber Incident Information

EDUCATION AND AWARENESS

A continuing cooperative effort to inform the Nation about the nature of the cyber threat and the potential for damage from this threat is required. Such an effort involves U.S. Industry, Academia, and the U.S. Government, and this hearing is certainly an example of such a joint endeavor. One of the goals of this thrust is to significantly increase the number of students in U.S. colleges and universities pursuing degrees in Information Assurance-related fields. In this regard, we at NSA have designated 23 universities as Centers of Academic Excellence in Information Assurance under the Centers of Academic Excellence Program. NSA granted the designations following a rigorous review of university applications against published criteria based on training standards established by the national computer network defense community.

ANTICIPATORY DEFENSIVE MEASURES

The majority of cyber attacks exploit well-known vulnerabilities for which preventive measures are available. System administrators are encouraged to stay informed about such measures, heed compliance messages, install patches for known vulnerabilities, and configure systems to allow only necessary services. This guidance cannot be overemphasized. For example, last year, of the more than 24,000 cyber incidents reported by DoD elements, it is projected that nearly 80% would have been prevented if the proper vulnerability-closing patches had been installed.

RESPONSIBLE EXCHANGE OF ACTIONABLE CYBER INCIDENT INFORMATION

Today there are many excellent cyber incident reporting and analysis activities in operation within government and industry. During the most recent CODE RED activity, there was unprecedented coordination and cooperation among these many centers. This interaction is absolutely essential if we as a Nation are to achieve the real-time, cyber situational awareness that will be necessary to protect our vital e-commerce interest and our sustained National Security-related use of cyberspace.

Mr. Chairman, this concludes my testimony and Statement for the Record. Once again I thank you and the Members of the Committee for the opportunity to share with you some of the insights that we at the National Security Agency have with regard to the cyber threats and initiatives to counter these threats.

Mr. HORN. Well, thank you very much. We'll have a number of questions very shortly here.

Now we have Leslie Wiser, the Section Chief for the National Infrastructure Protection Center of the Federal Bureau of Investigation. I want to thank you very much for the cooperation you have had with the Congress and this committee and bringing people from all over the world so we could get a good look at them. You've always helped us in this area, and thank you, just as the National Security Agency has helped us.

So proceed, Mr. Wiser.

STATEMENT OF LESLIE G. WISER, JR., SECTION CHIEF, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION

Mr. WISER. Chairman Horn, thank you for those kind comments and thank you for inviting me here today to testify about how the National Infrastructure Protection Center [NIPC], is addressing the threats posed to government systems by computer viruses and worms. I have a formal statement that I will submit for the committee, and I will continue with other remarks.

I spoke with NIPC Director Ron Dick yesterday, and he regrets not being able to attend but asked me to forward his gratitude as well to this committee. It's been suggested that www stands not for World Wide Web; rather, in this context, it seems to mean wild, wild west. Cyber crime is a new frontier requiring new thinking and new skills. Dealing with Internet viruses, worms and the vast spectrum of threats to government and private sector information systems requires a dedicated and cooperative effort. It is fitting that we are in the heart of the information technology community. It's that cooperative effort that I will focus on here today.

The mission of the NIPC is to detect, deter, warn of, investigate and respond to cyber intrusions that threaten our critical infrastructures. It is the only organization in the United States with this national infrastructure protection mandate. The NIPC gathers together under one roof representatives from, among others, the law enforcement, intelligence, and defense communities which collectively provide a unique analytical perspective to cyber intrusion information obtained from investigation, intelligence collection, foreign liaison and private sector cooperation. This perspective ensures that no single discipline addresses cyber intrusions of critical infrastructures in a vacuum. Rather, a cyber incident is examined as a system security matter as well as for its potential as a counter-intelligence defense and law enforcement matter.

While the mission of the NIPC outlined in Presidential Decision Directive 63 is broad, our complement is relatively small with 91 FBI employees and 18 detailees, many of whom field critical leadership roles. I am pleased to serve with a fine staff of dedicated men and women including NIPC's Deputy Director, Rear Admiral James Plehal of the U.S. Naval Reserve, who hail from 12 Federal entities and 3 foreign governments. Please allow me to provide a few examples that demonstrate our approach to protecting U.S. critical infrastructures including our government information systems.

In July 2001 the NIPC issued a series of timely predictive warnings regarding the Code Red worm. Before issuing these warnings, the NIPC conducted daily tele-conferences with the National Security Council, the National Security Agency, the Defense Department's Joint Task Force for Computer Network Operations, the Justice Department, the CIA, CERT and others to form a consensus response strategy. As a result of this cooperation, the impact of Code Red was successfully mitigated. The NIPC was quick to fulfill its warning mission while simultaneously coordinating the FBI investigation which is continuing.

Similarly, on July 23, 2001 the NIPC, again working with the same partners, issued an advisory regarding the Leave worm which infected over 20,000 machines. The FBI's investigation and analysis determined the infected computers were synchronizing, possibly for an attack. Through the execution of several search warrants and sophisticated analysis by our computer scientists, we followed the trail to the United Kingdom where New Scotland Yard identified a subject and arrested him. In this example, the successful investigation itself ended the threat.

In contrast to the success of the Leave worm investigation, we are often frustrated when we are forced to obtain several separate court orders tracing intruders back through several ISP hot points. This is difficult enough when all the activity is within the United States. It often becomes formidable when the trail leads overseas. The trans-national nature of cyber attacks requires solid liaison with foreign partners with whom we can exchange warnings of malicious computer activity.

Currently, the NIPC has connectivity with similar centers in the U.K., Canada, Australia, New Zealand and Sweden and in May, I extended an offer to the German Government, which is under consideration. We think there is great benefit in establishing a global network including partners in time zones ahead of us to provide early warning of attacks.

Along with foreign collaboration, cooperation with the private sector is absolutely essential to successfully protect U.S. critical infrastructures. As a result, the NIPC established InfraGard where like-minded professionals can share best practices and discuss other issues of importance to them. InfraGard is like a neighborhood watch because members band together to protect each other. They have shared information about attacks with each other on a confidential basis by providing sanitized reports to the NIPC.

In May the Safe America Foundation presented its 2001 World Safe Internet Safety Award to the NIPC for the InfraGard partnership. Today InfraGard boasts over 1,800 members including 87 Fortune 500 companies in 65 chapters across the United States and Puerto Rico.

In June the NIPC hosted the first annual InfraGard Congress here in California where private sector representatives from around the country gathered and elected an executive committee to help lead this important initiative. In particular, small startup businesses that cannot afford a dedicated security office or fees charged by for profit security enterprises have found a home in InfraGard.

InfraGard is a free service and puts a face on law enforcement that enhances accessibility, communication, cooperation and trust. I don't know of another program like it in the world, and foreign officials and companies have expressed an interest in creating InfraGard-like programs in their countries. For example, Mr. Elfen Menses of the Philippine National Bureau of Investigation, who testified before this subcommittee last year, attended the InfraGard Congress as an observer. He left energized and committed to starting an InfraGard-like program in the Philippines, and we embrace efforts to establish foreign public/private partnerships as a step to enhancing global security.

Pursuant to PDD63, the NIPC was appointed to be the Federal Government's liaison for Emergency Law Enforcement Services Sector, the ELES Center, one of the critical infrastructures identified in PDD63. The NIPC works cooperatively with the ELES Sector Forum, a group of seasoned State and local law enforcement professionals, to protect State and local law enforcement data and communication systems, including the 911 system.

On March 2 the NIPC and members of the forum led by Sheriff Pat Sullivan of Colorado presented the completed sector plan to the White House. The plan and an accompanying guide, a toolbox of best practices, worksheets and checklists, is the Nation's only completed infrastructure protection plan. It is being used as a model for other infrastructures.

Yet we will not succeed in stemming the tide of devastating viruses and worms on the Internet without raising public awareness, continued cooperation with the private sector, strong relationships at all levels of government, and a united front with foreign governments. The good news is that through new thinking and new skills, we have made significant progress in all these areas.

I remain grateful for the opportunity to discuss this important topic with you. I'm also gratified to see many of our U.S. Government and private sector partners here at the table. We want to work closely with them, this subcommittee, and with other Members of Congress on infrastructure protection issues.

Thank you very much, sir.

[The prepared statement of Mr. Wiser follows:]

WWW = wild wild west

Statement of Leslie G. Wiser, Jr.
Chief
Training, Outreach, and Strategy Section
National Infrastructure Protection Center
Federal Bureau of Investigation
before the
House Committee on Government Affairs
Subcommittee on Government Efficiency, Financial Management,
and Intergovernmental Relations
San Jose, California Field Hearing

August 29, 2001

Good morning Chairman Horn, thank you for inviting me here today to discuss cyber security issues. While I am going to discuss broad aspects of cyber security and the role of the NIPC in helping to secure the nation's critical infrastructures, I am going to focus on some recent incidents that demonstrate the success we can have when government partners with other nations and with the private sector. I will then discuss the NIPC's role in cyber security with respect to predicting, preventing, detecting, and responding to incidents with an emphasis on computer viruses and worms. The final part of my statement will focus on some of the recent virus and worm cases we have faced.

A virus is malicious computer code embedded within an executable program that victims activate on their machines, usually by opening an e-mail attachment. Often viruses are sent with notes instructing recipients to open the attachment, such as the note with the Melissa Macro Virus which stated "here is the document you requested," or with a tantalizing title such as "sexxxy.jpg," or "naked wife." Worms, on the other hand, require no action by the victims to activate. They spread on their own from system to system without need for the victim to do anything. The Code Red Worm, for example, automatically sends itself to 99 IP addresses it generates. Once activated, viruses and worms can do anything from deleting files to sending themselves, together with documents on your harddrive, to some or all of the names in your address book or to any internet protocol address.

Arrest in Leave Worm case

On June 23, 2001, the NIPC issued "Advisory 01-014," "New Scanning Activity (with W32-Leave.worm) Exploiting SubSeven Victims," regarding the Leave Worm activity. This particular worm allowed the intruder access to an infected system while the victim machine was connected to the Internet. It is believed that home-users' computers, without updated anti-virus software, were the systems primarily infected by this worm. Current anti-virus software will detect the presence of the W32-Leave.worm. Full descriptions and removal instructions can be found at various anti-virus web sites.

A 24 year old male was arrested on July 23, 2001, in the United Kingdom for violation of its "Computer Misuse Act 1990." The announcement of his arrest was delayed to avoid potentially compromising the ongoing investigation. This individual who, under British Law, cannot be identified at this time, was arrested in connection with designing and propagating malicious code, known as the W32-Leave.worm, or Leaves worm, into Windows-based computer systems. This individual has been released from custody and ordered to return to New Scotland Yard on September 24, 2001.

This malicious code was discovered by the analytical efforts of the employees of the Systems Administration and Network Security (SANS) Institute and reported by SANS to the NIPC. This arrest came as a result of a joint FBI/New Scotland Yard, UK, investigation, and illustrates the benefits of law enforcement and private industry working together.

Ongoing Efforts on Code Red

July 19

The Code Red Worm was discovered in the wild on July 13, 2001by network administrators who were experiencing a large number of attacks targeting the buffer overflow vulnerability first reported in June, 2001. On June 19, 2001, the NIPC and FedCIRC issued a joint advisory about the buffer overflow vulnerability that targeted Microsoft Windows NT and Microsoft Windows 2000 operating systems running IIS 4.0 and 5.0. The advisory stated that "the activity of the Ida Code Red Worm has the potential to degrade services running on the Internet." In one day alone the Code Red Worm infected more than 250,000 systems in just nine hours. The Code Red Worm, which was first reported by eEye Digital Security, takes advantage of known vulnerabilities in the Microsoft IIS Internet Server Application Program Interface (ISAPI) service. Un-patched systems are susceptible to a "buffer overflow" in the Idq.dll, which permit the attacker to run embedded code on the affected system. This memory resident worm, once active on a system, first attempts to spread itself by creating a sequence of random IP addresses to infect unprotected web servers. Each worm thread will then inspect the infected computer's time clock. The trigger time for the DOS execution of the Code Red Worm was at midnight on July 20, 2001. Upon successful infection, the worm proceeded to use the time thread in an effort to bring down the www.whitehouse.gov domain by having the infected systems simultaneously send 100 connections to port 80 of the whitehouse's Internet Protocol address.

The original variant of the worm also placed the words "Welcome to worm.com! Hacked by Chinese!" on the victim sites. Two other variants of the original worm do not deface victim web sites. The NIPC, along with its government and private sector partners, realized that persons using Microsoft Windows NT and Microsoft Windows 2000 operating systems running IIS 4.0 and 5.0 needed to be warned to patch their systems for the safety of the entire Internet. Officials from the following organizations were all involved in the response effort working through the weekend of July 28-29: National Infrastructure Protection Center (NIPC) of the FBI, Critical Infrastructure Assurance Office (CIAO) of the Department of Commerce, Federal Computer

Incident Response Center (FedCIRC) of the General Services Administration, Computer Emergency Response Team Coordination Center (CERT/CC) of Carnegie Mellon University, Systems Administration and Network Security (SANS) Institute, Microsoft, Internet Security Systems, Inc. (ISS), Cisco Systems, Inc., Partnership for Critical Infrastructure Security (PCIS), Information Technology Association of America (ITAA), Digital Island, Inc., Information Technology Information Sharing and Analysis Center (IT-ISAC), Internet Security Alliance (ISA), UUNet, and America Online.

On Sunday July 29 the NIPC, Microsoft Corporation, Federal Computer Incident Response Center (FedCIRC), the Information Technology Association of America (ITAA), CERT Coordination Center (CERT/CC), SANS Institute, Internet Security Systems (ISS), and the Internet Security Alliance (ISA) issued a joint warning message about Code Red.

The NIPC posted the warning and numerous updates on its public website (www.nipc.gov) and pushed the warning to InfraGard members through the InfraGard communications network, to state and local police through the National Threat Warning System, and to tens of thousands of private sector companies via the FBI's Awareness National Security Issues and Response (ANSIR) network. By forwarding the warning message to those who may need it, the NIPC strives to ensure that those who are part of its information sharing networks receive the information as quickly as possible with minimal effort on their part. In other cases InfraGard has already prevented cyber attacks by discretely alerting InfraGard members to compromises on their systems. For efforts such as the one made on Code Red, the InfraGard initiative recently received the 2001 WorldSafe Internet Safety Award from the Safe America Foundation.

On July 30 a joint news conference was held at the Ronald Reagan Building in Washington, DC. The presence of representatives of agencies, companies, and organizations which produced the Code Red warning demonstrated the seriousness of the threat and the public-private partnership that has developed with regard to protecting our information systems from attack. The urgency of the news conference lay in the fear that the spread of the worm could absorb so much bandwidth as to degrade the overall functioning of the Internet. Since business, medical, and government professionals increasingly depend on the Internet's functioning to conduct normal operations, service degradation poses an emerging threat to America's economy and security.

Microsoft has developed a patch for the identified vulnerability. According to Microsoft, over 2 million copies of the IIS patch have been downloaded. The July 30 news conference no doubt accelerated this process. Since the patches can be downloaded and installed on a number of machines, the actual number of systems patched may be higher than 2 million. The NIPC and its partners have received much positive feedback from the user community regarding these efforts on Code Red.

We are hopeful that the worst of the damage feared was averted based on this awareness campaign. Nevertheless Computer Economics, a California-based Internet research organization, estimates that the worm has already cost $2.4 billion in economic impact, including $1 billion to cleanse, inspect, patch and return systems to normal service, and $1.4 billion for other support functions related to lost productivity due to the worm. As of August 8, the SANS Internet Storm Center noted that 661,044 unique IP addresses have been infected, with 150-175,000 machines infected (machines can have more than one associated IP address). While all of these figures are subject to revision, two trends seem clear. First, the rate of infections from the original worm have been substantial, although not at the same rate as in July. Second, the aggressive efforts on the part of the government and private sector urging computer users to patch their systems seems to have paid off.

Self-propagating worms that exploit vulnerabilities in commonly used software platforms will continue to pose a security challenge. These worms require no social engineering (i.e. no one needs to be tricked into revealing any information) and require no action on the part of users (i.e. the opening of attachments). As we saw with Code Red, they can hurt us in two ways: they can consume Internet bandwidth during their propagation phase if enough machines are infected, and they can carry harmful payloads, like the instructions to launch against a chosen target. Anyone can be the next target as future worms may result in much more destructive activity.

There is another worm we have been tracking since early August dubbed "Code Red II." This worm exploits the same vulnerability as the original Code Red Worm and its variants, but instead of compromising a system to launch Denial of Service attacks, it installs a backdoor into infected systems that can be accessed by anyone knowing that the victim system has been compromised.

On August 16 the NIPC released an assessment entitled "Code Red Reminder and Clarification, Assessment 01-018." That assessment clarifies issues related to which operating systems and software are vulnerable to Code Red and also makes clear that, contrary to some reports, we have not yet identified a Code Red III.

The NIPC Approach to the Problem

Because the NIPC is an interagency Center, it could quickly react to the recent infections of the Leave and Code Red Worms. Senior leadership positions in the NIPC are held by personnel from several agencies. The NIPC Director is a senior FBI executive. The Deputy Director of the NIPC is a two-star Navy Rear Admiral and the Executive Director is detailed from the Air Force Office of Special Investigations. The Section and Unit Chiefs in the Computer Investigation and Operations Section and the Training, Outreach, and Strategy Section are from the FBI. The Assistant Section Chief for Training, Outreach and Strategy is detailed from the Defense Criminal Investigative Service. The Section Chief of the Analysis and Warning Section is from the CIA and his deputy is a senior FBI agent. The head of the NIPC Watch and Warning Unit is reserved for a uniformed service officer, and the head of the Analysis and Information Sharing Unit is reserved for a National Security Agency manager. This breadth of leadership has meant that when worms such as Code Red appear, coordination across the civilian and military agencies of the government is rapid and efficient.

But it is not just in the leadership ranks that the NIPC has broad representation. Currently the Center has representatives from the following agencies: FBI, Office of the Secretary of Defense, Army, Air Force Office of Special Investigations, Defense Criminal Investigative Service, National Security Agency, United States Postal Service, Department of Transportation/Federal Aviation Administration, Central Intelligence Agency, Department of Commerce/Critical Infrastructure Assurance Office, and the Department of Energy. This representation has given us the unprecedented ability to reach back to the parent organizations of our interagency detailees on intrusions and infrastructure protection matters in order to provide and receive information. In addition, we have formed an interagency coordination cell at the Center which holds monthly meetings with U.S. Secret Service, U.S. Customs Service, representatives from DoD investigative agencies, the Offices of Inspector General of NASA, Social Security Administration, Departments of Energy, State, and Education, and the U.S. Postal Service, to discuss topics of mutual concern.

This representation is not enough, however. The NIPC would like to see all lead agencies represented in the Center. The more broadly representative the NIPC is, the better job it can do in responding to viruses, worms, and other intrusions into critical U.S. systems.

We have established four strategic directions for our capability growth: prediction, prevention, detection, and mitigation/response. None of these are new concepts but the NIPC will renew its focus on each of them in order to strengthen our strategic analysis capabilities. The NIPC will work to further strengthen its longstanding efforts on the early detection and mitigation of cyber attacks. These strategic directions will be significantly advanced by our intensified cooperation with federal agencies and the private sector.

Prediction:

Our most ambitious strategic directions, prediction and prevention, are intended to forestall attacks before they occur. We are seeking ways to forecast or predict hostile capabilities in much the same way that the military forecasts weapons threats. The goal here is to forecast these threats with sufficient warning to prevent them. A key to success in these areas will be strengthened cooperation with intelligence collectors and the application of sophisticated new analytic tools to better learn from day-to-day trends. The strategy of prevention is reminiscent of traditional community policing programs but with our infrastructure partners and key systems vendors. As the recent Leave and Code Red Worm incidents demonstrate, our working relations have never been closer with key federal agencies, like FedCIRC, NSA, CIA, and the Joint Task Force - Computer Network Operations (JTF-CNO), and private sector groups such as SANS, the anti-virus community, major Internet Service Providers, and the backbone companies. These close relationships aid in predicting events before they happen.

Prevention:

Our role in preventing the spread of computer viruses and worms as well as other cyber intrusions into critical U.S. systems is not to provide advice on what hardware or software to use or to act as a federal systems administrator. Rather, our role is to provide information about threats, ongoing incidents, and exploited vulnerabilities so that government and private sector system administrators can take the appropriate protective measures. The NIPC has a variety of products to inform the private sector and other domestic and foreign government agencies of the threat, including: alerts, advisories, and assessments; biweekly *CyberNotes*; monthly *Highlights*; and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law and the need to protect intelligence sources and methods, and law enforcement investigations. For example, *Highlights* is a publication for sharing analysis and information on critical infrastructure issues. It provides analytical insights into major trends and events affecting the nation's critical infrastructures. It is usually published in an unclassified format and reaches national security and civilian government agency officials as well as infrastructure owners and operators. *CyberNotes* is another NIPC publication designed to provide security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices. It is published on our website and disseminated in hardcopy to government and private sector audiences.

The NIPC has elements responsible for both analysis and warning. What makes the NIPC unique is that it has access to law enforcement, intelligence, private sector, foreign liaison, and open source information. No other entity has this range of information. Complete and timely reporting of incidents from private industry and government agencies allows NIPC analysts to make the linkages between government and private sector intrusions. We are currently working on integrating our databases consistent with the law to allow us to more quickly make the linkages among seemingly disparate intrusions. This database will leverage both the unique information available to the NIPC through FBI investigations and information available from the intelligence community and open sources. Having these analytic functions at the NIPC is a central element of its ability to carry out its preventive mission.

The NIPC also shares information via its InfraGard Initiative. All 56 FBI field offices now have InfraGard chapters. Just in the last six months the InfraGard Initiative has added over 1000 new members to increase the overall membership to over 1800. It is the most extensive government-private sector partnership for infrastructure protection in the world, and is a service we provide to InfraGard members free of charge. InfraGard expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices and several of its Resident Agencies (subdivisions of the larger field offices).

A key element of the InfraGard initiative is the confidentiality of reporting by members. The reporting members edit out the identifying information about themselves on the notices that are sent to other members of the InfraGard network. This process is called sanitization and it protects the information provided by the victim of a cyber attack. Much of the information provided by the private sector is proprietary and is treated as such. InfraGard provides its membership with the capability to write an encrypted sanitized report for dissemination to other members. This measure helps to build a trusted relationship with the private sector and at the same time encourages other private sector companies to report cyber attacks to law enforcement.

InfraGard held its first national congress from June 12-14, 2001. This conclave provided an excellent forum for NIPC senior managers and InfraGard members to exchange ideas. InfraGard's success is directly related to private industry's involvement in protecting its critical systems, since private industry owns most of the infrastructures. The dedicated work of the NIPC and the InfraGard members is paying off. InfraGard has already prevented cyber attacks by discretely alerting InfraGard members to compromises on their systems.

The NIPC is also working with the Information Sharing and Analysis Centers (ISACS) established under the auspices of PDD-63. The North American Electric Reliability Council (NERC) serves as the electric power ISAC. The NIPC has developed a program with the NERC for an Indications and Warning System for physical and cyber attacks. Under the program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the program have stated that the information and analysis provided by the NIPC makes this program especially worthwhile. NERC has recently decided to expand this initiative nationwide. This initiative will serve as a good example of government and industry working together to share information, and the Electric Power Indications and Warning System will provide a model for the other critical infrastructures.

With the assistance of NERC, the NIPC conducted a six-month pilot program and a series of workshops to familiarize participants with the program's operating procedures. The workshops included hands-on table-top exercises that required program participants to work through simulated scenarios dealing with credible cyber and physical attacks directed against the power industry. In the summer of 2000, a half-day table-top exercise was held for companies in NERC's Mid-Atlantic region allowing them to role-play in responding to simulated incidents pre-scripted by NIPC and company representatives. Since October 2000, the NIPC supported by NERC conducted three workshops around the country in order to provide program participants with hands-on experience in responding to attacks against the electric power grid. Eventually, the NIPC will strive to have similar models and exercises for all the infrastructures.

The NIPC serves as sector liaison for the Emergency Law Enforcement Services (ELES) Sector at the request of the FBI. The NIPC completed the ELES Sector Plan in February, 2001. The ELES Sector Plan was the first completed sector report under PDD-63 and was delivered to the White House on March 2, 2001. At the Partnership for Critical Infrastructure Security in Washington, D.C., in March, 2001, the ELES Plan was held up as a model for the other sectors. The NIPC also sponsored the formation of the Emergency Law Enforcement Services Sector Forum, which meets quarterly to discuss issues relevant to sector security planning. The Forum contains federal, state, and local representatives. The next meeting of the Forum is scheduled for September, 2001.

The Plan was the result of two years' work in which the NIPC surveyed law enforcement agencies concerning the vulnerabilities of their infrastructure, in particular their data and communications systems. Following the receipt of the survey results, the NIPC and the ELES Forum produced the ELES Sector Plan. The NIPC also produced a companion "Guide for State and Local Law Enforcement Agencies" that provides guidance and a "toolkit" that law enforcement agencies can use when implementing the activities suggested in the Plan.

The importance of the ELES Sector Plan and the Guide cannot be overstated. These documents will aid some 18,000 police and sheriff's departments located in towns and neighborhoods to better protect themselves from attack by providing them with useful checklists and examples of procedures they can use to improve their security. Since the local police are usually among the first responders to any incident threatening public safety, their protection is vital.

Also, the NIPC has prepared model agreements to promote information sharing and has presented them for negotiation to the following existing or potential ISACs: Association of Metropolitan Water Agencies (AMWA), Financial Services, Information Technology, National Association of State Chief Information Officers (NASCIO), National Coordinating Center (NCC) for Telecommunications, National Emergency Management Association (NEMA), National Petroleum Council (NPC), and US Fire Administration (USFA). Offers for information sharing arrangements will be made to the emerging Rail and Aviation ISACs. We are promoting the establishment of an ISAC for the Public Health Services Sector. With respect to the federal agencies, NIPC has developed a model agreement for use in promoting information sharing with the other 70 plus executive branch agencies, and will soon launch a campaign to formalize these arrangements.

Detection:

Given the ubiquitous vulnerabilities in existing Commercial Off-the-Shelf (COTS) software, intrusions into critical systems are inevitable for the foreseeable future. Thus detection of these viruses, worms, and other intrusions is crucial if the U.S. Government and critical infrastructure owners and operators are going to be able to respond effectively. To improve our detection capabilities, we first need to ensure that we are fully collecting, sharing, and analyzing all extant information. It is often the case that intrusions can be discerned simply by collecting bits of information from various sources; conversely, if we do not collate these pieces of information for analysis, we might not detect the intrusions at all. Thus the NIPC's role in collecting information from all sources and performing analysis in itself serves the role of detection.

Federal Agency system administrators need to work with NIPC. PDD-63 makes clear the importance of such reporting. It states, "All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law."

In order to carry out this mandate, the NIPC is working closely with FedCIRC and the anti-virus community. The NIPC and the Computer Emergency Response Team (CERT) at Carnegie Mellon University have formed a mutually beneficial contractual relationship. The NIPC receives information from the CERT that it incorporates into strategic and tactical analyses and utilizes as part of its warning function. The NIPC is routinely in telephonic contact with CERT/CC and the anti-virus community for purposes of sharing vulnerability and threat information on a real-time basis. CERT/CC input is often sought when an NIPC warning is in production. The NIPC also provides information to the CERT that it obtains through investigations and other sources, using CERT as one method for distributing information (normally with investigative sources sanitized) to security professionals in industry and to the public. The Watch also provides the NIPC *Daily Report* to the CERT/CC via Internet e-mail. On more than one occasion, the NIPC provided CERT with the first information regarding a new threat, and the two organizations have often collaborated in putting information out about incidents and threats.

The NIPC has an excellent relationship with the General Services Administration's Federal Computer Incident Response Center (FedCIRC). NIPC and FedCIRC are both crucial to effective cyber defense but serve different roles. When an agency reports an incident, FedCIRC works with the agency to identify the type of incident, mitigate any damage to the agency's system, and provide guidance to the agency on recovering from the incident. FedCIRC has detailed a person to the NIPC Watch Center. In addition, the NIPC sends draft alerts, advisories, and assessments on a regular basis to FedCIRC for input and commentary prior to their release. NIPC and FedCIRC information exchange assists both centers with their analytic products. The NIPC and FedCIRC are currently discussing ways to improve the flow of information between the two organizations and encourage federal agency reporting of incident information to the NIPC.

In response to victim reports, the NIPC sponsored the development of tools to detect malicious software code. For example, in December 1999, in anticipation of possible Y2K related malicious conduct, the NIPC posted a detection tool on its web site that allowed systems administrators to detect the presence of certain Distributed Denial of Service (DDoS) tools on their networks. In those cases, hackers planted tools named Trinoo, Tribal Flood Net (TFN), TFN2K, and Stacheldraht (German for barbed wire) on a large number of unwitting victim systems. Then when the hacker sent a particular command, the victim systems in turn began sending messages against target systems. The target systems became overwhelmed with the traffic and were unable to function. Users trying to access the victim system were denied its services. The NIPC's detection tools were downloaded thousands of times and have no doubt prevented many DDoS attacks. In fact, in this cutting edge area of network security, the NIPC's Special Technologies and Applications Unit (STAU) received the 2000 SANS Award.

If we determine that an intrusion is imminent or underway, the NIPC Watch is responsible for formulating assessments, advisories, and alerts, and quickly disseminating them. The substance of those products will come from work performed by NIPC analysts. We can notify both private sector and government entities using an array of mechanisms so they can take protective steps. In some cases these warning products can prevent a wider attack; in other cases warnings can mitigate an attack already underway. This was the case both with our warnings regarding e-commerce vulnerabilities and the more recent warnings posted about Code Red. Finally, these notices can prevent attacks from ever happening in the first place. For example, the NIPC released an advisory on March 30, 2001 regarding the "Lion Internet Worm," which is a DDoS tool targeting Unix-based systems. Based on all-source information and analysis, the NIPC alerted systems administrators how to look for this compromise of their system and what specific steps to take to remove the tools if they are found. This alert was issued after consultation with FedCIRC, JTF-CNO, a private sector ISAC, and other infrastructure partners.

Mitigation/Response:

Despite our efforts, we know that critical U.S. systems will continue to be attacked. The perpetrators could be criminal hackers, teenagers, cyber protestors, terrorists, or foreign intelligence services. In order to identify an intruder, the NIPC coordinates an investigation that gathers information using either criminal investigative or foreign counter-intelligence authorities, depending on the circumstances. We also rely on the assistance of other nations when appropriate.

In the cyber world, determining the "who, what, where, when, and how" is difficult. An event could be a system probe to find vulnerabilities or entry points, an intrusion to steal data or plant sniffers or malicious code, the spreading of a virus or worm, an act of teenage vandalism, an attack to disrupt or deny service, or even an act of war. The crime scene itself is totally different from the physical world in that it is dynamic--it grows, contracts, and can change shape. Further, the tools used to perpetrate a major infrastructure attack can be the same ones that are freely available on the Internet and used for other cyber intrusions (such as simple hacking, foreign intelligence gathering, or organized crime activity to steal property), making identification more difficult. Obtaining reliable information is necessary not only to identify the perpetrator but also to determine the size and nature of the intrusion and what information security response may prevent further attack: how many systems are affected, what techniques are being used, and what is the purpose of the intrusions--disruption, economic espionage, theft of money, etc..

Relevant information could come from existing criminal investigations or other contacts at the FBI Field Office level. It could come from the U.S. Intelligence Community, other U.S. Government agency information, private sector contacts, the media, other open sources, or foreign law enforcement contacts. The NIPC's role is to coordinate, collect, analyze, and disseminate this information. Indeed this is one of the principal reasons the NIPC was created.

Because the Internet by its nature embodies a degree of anonymity, our government's proper response to an attack first requires significant investigative steps. Investigators typically need a full range of criminal and/or national security authorities to determine who launched the attack or authored the malicious code. There are many federal statutes that criminalize unauthorized conduct over the Internet. The law prohibits a wide variety of acts conducted with computers, some of which are traditional crimes (such as wire fraud and pornography) and others of which are more technology-specific crimes, such as hacking.

The primary Federal statute that criminalizes breaking into computers and spreading malicious viruses and worms is the Computer Fraud and Abuse Act, codified at Title 18 of the United States Code, Section 1030. Other statutes that are typically implicated in a hacking case include Section 1029 of Title 18, which criminalizes the misuse of computer passwords, and Section 2511 of Title 18, which criminalizes those hackers that break into systems and install "sniffers" to illegally intercept electronic communications. In order to investigate these violations, law enforcement relies on traditional sources and techniques to gather evidence, ranging from the public's voluntary assistance to court authorized searches and court authorized surveillance. We have similar investigative capabilities when pursuing cases in which foreign powers or terrorist organizations are impairing the confidentiality, integrity, or availability of our networks, although in these cases our legal authority typically is derived from the National Security Act of 1947 and the Foreign Intelligence Surveillance Act (FISA), both codified in Title 50 of the United States Code, rather than pursuant to the Federal Criminal Code.

The FBI has designated the NIPC to act as the program manager for all of its computer intrusion investigations, and the NIPC has made enormous strides in developing this critical nationwide program. In that connection, the NIPC works closely with the Department of Justice Criminal Division's Computer Crime and Intellectual Property Section, Office of Intelligence Policy and Review, and the U.S. Attorney's Offices in coordinating legal responses.

In the event of a national-level set of intrusions into significant systems or a major virus outbreak, the NIPC will form a Cyber Crisis Action Team (C-CAT) to coordinate response activities and use the facilities of the FBI's Strategic Information and Operations Center (SIOC). The team will have expert investigators, computer scientists, analysts, watch standers, and other U.S. government agency representatives. Part of the U.S. government team might be physically located at FBI Headquarters and part of the team may be just electronically connected. The C-CAT will immediately contact field offices responsible for the jurisdictions where the attacks are occurring and where the attacks may be originating. The C-CAT will continually assess the situation and support/coordinate investigative activities, issue updated warnings, as necessary, to all those affected by or responding to the crisis. The C-CAT will then coordinate the investigative effort to discern the scope of the attack, the technology being used, and the possible source and purpose of the attack.

The NIPC's placement in the FBI's Counterterrorism Division will allow for a seamless FBI response in the event of a terrorist action that encompasses both cyber and physical attacks. The NIPC and the other elements of the FBI's Counterterrorism Division have conducted joint operations and readiness exercises in the FBI's SIOC. We are prepared to respond when called upon.

As the Worm Turns

Over the past several years we have seen a wide range of cyber threats ranging from defacement of websites by juveniles to devastating worms and viruses released on the Internet. Some of these are obviously more significant than others. The theft of national security information from a government agency, or the interruption of electrical power to a major metropolitan area would have greater consequences for national security, public safety, and the economy than the defacement of a web-site. But even the less serious categories have real consequences and, ultimately, can undermine confidence in e-commerce and violate privacy or property rights. A web site hack that shuts down an e-commerce site can have disastrous consequences for a business. An intrusion that results in the theft of credit card numbers from an online vendor can result in significant financial loss and, more broadly, reduce consumers' willingness to engage in e-commerce. Because of these implications, it is critical that we have in place the programs and resources to investigate and, ultimately, to deter these sorts of crimes.

Virus attacks have become more prevalent in recent years. While tens of thousands of viruses and worms exist in the wild, the vast majority of them are not serious threats. But just a few of them have unleashed havoc on the networks. A survey by InformationWeek and PriceWaterhouseCoopers conducted in the summer of 2000 estimated viruses would cause $1.6 trillion worth of damage in the year 2000 worldwide. That figure is larger than the gross domestic product of all but a handful of nations and demonstrates the huge economic costs that viruses and worms can have on the global economy.

In addition, because it is often difficult to determine whether a virus outbreak or worm propagation is the work of an individual with criminal motives or a foreign power, we must treat certain cases for their potential as a national security matter until we gather sufficient information to determine the nature, purpose, scope, and perpetrator of the attack. While we cannot discuss ongoing investigations, we can discuss closed cases that involve FBI and other agency investigations in which the intruder's methods and motivation were similar to what we are currently seeing. A few illustrative cases are described below:

As discussed above, Code Red infected over 150,000 systems and has yet to be stopped. But this is only the most recent in a growing list of computer worms. The first worm to get the attention of the computer users community was the Morris worm, released on November 2, 1988 by Robert Tappan Morris, a 23 year old graduate student at Cornell University. The infant Internet community had never seen anything like this worm. In a matter of hours it had infected 6,000 machines and, while it did not damage files, it clogged the machines and made them unusable. The machines had to be disconnected from the Internet and repaired. Morris was convicted of violating the Computer Fraud and Abuse Act and sentenced to three years probation, 400 hours of community service, and fined $10,500.

In May 2000 companies and individuals around the world were stricken by the "Love Bug," a virus (or, technically, a "worm") that traveled as an attachment to an e-mail message and propagated itself extremely rapidly through the victim's address books. The virus/worm also reportedly penetrated at least 14 federal agenciesCincluding the Department of Defense (DOD), the Social Security Administration, the Central Intelligence Agency, the Immigration and Naturalization Service, the Department of Energy, the Department of Agriculture, the Department of Education, the National Aeronautics and Space Administration (NASA), along with the House and Senate.

Investigative work by the FBI's New York Field Office, with assistance from the NIPC, traced the source of the virus to the Philippines within 24 hours. The FBI then worked, through the FBI Legal Attaché in Manila, with the Philippines' National Bureau of Investigation, to identify the perpetrator. The speed with which the virus was traced back to its source is unprecedented. The prosecution in the Philippines was hampered by the lack of a specific computer crime statute. Nevertheless, Onel de Guzman was charged on June 29, 2000 with fraud, theft, malicious mischief, and violation of the Devices Regulation Act. However, those charges were dropped in August by Philippine judicial authorities. As a postscript, it is important to note that the Philippines' government on June 14, 2000 reacted quickly and approved the E-Commerce Act, which now specifically criminalizes computer hacking and virus propagation. Also, the NIPC continues to work with other nations to provide guidance on the need to update criminal law statutes.

In some cases, we have been able to prevent the release of malicious code viruses against public systems. On March 29, 2000, FBI Houston initiated an investigation when it was discovered that certain small businesses in the Houston area had been targeted by someone who was using their Internet accounts in an unauthorized manner and causing their hard drives to be erased. The next day, FBI Houston conducted a search warrant on the residence of an individual who allegedly created a computer "worm" that seeks out computers on the Internet. This "worm" looked for computer networks that have certain enabled sharing capabilities, and uses them for the mass replication of the worm. The worm caused the hard drives of randomly selected computers to be erased. The computers whose hard drives are not erased actively scan the Internet for other computers to infect and force the infected computers to use their modems to dial 911. Because each infected computer can scan approximately 2,550 computers at a time, this worm could have the potential to create a denial of service attack against the 911 system. The NIPC issued a warning to the public through the NIPC webpage, SANS, InfraGard, and teletypes to government agencies. On May 15, 2000 Franklin Wayne Adams of Houston was charged by a federal grand jury with knowingly causing the transmission of a program onto the Internet that caused damage to a protected computer system by threatening public health and safety and by causing loss aggregated to at least $5000. Adams was also charged with unauthorized access to electronic or wire communications while those communications were in electronic storage. On April 5, 2001, Adams was sentenced to 5 years probation and fined $12,353 restitution. Under the terms of his sentencing, Adams is restricted to using a computer only for work and educational purposes.

National security threats remain our top concern. As Dr. Lawrence Gershwin, National Intelligence Officer for Science and Technology, told the Joint Economic Committee in June, 2001, "For attackers, viruses and worms are likely to become more controllable, precise, and predictable--making them more suitable for weaponization. Advanced modeling and simulation technologies are likely to assist in identifying critical nodes for an attack and conducting battle damage assessments." The NIPC is concerned about three specific categories of national security intruders: terrorists, foreign intelligence services, and information warriors. As Gershwin noted in June, "Most U.S. adversaries have access to the technology needed to pursue computer network operations."

Terrorists groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely. In his statement on the worldwide threat in 2000, Director of Central Intelligence George Tenet testified that terrorists groups, "including Hizbollah, HAMAS, the Abu Nidal organization, and Bin Laden's al Qa'ida organization are using computerized files, e-mail, and encryption to support their operations." In one example, convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his laptop computer. While we have not yet seen these groups employ cyber tools as a *weapon* to use against critical infrastructures, their reliance on information technology and acquisition of computer expertise are clear warning signs. During the riots on the West Bank in the fall of 2000, Israeli government sites were subjected to e-mail flooding and "ping" attacks. The attacks originated with sympathetic Islamic elements trying to inundate the systems with email messages. As one can see from these examples overseas, "cyber terrorism" which refers to malicious conduct in cyberspace to commit or threaten to commit acts dangerous to human life, or against a nation's critical infrastructures, such as such as energy, transportation, or government operations in order to intimidate or coerce a government or civilian population, or any segment thereof, in furtherance of political or social objectives – is a very real threat.

Foreign intelligence services have adapted to using cyber tools as part of their information gathering tradecraft. While I cannot go into specific cases, there are overseas probes against U.S. government systems every day. It would be naive to ignore the possibility or even probability that foreign powers were behind some or all of these probes. The motivation of such intelligence gathering is obvious. By coordinating law enforcement and intelligence community assets and authorities in one Center, the NIPC can work with other agencies of the U.S. government to detect these foreign intrusion attempts.

The prospect of "information warfare" by foreign militaries against our critical infrastructures is perhaps the greatest potential cyber threat to our national security. We know that many foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States or other nations. In testimony in June, 2001 National Intelligence Officer Gershwin stated that "for the next 5 to 10 years or so, only nation states appear to have the discipline, commitment and resources to fully develop the capabilities to attack critical infrastructures."

Conclusion

While the NIPC has accomplished much over the last three years in building the first national-level operational capability to respond to cyber intrusions, much work remains. We have learned from cases that successful network investigation is highly dependent on expert investigators and analysts, with state-of-the-art equipment and training. We have had the resources to build some of that capability both in the FBI Field Offices and at the NIPC, but we have much work ahead if we are to build our resources and capability to keep pace with the changing technology and growing threat environment, while at the same time being able to respond to several major incidents at once.

We are building the agency to agency, government to private sector, foreign liaison, and law enforcement partnerships that are vital to this effort. The NIPC is well suited to foster these partnerships since it has analysis, information sharing, outreach, and investigative missions. We are working with the executives in the infrastructure protection community to foster the development of safe and secure networks for our critical infrastructures. While this is a daunting task, we are making progress.

Within the federal sector, we have seen how much can be accomplished when agencies work together, share information, and coordinate their activities as much as legally permissible. But on this score, too, more can be done to achieve the interagency and public-private partnerships called for by PDD-63. We need to ensure that all relevant agencies are sharing information about threats and incidents with the NIPC and devoting personnel and other resources to the Center so that we can continue to build a truly interagency, "national" center. Finally, we must work with Congress to make sure that policy makers understand the threats we face in the Information Age and what measures are necessary to secure our Nation against them. I look forward to working with the Members and Staff of this Subcommittee to address these vitally important issues.

Thank you.

Mr. HORN. Thank you very much. We appreciate your testimony and all your excellent people over there.

We now go to Jeff Carpenter. He is the manager of the CERT Coordination Center of Carnegie-Mellon University and the CERT I think has probably got a patent on it or a copyright, but it stands for Computer Emergency Response Team. We have been looking with great interest over the last few years that in all our feeling, Carnegie-Mellon University is ahead of the pack in terms of the universities of America. So thank you very much for coming.

STATEMENT OF JEFFREY J. CARPENTER, MANAGER, CERT COORDINATION CENTER, CARNEGIE MELLON UNIVERSITY

Mr. CARPENTER. Thank you, Mr. Chairman. Thank you for your remarks. My name is Jeff Carpenter. I manage the CERT Coordination Center which is part of the Software Engineering Institute at Carnegie-Mellon University. Thank you for the opportunity to testify before your subcommittee today. I have a formal statement which I am submitting for the record, and I will just summarize my remarks now. Today I'm going to talk about the Code Red worm attacks and the broader implications of those attacks.

In our first full year of operation in 1989, CERT responded to more than 100 computer security incidents. In the year 2000, staff handled more than 21,000 incidents. In total, CERT staff has handled over 63,000 incidents and catalogued more than 3,700 computer vulnerabilities. This testimony is based on that broad experience as well as our specific experience with the Code Red worm.

To begin the story of the Code Red worm, we need to look back to June 19. On that day, we published an advisory describing a vulnerability in Microsoft's Internet information server, Web server software. This vulnerability could allow intruders to compromise computers running vulnerable versions of IIS. This means that an intruder could take control of a vulnerable computer, accessing or changing data on that computer, or using that computer to launch attacks against other organizations.

A month later the first signs of Code Red worm appeared on July 13. Code Red is called a worm because it's self-propagating. When it compromises a computer, the worm looks for computers to compromise, compromises those computers and then those computers begin compromising other computers without the direct intervention of the intruder that initially launched the worm. Code Red took advantage of the fact that many computers on the Internet that were running IIS still a month later were running vulnerable versions of IIS.

On July 19 the more aggressive version of the worm began spreading rapidly. As the day progressed, the rate of computers being scanned and compromised continued to increase exponentially. On July 20 Code Red changed its type of activity. Instead of propagating the worm, it changed into launching a denial of service attack against a high-profile Web site. When this change occurred, the spreading of the attack stopped. By the time that the spreading of the attack stopped, more than 250,000 computers had been compromised and that was unprecedented in a 24-hour time period.

CERT, along with a number of other government and industry organizations, worked over the next few weeks to raise awareness of the need to patch systems immediately. There was a sense of urgency connected with this joint warning because we anticipated that the worm would change back to propagation mode on August 1. Even with the publicity that we did over the next week or so, when the worm started spreading again on August 1, about 150,000 computers were compromised by the next day. So even with the publicity, many machines were not patched.

The significance of Code Red lies beyond the specific activity we've described. Rather, the worm represents a larger problem with Internet security and forecasts what we can expect in the future. My most important message today is not only is the Internet vulnerable to attack today, but it's going to stay vulnerable to attack for the foreseeable future. Systems are vulnerable to problems that have already been discovered, sometimes years ago, and they remain vulnerable to problems that will be discovered in the future.

Multiple factors contribute to this problem. CERT experience shows that intruders will develop exploit scripts for vulnerabilities in products such as IIS. They will then use these scripts to compromise computers and will share these scripts with other intruders so those intruders can attack systems using them.

New exploits are causing damage more quickly than those created in the past. One primary reason is that intruders are developing better techniques for identifying vulnerable computers and exploiting them. The ability of intruders to compromise systems quickly limits the time that security experts have to analyze the problem and warn the Internet community. Likewise, system administrators and users have little time to protect their systems from these attacks.

This year CERT expects to catalog well over 2,000 vulnerabilities by the end of the year. The rate of reports is doubling each year. There's little evidence of improvement in the security of most products. Developers are not devoting sufficient effort to applying lessons learned about sources of vulnerabilities. While we continue to see exploitation of old vulnerabilities, we're also seeing an increase in new vulnerabilities. Many of them have the same root causes and many of them could have been prevented by good software development practices.

System and network administrators are challenged with keeping up with all of the systems they have and all the patches released for those systems. We have found that after a vendor releases a security patch it takes a long time for system administrators to fix all the vulnerable computer systems. It can be months or years before patches are applied to only 90 percent of the vulnerable computers. For example, we still to this day receive reports of outbreaks of the Melissa virus which is over 2 years old.

There are a variety of reasons for the delay. The job might be time-consuming, too complex or low-priority for the system administration's staff to handle. But even in an ideal situation, conscientious system administrators cannot adequately protect their computer systems because other system administrators and users including home users do not adequately protect their systems. The security of each system on the Internet affects the security of other systems.

Federal, State and local governments should be concerned. Their increased use of the Internet to conduct business and provide information has a corresponding increase in the risk of compromise. Action is needed on many fronts. With the technology product development, vendors need to be proactive in proving their software development practices and shipping products that are configured securely out of the box. Improved practices will reduce vulnerabilities in products on the market and reduce risk of compromise. In our experience, once a vulnerability makes it out into the field installed on systems, it's very difficult to have that vulnerability fixed on all of the systems that it reaches. So we want to try to prevent the vulnerabilities from being in the products that get released to the field to begin with.

System administrators also need better tools to manage the updating of software and computers. Home users and business users alike need to be educated on how to operate computers most securely and consumers need to be educated on how to select the products they buy.

To the acquisition community, it's important to evaluate suppliers for product security but the current ways of describing security requirements are immature and the problem today is not the lack of features, it's the software is flawed.

For long-term improvements to occur, the government should sponsor research and development leading to safer operating systems that are also easier to maintain and manage. There should also be increased research in survival of systems that are better able to resist, recognize and recover from attacks while still providing critical functionality.

And finally, the government should provide meaningful infrastructure support for university programs and information security education and research to produce a new generation of experts in this field. Problems such as Code Red will occur again. Solutions are not simple because the underlying causes must be addressed. However, we can make significant progress through changes in software design and development practices and system administration in the knowledge of users and in acquisition practices. Additionally, the government should support research and development and education in computer network security.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Carpenter follows:]

Computer Security Issues that Affect Federal, State, and Local Governments and the Code Red Worm

Testimony of Jeffrey J. Carpenter
Manager, CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Before the
House of Representatives
Committee on Government Reform,
Subcommittee on Government Efficiency,
Financial Management and
Intergovernmental Relations

August 29, 2001

Introduction

Mr. Chairman and Members of the Committee:
My name is Jeffrey Carpenter. I manage the CERT® Coordination Center (CERT/CC), which is part of the Software Engineering Institute (SEI) at Carnegie Mellon University. Thank you for the opportunity to testify on computer security issues that affect the government. Today I will discuss the Code Red worm attacks, the broader implications, and considerations for the future.

The CERT® Coordination Center (CERT/CC) is part of the Survivable Systems Initiative of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The CERT/CC was established in 1988, after an Internet "worm" stopped as much as 10 percent of the computers connected to the Internet. This program—the first Internet security incident to make headline news—was the wake-up call for network security. In response, the CERT/CC was established at the SEI. The center was activated in just two weeks, and we have worked hard to maintain our ability to react quickly.

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, the CERT/CC identifies preventive security practices, conducts research, and provides training to system administrators, managers, and incident response teams. More details about our work are attached to the end of this testimony (see *Meet the CERT Coordination Center*).

In the first full year of operation, 1989, the CERT/CC responded to 132 computer security incidents. In 2000, the staff handled more than 21,700 incidents. In total, the CERT/CC staff has handled well over 63,000 incidents and cataloged more than 3,700 computer vulnerabilities. This testimony is based on that broad experience as well as our specific experience with the Code Red worm.

The Code Red Worm

Of the thousands of vulnerability reports that come into the CERT/CC, it is difficult to predict which ones the intruder community will exploit and how rapidly exploit scripts (computer programs the intruders use to take advantage of a vulnerability in a computer) will become available. CERT/CC security experts analyze every vulnerability and widely disseminate information on the most serious ones. These are published as CERT advisories, which are posted on the CERT/CC web site (www.cert.org) and sent to a mailing list of 150,000 addresses, most of which go to system and network administrators.

On June 19, 2001, we published an advisory describing the vulnerability that was later exploited by the Code Red worm. CERT advisory CA-2001-13, "Buffer Overflow in the IIS Indexing Service DLL," describes a vulnerability in Microsoft's Internet Information Server (IIS—a web server) that could allow an intruder to compromise the web server. This means an intruder could take control of a vulnerable computer, access or change data on that computer, or use that computer to launch attacks against other sites. The advisory includes links to a Microsoft bulletin and patches. (This advisory and other CERT/CC publications on Code Red are appended to this testimony.)

The first signs of the Code Red worm appeared on July 13, 2001. Code Red is a malicious program called a worm because it is self-propagating. When it compromises a computer, the worm uses that computer to begin looking for other vulnerable computers; it then propagates itself to those computers without any user action. Code Red took advantage of the fact that many computers on the Internet ran vulnerable versions of IIS.

On July 19, a more aggressive version of the Code Red worm began spreading rapidly. We published an incident note (IN-2001-08) that describes the activity and the need for system administrators and users to apply the appropriate patch if they are running a vulnerable version of IIS. As the day progressed, the rate of computers being scanned and compromised continued to increase. We were aware of tens of thousands of computers compromised, which was unprecedented for this type of activity in a 24-hour time frame. This increase in activity warranted another advisory—CA-2001-19, "Code Red Worm Exploiting Buffer Overflow in IIS Indexing Service DLL."

On July 20, Code Red changed its type of activity. Instead of propagating, the worm attempted to launch a denial-of-service attack against a high-profile web site. When this change occurred, the worm stopped spreading. The CERT/CC helped to coordinate an effort by the major Internet Service Providers to mitigate the effectiveness of the denial-of-service attack.

By this time, more than 250,000 computers had been compromised. In other words, in the month after the advisories were released by both the CERT/CC and Microsoft, more than 250,000 computers still had not been patched. (Even people who removed the worm remained vulnerable to attack if they did not patch their systems.) The CERT/CC, along with a number of government and industry organizations, worked over the next few weeks to publicize this fact and to raise awareness of the need to patch systems immediately. There was an urgency connected with this joint warning because we anticipated a change back to propagation mode on August 1, 2001.

Even with the publicity, when the worm began propagating again on the first of August, 150,000 computers were compromised by the very next day.

The Implications

The significance of the Code Red worm lies beyond the specific activity we have described. Rather, the worm represents 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; it will stay vulnerable to attack in the foreseeable future. This includes computers used by government organizations at all levels, 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 is that their computer systems are vulnerable both to attack and to being used to further attacks on others. The confidentiality, integrity, and availability of their information is at risk of compromise.

Contributing Factors and Trends

Multiple factors contribute to the problem and pose obstacles to the solutions. They include the nature of intruder activity, the vulnerability of technology on the Internet, and the difficulty of fixing vulnerable systems.

Intruder Activity: The Ease of Exploitation

CERT/CC experience shows that the intruders will develop exploit scripts for vulnerabilities in products such as IIS. They then use these scripts to compromise computers and, moreover, share these scripts so that more attackers can use them. Automation increases the efficiency of the attacks.

New exploits are causing damage more quickly than those created in the past. The Code Red worm spread around the world faster than the so-called Morris worm moved through U.S. computers in 1988, and faster than the Melissa virus in 1999. One primary reason is that intruders are developing better techniques for identifying vulnerable computers and exploiting them. (See the *Attack Sophistication* diagram appended to this testimony.) After the Morris worm in 1988, we saw little significant use of worms until last year. In the past, intruders found vulnerable computers by scanning each computer individually, in effect limiting the number of computers that could be compromised in a short period of time. Now intruders use worm technology to achieve exponential growth in the number of computers scanned and compromised. They can now reach tens of thousands of computers in minutes or hours, where it once took weeks or months.

This 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.

Vulnerability of Technology on the Internet

Last year, the CERT/CC received 1,090 vulnerability reports, more than double the number of the previous year. In the first half of 2001, we have already received 1,151 reports and expect well over 2,000 reports by the end of the year.

Among the reasons for the vulnerabilities are software design and development practices that do not focus sufficiently on security and system administration practices that leave systems vulnerable.

There is little evidence of improvement in the security of most products; developers are not devoting sufficient effort to applying lessons learned about the sources of vulnerabilities. The CERT/CC routinely receives reports of new vulnerabilities. We continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on the security of their products. Until customers demand products that are more secure or there are legal or liability changes, the situation is unlikely to change.

Good security practice is as important in system administration as it is in software development. The Internet is becoming increasingly complex and dynamic, but among those connected to the Internet there is a general lack of adequate knowledge about the network and about security. The rush to the Internet, coupled with a lack of understanding, is leading to the exposure of sensitive data and risk to safety-critical systems. Misconfigured or outdated operating systems, mail programs, and web sites result in vulnerable computer systems that intruders can exploit.

Difficulty of Fixing Vulnerable Systems

With an estimated 2,000 (and climbing) vulnerabilities being discovered each year and exploit scripts available for many, it can be difficult to quickly determine how serious the spread of a particular exploit will be. Analyzing the exploit scripts is time consuming even when source code is available. These obstacles, combined with fast exploitation, make it difficult for security experts to provide timely warnings and workarounds.

System and network administrators are also 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 administrators 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, we still receive reports of outbreaks of the Melissa virus, which is more than two years old.

There are a variety of reasons for the delay. The job might be too time-consuming, too complex, or just at too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long term—system maintenance is never-ending. Because many managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.

Even in an ideal situation, conscientious system administrators cannot adequately protect their computer systems because other system administrators and users, including home users, do not adequately protect *their* systems. People don't keep their anti-virus software up-to-date; and they don't apply patches to close vulnerabilities. Computers on the Internet are more interdependent than most people realize. The security of each system on the Internet affects the security of every other system.

Prognosis for the Future

Things are not going to get better in the foreseeable future. The number of Internet users increases daily (an estimated 109 million computers were connected to the Internet at the beginning of this year). Many users aren't aware of security issues—or aren't aware that their computer can be used to attack others. Even if they are aware, they aren't knowledgeable enough to implement appropriate security. The lack of security on their systems puts all other systems on the Internet at risk.

While we continue to see exploitation of old vulnerabilities, we are also seeing an increase in new vulnerabilities. Many of them have the same root causes. And many of them can be prevented by good software development practices and good system administration practices. The continuing increases in incident reports to the CERT/CC suggest that the use of these practices is limited.

Federal, state, and local governments should be concerned. Their increased use of the Internet to conduct business and provide information results in a corresponding increase in the risk of compromise.

Recommended Actions

Action is needed on many fronts: product development, system administration, home use, and acquisition. The government needs to support research on computer security and network survivability, as well as supporting education.

Technology product development: Most vulnerabilities in products come from a few root causes. They remain in products, waiting to be discovered, and are fixed only after they are discovered while in use. Worse, the same flaws continue to be introduced in new products. Vendors need to be proactive, improving their development practices and shipping products configured securely "out of the box." Improved practices will reduce the vulnerabilities in products on the market and thus reduce the risk of compromise.

System administration: While we tell system and network administrators to keep their systems up to date with security patches and workarounds, the volume of patches and difficulty in installing them makes it very difficult for system and network administrators to keep up to date. System administrators need better tools to manage the updating of software and computers.

Computer users/consumers: 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.

Acquisition: It is important to evaluate suppliers for product security, but the current ways of describing security in requirements are immature. Using a list of features (such as encryption and a firewall) is helpful but not sufficient. The problem is not a lack of features, but software that is flawed.

In addition to improving the way security requirements are described, we recommend that acquisition practices encourage diversity. Malicious code like Melissa and Code Red spread better in a highly homogeneous environment. Diversity improves survival.

Government support: For long-term improvements to occur, the government should do the following:

- Sponsor research and development leading to safer operating systems that are also easier to maintain and manage.
- Sponsor research into survivable systems that are better able to resist, recognize, and recover from attacks while still providing critical functionality.
- Provide meaningful infrastructure support for university programs in information security education and research to produce a new generation of experts in the field.

Conclusion

Problems such as the Red Code worm are likely to occur again. Solutions are not simple because the underlying causes must be addressed. However, we can make significant progress through changes in software design and development practices, in system administration, in the knowledge level of users, and in acquisition practices. Additionally, the government should support research, development, and education in computer and network security.

Attachments to the Testimony

# of Jeffrey J. Carpenter

CERT@ Coordination Center

August 29, 2001

Diagram: Attacker Sophistication

Meet the CERT® Coordination Center

CERT Incident Note IN-2001-10 "Code Red" Worm Crashes IIS 4.0 Servers with URL Redirection Enabled

CERT Incident Note IN-2001-09 "Code Red II": Another Worm Exploiting Buffer Overflow in IIS Indexing Service DLL

Joint Announcement "A Very Real and Present Threat to the Internet"

CERT Advisory CA-2001-23 Continued Threat of the "Code Red" Worm

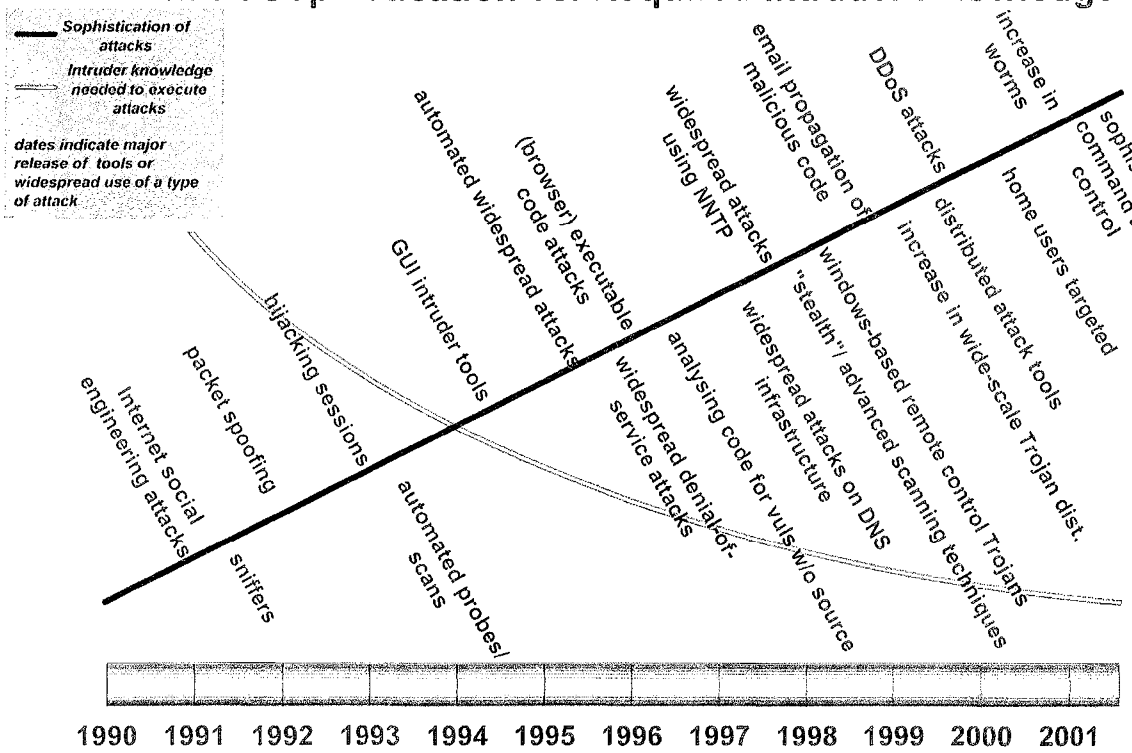
CERT Advisory CA-2001-20 Continuing Threats to Home Users

CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow in IIS Indexing Services DLL

CERT Incident Note IN-2001-08 "Code Red" Worm Exploiting Buffer Overflow in IIS Indexing Service DLL

CERT Advisory CA-2001-13 Buffer Overflow in IIS Indexing Service DLL

Attack Sophistication vs. Required Intruder Knowledge



CERT Coordination Center
www.cert.org

Copyright 1999-2001
Carnegie Mellon University

Meet the CERT® Coordination Center

Overview

Areas of Work

Information Dissemination

Advocacy and Other Interactions with the Community

Appendix A: The CERT/CC Charter

Appendix B: The CERT/CC and the Internet Community

Overview

The CERT Coordination Center (CERT/CC) is located at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the Internet Worm incident, which brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. Since then, the CERT/CC has helped to establish other response teams and our incident handling practices have been adapted by more than 90 response teams around the world.

While we continue to respond to security incidents and analyze product vulnerabilities, our role has expanded over the years. Each year, commerce, government, and individuals grow increasingly dependent on networked systems. Along with the rapid increase in the size of the Internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty of detecting an attack, and increased difficulty of catching the attackers. To better manage these changes, the CERT/CC is now part of the larger SEI Networked Systems Survivability Program, whose primary goals are to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks ("survivability").

To accomplish our goals, we focus our efforts on the following areas of work: survivable network management, survivable network technology, incident handling, incident and vulnerability analysis, and courses and seminars.

We are also committed to increasing awareness of security issues and helping organizations improve the security of their systems. Therefore, we disseminate information through many channels.

--Back to top.--

Areas of Work

Survivable Network Management

Our survivable network management effort focuses on publishing security practices and developing a self-directed method for organizations to improve the security of their network computing systems.

CERT security practices provide concrete, practical guidance that help organizations improve the security of their networked computer systems. These practices address the most pervasive problems, as reported to the CERT/CC. They are technology-neutral for broad application; many of the practices are accompanied by technology-specific instructions for implementing the practice. We have published seven *security improvement modules,* each of which focuses on one aspect of network security. The modules incorporate more than 100 recommended practices and technology-specific implementations. A complete list of the modules, practices, and implementations can be found on the CERT/CC web site at http://www.cert.org/security-improvement/

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a self-directed approach that gives organizations a comprehensive, repeatable technique for identifying risk in their networked systems and keeping up with changes over time. The method takes into consideration assets, threats, and vulnerabilities (both organizationally and technologically) so that the organization gains a comprehensive view of the state of its systems' security. Details are available from http://www.cert.org/octave/

Survivable Network Technology

In the area of survivable network technology, we are concentrating on the technical basis for identifying and preventing security flaws and for preserving essential services if a system is penetrated and compromised. Approaches that are effective at securing bounded systems (systems that are controlled by one administrative structure) are not effective at securing unbounded systems such as the Internet. Therefore, new approaches to system security must be developed. They include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Current work includes the development of our Survivable Network Analysis method and Easel, a simulation language and tool. This work draws on the vast collection of incident data collected by the CERT/CC. For introductory information, technical reports, and more details, see http://www.cert.org/research/

Incident Handling and Analysis

We continue to provide advice to computer system administrators in the Internet community who report security problems. In addition, one of our primary objectives is to analyze the state of Internet security and convey that information to the system administrators, network managers, and others in the Internet community through the various channels described in the Information Dissemination section.

Our understanding of current security problems and potential solutions comes from analysis of security incidents, intrusion techniques, configuration problems, and software vulnerabilities. Contributing to our broad view of the state of security is the information reported to us. Since our inception in 1988, we have received more than 337,000 email messages and 19,000 hotline calls reporting computer security incidents or requesting information. We have handled more than 54,700 computer security incidents and received 3,300 vulnerability reports. Organizations trust us with sensitive information about security compromises and network vulnerabilities because we have proven our ability to keep their identities and other sensitive information confidential.

The scale of emerging networks and the diversity of user communities make it impractical for a single organization to provide universal support for addressing computer security issues. Therefore, the CERT/CC staff regularly works with sites to help them form computer security incident response teams (CSIRTs) and provides guidance and training to both new and existing teams. For more information about this work, see http://www/cert.org/csirts/

Work is under way on AirCERT, an open-source infrastructure for automatically collecting information on security events at Internet sites and automatically handling well-understood attacks.

FedCIRC - FedCIRC is the Federal Computer Incident Response Center, an organization that provides incident response and other security-related services to Federal civilian agencies. FedCIRC is managed by the General Services Administration (GSA). The CERT/CC performs incident and vulnerability analysis for FedCIRC.

More information about FedCIRC is available from http://www.fedcirc.gov/. Federal agencies can contact FedCIRC by sending email to fedcirc-info@fedcirc.gov or by calling the FedCIRC Management Center at (202) 708-5060. To report an incident, affected sites should send email to fedcirc@fedcirc.gov or phone the FedCIRC hotline at (888) 282-0870.

Vulnerability Analysis

The CERT/CC has become a major reporting center for both incidents and vulnerabilities because we have an established reputation for discretion and objectivity. Our connection with the Software Engineering Institute and Carnegie Mellon University contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias.

When we receive a vulnerability report, our vulnerability experts analyze the potential vulnerability and work with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Another source of vulnerability information comes from incident analysis. Repeated incidents of the same type often point to the existence of a vulnerability and, often, the existence of public information or automated tools for exploiting the vulnerability.

The CERT/CC makes vulnerability information widely available through a Vulnerability Database: http://kb.cert.org/vuls/.

Education and Training

We offer public training courses for technical staff and managers of computer security incident response teams as well as for system administrators and other technical personnel interested in learning more about network security. In addition, several CERT/CC staff members teach courses in the Information Security Management specialization of the Master of Information Systems Management program in the H. J. Heinz III School of Public Policy and Management at Carnegie Mellon University. For more information, see http://www.cert.org/training/

--Back to top.--

Information Dissemination

To increase awareness of security issues and help organizations improve the security of their systems, we collect and disseminate information through multiple channels:

- telephone and email
  hotline: (412) 268-7090
  email: cert@cert.org
  mailing list: majordomo@cert.org
- USENET newsgroup: comp.security.announce
- World Wide Web: http://www.cert.org/
- CERT/CC Knowledgebase (the Vulnerability Database is publicly accessible): http://kb.cert.org/vuls/

In addition, headlines about recently published alerts, incident notes, and vulnerability notes are available through an RSS channel.

In addition to responding to more than 19,000 hotline calls and 337,000 email messages, we have published 350 security alerts (advisories, incident notes, vulnerability notes, CERT summaries, and other bulletins).

Publications

Advisories - CERT/CC advisories address Internet security problems. They offer an explanation of the problem, information that helps you determine if your site has the problem, fixes or workarounds, and vendor information. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and the existence of a software patch or workaround. On the day of release, we send advisories to a mailing list, post them to the USENET newsgroup comp.security.announce and make them available on the CERT web site at http://www.cert.org/advisories/.

CERT summaries - We publish the CERT summary as part of our ongoing efforts to disseminate timely information about Internet security issues. The summary is typically published four to six times a year. The primary purpose of the summary is to call attention to the types of attacks currently being reported to the CERT/CC. Each summary includes pointers to advisories or other publications that explain how to deal with the attacks. Summaries are distributed in the same way as advisories.

Incident notes and vulnerability notes - We publish two web documents, incident notes and vulnerability notes, as an informal means for giving the Internet community timely information relating to the security of its sites. Incident notes describe current intruder activities that have been reported to the CERT/CC incident response team. Vulnerability notes describe weaknesses in Internet-related systems that could be exploited but that do not meet the criteria for advisories.

Security Improvement Modules - Security Improvement Modules address an important but narrowly defined problem in network security. They provide concrete, practical guidance that will help organizations improve the security of their network computer systems. The modules are available on the CERT web site at http://www.cert.org/security-improvement/. We have published, in web form only, technology-specific implementation details for the modules.

Other security information - We capture lessons learned from incident handling and vulnerability analysis and make them available to users of the Internet through a web site archive of security information and products. These include answers to frequently asked questions, a security checklist, "tech tips" for system administrators, research and technical reports, and a handbook for new computer security incident response teams.

--Back to top.--

Advocacy and Other Interactions with the Community

The CERT/CC has the opportunity to advocate high-level changes that improve Internet security and network survivability. Additionally, CERT/CC staff members are invited to give presentations at conferences, workshops, and meetings. These activities enhance the understanding of Internet security and related issues.

Forum of Incident Response and Security Teams (FIRST) - FIRST is a coalition of individual response teams around the world. Each response team builds trust within its constituent community by establishing contacts and working relationships with members of that community. These relationships enable response teams to be sensitive to the distinct needs, technologies, and policies of their constituents. FIRST members collaborate on incidents that cross boundaries, and they cross-post alerts and advisories on problems relevant to their constituents.

The CERT/CC was a founding member of FIRST, and staff members continue to be active participants in FIRST. A current list of FIRST members is available from http://www.first.org/team-info/. More than 85 teams belonged to FIRST, and membership applications for additional teams are pending.

Vendor Relations

We work closely with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Staff members have worked to influence the vendors to improve the basic, as shipped, security within their products and to include security topics in their standard customer training courses. We interact with more than 100 vendors, as well as developers of freely available software.

Vendors often provide information to the CERT/CC for inclusion in advisories.

External Events

CERT/CC staff members are regularly invited to give presentations at conferences, workshops, and meetings. We have found this to be an excellent way to help attendees learn more in the area of network information system security and incident response.

Infrastructure Protection

In its incident and vulnerability handling activities, the CERT/CC assigns a higher priority to attacks and vulnerabilities that directly affect the Internet infrastructure (for example, network service providers, Internet service providers, and domain name servers and routers). In addition, CERT/CC staff participates in meetings related to the security of the information infrastructure. One example is meetings of the National Security Telecommunications Advisory Committee's Network Security Information Exchange (NSTAC NSIE) group, which works to reduce vulnerabilities in critical infrastructures.

Media Relations

The CERT/CC works with the news media to raise the awareness of a broad population to the risks they face on the Internet and steps they can take to protect themselves. Ultimately, the increased visibility of security issues may lead consumers to demand increased security in the computer systems and network services they buy.

In the course of a year, the CERT/CC is referred to in major U.S. newspapers and in a variety of other publications, from the *Chronicle of Higher Education* to *IEEE Computer*. Our staff gives interviews to a selected number of reporters, under the guidance of the SEI public affairs manager.

In 2000, the CERT/CC was covered in radio, television, print, and online media around the world, including *Federal Computer News*, *Time*, *Wall Street Journal*, *Computerworld*, *The Washington Post*, *USA Today*, *Forbes*, *US News and World Report*, *Business Week*, *The Toronto Star*, The New York Times Online, CNBC, MSNBC, BBC London, National Public Radio, ABC, CNN, NBC, and more.

The CERT/CC was also named "Best Security Idea or Practice" by *Secure Computing Magazine*. In remarks at the awards ceremony, CERT/CC was referred to as "a beacon to the rest of the information security world," a compliment to both our staff and sponsors.

--Back to top.--

Appendix A: The CERT/CC Charter

The CERT/CC is chartered to work with the Internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents. In particular, our mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

--Back to top.--

Appendix B: The CERT/CC and the Internet Community

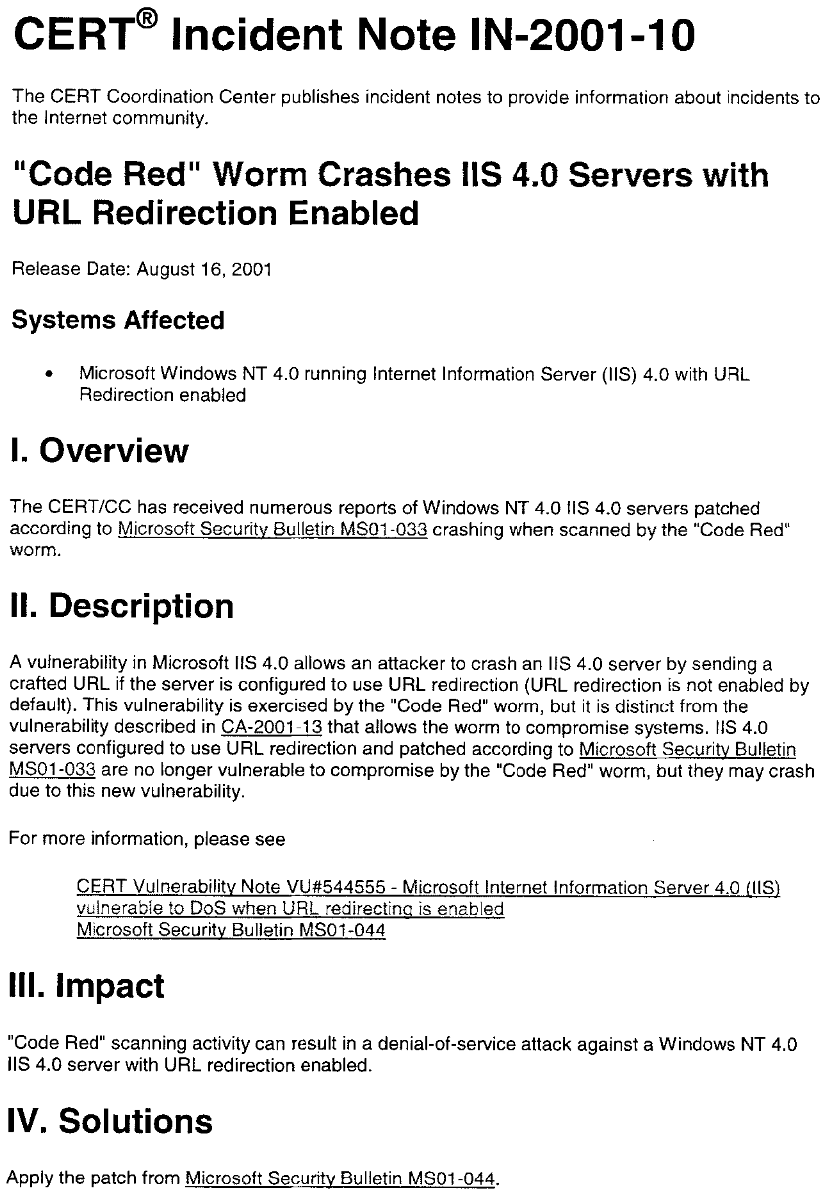
The CERT/CC operates in an environment in which intruders form a well-connected community and use network services to quickly distribute information on how to maliciously exploit vulnerabilities in systems. Intruders dedicate time to developing programs that exploit vulnerabilities and to sharing information. They have their own publications, and they regularly hold conferences that deal specifically with tools and techniques for defeating security measures in networked computer systems.

In contrast, the legitimate, often overworked, system administrators on the network often find it difficult to take the time and energy from their normal activities to stay current with security and vulnerability information, much less design patches, workarounds (mitigation techniques), tools, policies, and procedures to protect the computer systems they administer.

In helping the legitimate Internet community work together, we face policy and management issues that are perhaps even more difficult than the technical issues. For example, one challenge we routinely face concerns the dissemination of information about security vulnerabilities. Our experience suggests that the best way to help members of the network community to improve the security of their systems is to work with a group of technology producers and vendors to develop workarounds and repairs for security vulnerabilities disclosed to the CERT/CC. To this end, in the absence of a major threat, we do delay disclosing vulnerabilities to give vendors an opportunity to develop a solution. Our vulnerability disclosure policy contains details and an FAQ.

Disclaimers and copyright information

Last updated May 1, 2001.



CERT® Incident Note IN-2001-10

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

"Code Red" Worm Crashes IIS 4.0 Servers with URL Redirection Enabled

Release Date: August 16, 2001

Systems Affected

- Microsoft Windows NT 4.0 running Internet Information Server (IIS) 4.0 with URL Redirection enabled

I. Overview

The CERT/CC has received numerous reports of Windows NT 4.0 IIS 4.0 servers patched according to Microsoft Security Bulletin MS01-033 crashing when scanned by the "Code Red" worm.

II. Description

A vulnerability in Microsoft IIS 4.0 allows an attacker to crash an IIS 4.0 server by sending a crafted URL if the server is configured to use URL redirection (URL redirection is not enabled by default). This vulnerability is exercised by the "Code Red" worm, but it is distinct from the vulnerability described in CA-2001-13 that allows the worm to compromise systems. IIS 4.0 servers configured to use URL redirection and patched according to Microsoft Security Bulletin MS01-033 are no longer vulnerable to compromise by the "Code Red" worm, but they may crash due to this new vulnerability.

For more information, please see

> CERT Vulnerability Note VU#544555 - Microsoft Internet Information Server 4.0 (IIS) vulnerable to DoS when URL redirecting is enabled
> Microsoft Security Bulletin MS01-044

III. Impact

"Code Red" scanning activity can result in a denial-of-service attack against a Windows NT 4.0 IIS 4.0 server with URL redirection enabled.

IV. Solutions

Apply the patch from Microsoft Security Bulletin MS01-044.

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32061

V. Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are affected by this activity, please send mail to cert@cert.org.

Author(s): Brian B. King

This document is available from: http://www.cert.org/incident_notes/IN-2001-10.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site
http://www.cert.org/
To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties

of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

CERT® Incident Note IN-2001-09

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

"Code Red II:" Another Worm Exploiting Buffer Overflow In IIS Indexing Service DLL

Release Date: August 6, 2001

Systems Affected

- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed
- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)
- Cisco 600 series DSL routers

I. Overview

The CERT/CC has received reports of new self-propagating malicious code exploiting the vulnerability described in CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. These reports indicate that the worm has already affected thousands of systems. This new worm is being called "Code Red II," however, except for using the same buffer overflow mechanism, it is different from the original "Code Red" worm described in CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL.

The "Code Red II" worm causes system level compromise and leaves a backdoor on certain machines running Windows 2000. Vulnerable Windows NT 4.0 systems could experience a disruption of the IIS service.

II. Description

The "Code Red II" worm is self-propagating malicious code that exploits a known vulnerability in Microsoft IIS servers (CA-2001-13).

Attack Cycle

The "Code Red II" worm attacks as follows:

1. The "Code Red II" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found. Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit the buffer overflow in the Indexing Service described in CA-2001-13
2. The same exploit is sent to each of the randomly chosen hosts due to the self-propagating nature of the worm. However, there are varied consequences depending on the configuration of the host which receives this request.

- ○ **Unpatched Windows 2000 servers running IIS 4.0 or 5.0 with Indexing Service installed** are likely to be compromised by the "Code Red II" worm.
- ○ **Unpatched Windows NT servers running IIS 4.0 or 5.0 with Indexing Server 2.0 installed** could experience crashes of the IIS server.
- ○ **Unpatched Cisco 600-series DSL routers** will process the HTTP request thereby exploiting an unrelated vulnerability which causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
- ○ **Patched systems, or systems not running IIS with an HTTP server listening on TCP port 80** will probably accept the HTTP request, return with an "HTTP 4xx" error message, and potentially log this request in an access log.

3. If the exploit is successful, the worm begins executing on the victim host.

Payload

Upon successful compromise of a system, the worm

1. Checks to see if it has already infected this system by verifying the existence of the `CodeRedII` atom. If the worm finds this atom it sleeps forever. Otherwise it creates this atom and continues the infection process. Reference information regarding atoms may be found at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ipc/hh/winbase/atoms_0p83.asp
2. Checks the default system language, and spawns threads for propagation. If the default system language is "Chinese (Taiwanese)" or "Chinese (PRC)", 600 threads will be spawned to scan for 48 hours. Otherwise, 300 threads will be created which will scan for 24 hours.
3. Copies `%SYSTEM%\CMD.EXE` to `root.exe` in the IIS `scripts` and `MSADC` folders. Placing `CMD.EXE` in a publicly accessible directory may allow an intruder to execute arbitrary commands on the compromised machine with the privileges of the IIS server process.
4. Creates a Trojan horse copy of `explorer.exe` and copies it to `C:\` and `D:\`. The Trojan horse `explorer.exe` calls the real `explorer.exe` to mask its existence, and creates a virtual mapping which exposes the `C:` and `D:` drives.

   On systems not patched against the "Relative Shell Path" vulnerability (http://www.microsoft.com/technet/security/bulletin/MS00-052.asp), this Trojan horse copy of `explorer.exe` will run every time a user logs in. In this fashion, certain pieces of the worm's payload have persistence even after a reboot of the compromised machine.

System Footprint

The "Code Red II" worm can be identified on victim machines by the presence of the following string in IIS log files:

```
GET /default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%
u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a
```

The presence of this string in a log file does not neccessarily indicate compromise, it only implies that a "Code Red II" worm attempted to infect the machine.

The worm will create several files on the compromised machines. These files include `c:\explorer.exe` or `d:\explorer.exe`, as well as `root.exe` in the IIS `scripts` or `MSADC` folder. While the existence of the file `root.exe` could indicate compromise, it does not necessarily imply the presence of the "Code Red II" worm. This file name has been used for artifacts of other exploits, including the sadmind/IIS worm (see CA-2001-11).

Network Footprint

A host running an active instance of the "Code Red II" worm will scan random IP addresses on port 80/TCP looking for other hosts to infect. The IP addresses scanned by the "Code Red II" worm are determined in a probabilistic manner:

- There is a **one in two** chance that a given thread will scan random IP addresses with the same first byte as the infected host.
- There is a **three in eight** chance that a given thread will scan random IP addresses with the same first two bytes as the infected host.
- There is a **one in eight** chance that a given thread will scan random IP addresses.

Additional detailed analysis of this worm has been published by eEye Digital Security at http://www.eeye.com.

III. Impact

Intruders can execute arbitrary commands within the `LocalSystem` security context on Windows 2000 systems infected with the "Code Red II" worm. Compromised systems may be subject to files being altered or destroyed. Denial-of-service conditions may be created for services relying on altered or destroyed files. Hosts that have been compromised are also at high risk for being party to attacks on other Internet sites.

The widespread, automated attack and propagation characteristics of the "Code Red II" may cause bandwidth denial-of-service conditions in isolated portions of the network, particularly near groups of compromised hosts where "Code Red II" is running.

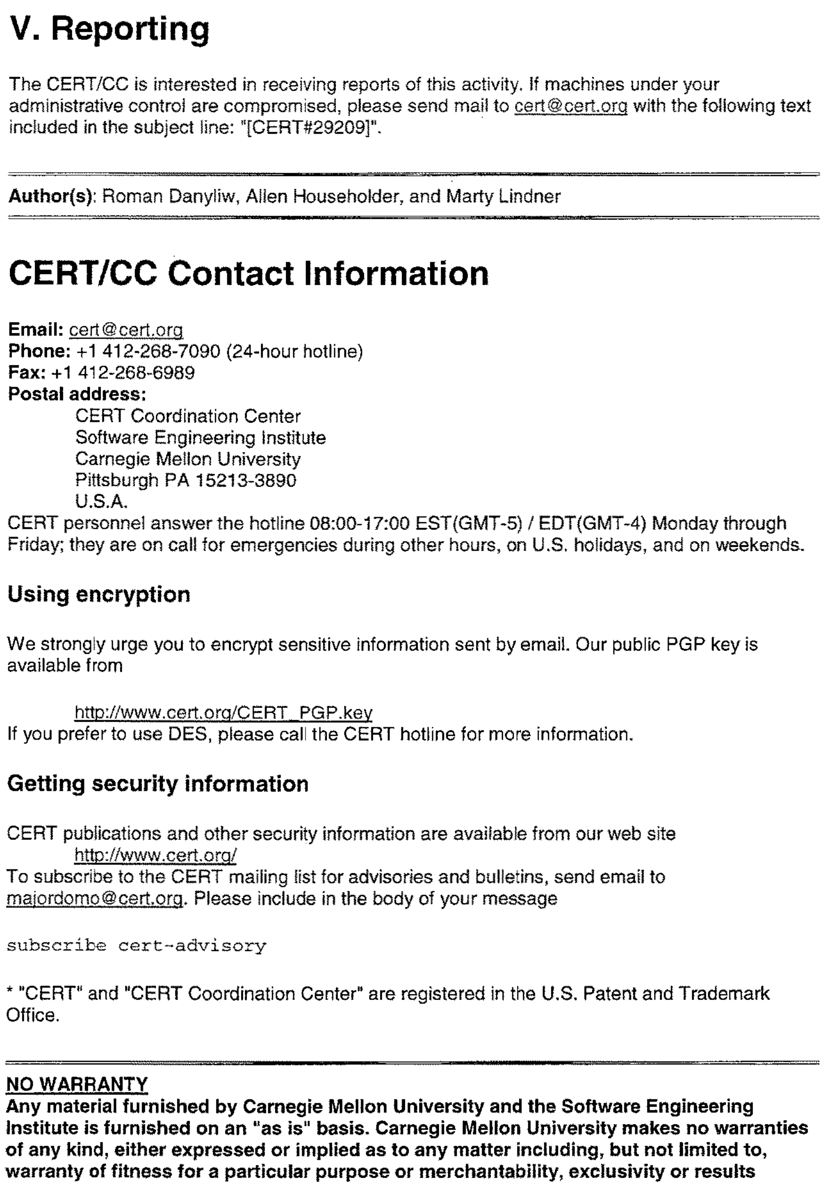
Windows NT 4.0 systems and Cisco 600-series DSL routers may experience denial-of-service as a result of the scanning activity of the worm.

IV. Solutions

Infection by the "Code Red II" worm constitutes a system level compromise. If you believe a host under your control has been compromised, please refer to

> Steps for Recovering from a UNIX or NT System Compromise

Consistent with the security best-practice of denying all network traffic and only selectively allowing that which is required, ingress and egress filtering should be implemented at the network edge. Likewise, controls must be in place to ensure that all software used on a network is properly maintained. See CA-2001-23 Continued Threat of the "Code Red" Worm for more information on these topics.



V. Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#29209]".

Author(s): Roman Danyliw, Allen Householder, and Marty Lindner

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site
http://www.cert.org/
To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

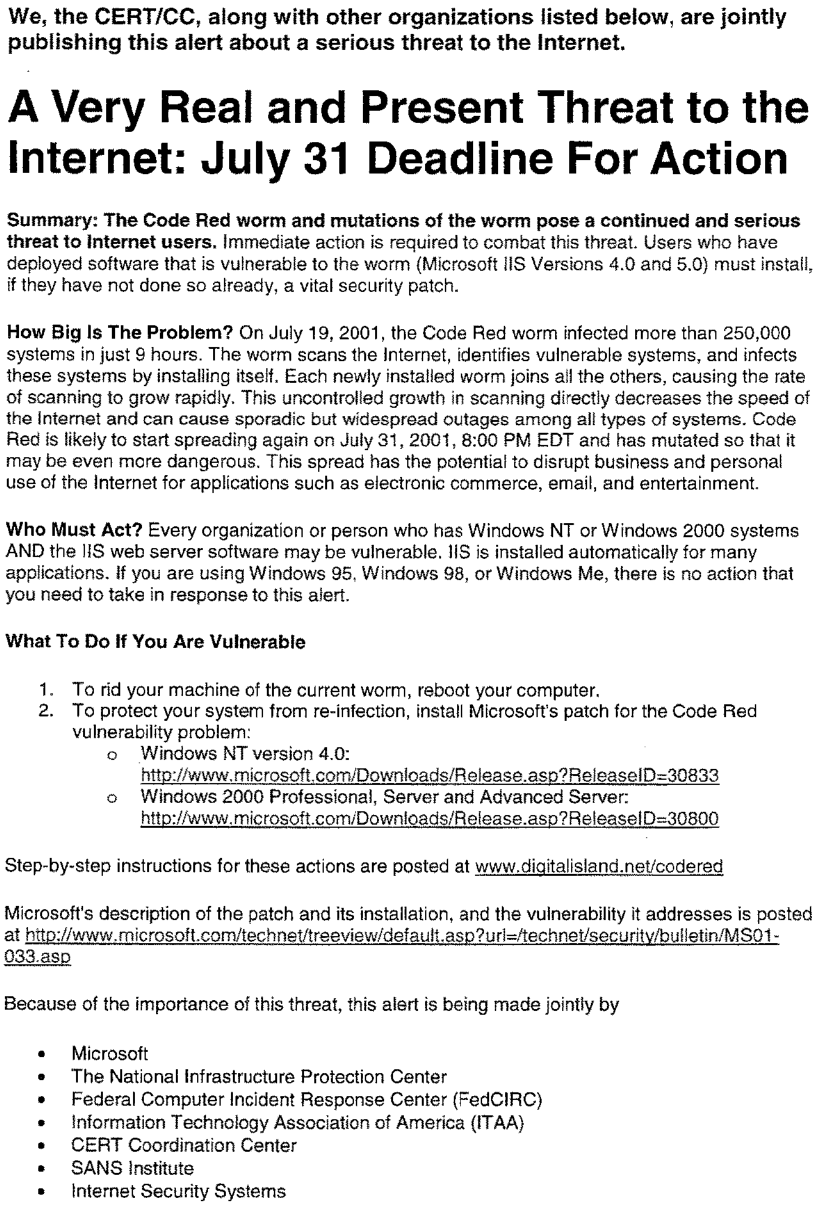
* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
August 6, 2001: Initial Release
```



We, the CERT/CC, along with other organizations listed below, are jointly publishing this alert about a serious threat to the Internet.

A Very Real and Present Threat to the Internet: July 31 Deadline For Action

Summary: The Code Red worm and mutations of the worm pose a continued and serious threat to Internet users. Immediate action is required to combat this threat. Users who have deployed software that is vulnerable to the worm (Microsoft IIS Versions 4.0 and 5.0) must install, if they have not done so already, a vital security patch.

How Big Is The Problem? On July 19, 2001, the Code Red worm infected more than 250,000 systems in just 9 hours. The worm scans the Internet, identifies vulnerable systems, and infects these systems by installing itself. Each newly installed worm joins all the others, causing the rate of scanning to grow rapidly. This uncontrolled growth in scanning directly decreases the speed of the Internet and can cause sporadic but widespread outages among all types of systems. Code Red is likely to start spreading again on July 31, 2001, 8:00 PM EDT and has mutated so that it may be even more dangerous. This spread has the potential to disrupt business and personal use of the Internet for applications such as electronic commerce, email, and entertainment.

Who Must Act? Every organization or person who has Windows NT or Windows 2000 systems AND the IIS web server software may be vulnerable. IIS is installed automatically for many applications. If you are using Windows 95, Windows 98, or Windows Me, there is no action that you need to take in response to this alert.

What To Do If You Are Vulnerable

1. To rid your machine of the current worm, reboot your computer.
2. To protect your system from re-infection, install Microsoft's patch for the Code Red vulnerability problem:
    - Windows NT version 4.0: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833
    - Windows 2000 Professional, Server and Advanced Server: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

Step-by-step instructions for these actions are posted at www.digitalisland.net/codered

Microsoft's description of the patch and its installation, and the vulnerability it addresses is posted at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp

Because of the importance of this threat, this alert is being made jointly by

- Microsoft
- The National Infrastructure Protection Center
- Federal Computer Incident Response Center (FedCIRC)
- Information Technology Association of America (ITAA)
- CERT Coordination Center
- SANS Institute
- Internet Security Systems

- Internet Security Alliance

Last updated July 29, 2001

CERT® Advisory CA-2001-23 Continued Threat of the "Code Red" Worm

Original release date: July 26, 2001
Last revised: August 16, 2001
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed
- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)
- Unpatched Cisco 600 series DSL routers

Overview

Since around July 13, 2001, at least two variants of the self-propagating malicious code "Code Red" have been attacking hosts on the Internet (see CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL). Different organizations who have analyzed "Code Red" have reached different conclusions about the behavior of infected machines when their system clocks roll over to the next month. Reports indicate that there are a number of systems with their clocks incorrectly set, so we believe the worm will begin propagating again on August 1, 2001 0:00 GMT. There is evidence that tens of thousands of systems are already infected or vulnerable to re-infection at that time. Because the worm propagates very quickly, it is likely that nearly all vulnerable systems will be compromised by August 2, 2001.

The CERT/CC has received reports indicating that at least 280,000 hosts were compromised in the first wave.

A translation of this advisory into Polish is available at http://www.cert.pl/CA/CA-2001-23-PL.html.

I. Description

The "Code Red" worm is malicious self-propagating code that exploits Microsoft Internet Information Server (IIS)-enabled systems susceptible to the vulnerability described in CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. Its activity on a compromised machine is time senstive; different activity occurs based on the date (day of the month) of the system clock. The CERT/CC is aware of at least two major variants of the worm, each of which exhibits the following pattern of behavior:

- **Propagation mode (from the 1st - 19th of the month)**: The infected host will attempt to connect to TCP port 80 of randomly chosen IP addresses in order to further propagate the worm. Depending on the configuration of the host that receives this request, there are varied consequences.

- *Unpatched IIS 4.0 and 5.0 servers with Indexing service installed* will almost certainly be compromised by the "Code Red" worm. In the earlier variant of the worm, victim hosts with a default language of English experienced a defacement on all pages requested from the web server. Hosts infected with the later variant did not experience any change in the served content.
- *Unpatched Cisco 600-series DSL routers* will process the HTTP request and trigger an unrelated vulnerability that causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
- *Systems not running IIS, but with an HTTP server listening on TCP port 80* will probably accept the HTTP request, return with an "HTTP 400 Bad Request" message, and potentially log this request in an access log.

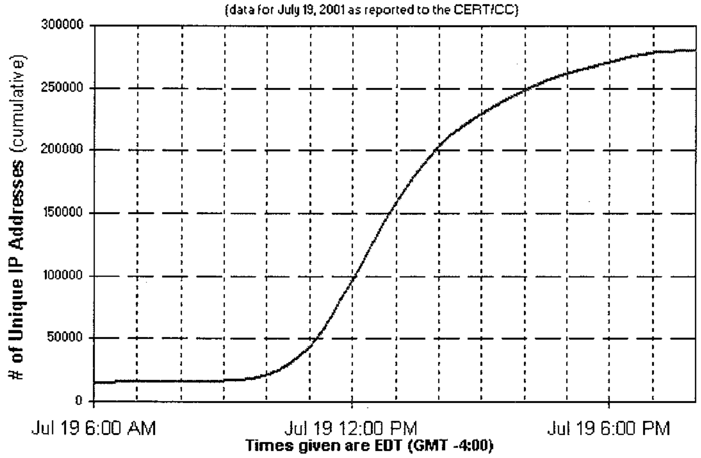
- **Flood mode (from the 20th - 27th of the month)**: A packet-flooding denial-of-service attack will be launched against a specific IP address embedded in the code.
- **Termination (after the 27th day)**: The worm remains in memory but is otherwise inactive.

Detailed technical analysis of the "Code Red" worm can be found in CA-2001-19.

II. Impact

Data reported to the CERT/CC indicates that the "Code Red" worm infected more than 250,000 sytems in just 9 hours. Figure 1 illustrates the activity between 6:00 AM EDT and 8:00 PM EDT on July 19, 2001.

Figure 1: IP Addresses Compromised by the "CodeRed" worm



http://www.cert.org/advisories/CA-2001-23.html

Source: incident data for CERT#36881

NOTE: After 8:00 PM EDT on July 19 (0:00 GMT July 20), the worm switched into flood mode on most infected systems, so the number of infected systems remained fairly constant after that time.

Our analysis estimates that starting with a single infected host, the time required to infect all vulnerable IIS servers with this worm could be less than 18 hours. Since the worm is programmed to continue propagating for the first 19 days of the month, widespread denial of service may result due to heavy scan traffic.

As reported in CA-2001-19, infected systems may experience web site defacement as well as performance degradation as a result of the propagating activity of this worm. This degradation can become quite severe, and in fact may cause some services to stop entirely, since it is possible for a machine to be infected with multiple copies of the worm simultaneously.

Furthermore, it is important to note that the IIS indexing vulnerability that the "Code Red" worm exploits can be used to execute arbitrary code in the Local System security context. This level of privilege effectively gives an attacker complete control of the infected system.

III. Solutions

The CERT/CC encourages all Internet sites to review CA-2001-13 and ensure workarounds or patches have been applied on all affected hosts on your network.

If you believe a host under your control has been compromised, you may wish to refer to

> Steps for Recovering from a UNIX or NT System Compromise

Known versions of the worm reside entirely in memory; therefore, a reboot of the machine will purge the worm from the system. However, due to the rapid propagation of the worm, the likelihood of re-infection is quite high. Taking the system offline and applying the vendor patch will eliminate the vulnerability exploited by the "Code Red" worm.

IV. Good Practices

Consistent with the security best-practice of denying all network traffic and only selectively allowing that which is required, ingress and egress filtering should be implemented at the network edge. Likewise, controls must be in place to ensure that all software used on a network is properly maintained.

Ingress filtering

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. Servers are typically the only machines that need to accept inbound connections from the public Internet. In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound connections to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound connections to non-authortized services. In this fashion, the effectiveness of many intruder scanning techniques can be dramatically reduced. With "Code Red," ingress filtering will prevent instances of the worm outside of your network from infecting machines in the local network that are not explicitly authorized to provide public web services. Cisco has published a tech tip specifically addressing ingress filtering for the "Code Red" worm at

> http://www.cisco.com/warp/public/63/nbar_acl_codered.shtml.

Egress filtering

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound connections to the Internet. In the case of "Code Red," employing egress filtering will prevent compromised IIS servers on your network from further propagating the worm.

Installing new software with the latest patches

When installing an operating system or application on a host for the first time, it is insufficient to merely use the install media. Vulnerabilities are often discovered after the software becomes widely distributed. Thus, prior to connecting this host to the network, the latest security patches for the software should be obtained from the vendor and applied.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Cisco Systems

Cisco has published a security advisory describing this vulnerability at

http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

Microsoft Corporation

The following document regarding the vulnerability exploited by the "Code Red" worm is available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

Author(s): Roman Danyliw and Allen Householder

This document is available from: http://www.cert.org/advisories/CA-2001-23.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key
If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site
http://www.cert.org/
To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
Jul 26, 2001: Initial release
Jul 30, 2001: Added link to Polish translation
Aug 16, 2001: Added link to Cisco ingress filtering tech tip, updated
link to Microsoft cumulative patch
```

CERT® Advisory CA-2001-20 Continuing Threats to Home Users

Original release date: July 20, 2001
Last revised: July 23, 2001
Source: CERT/CC

A complete revision history can be found at the end of this file.

Need to Protect Home Systems

This year, we have seen a significant increase in activity resulting in compromises of home user machines. In many cases, these machines are then used by intruders to launch attacks against other organizations. Home users have generally been the least prepared to defend against attacks. Many home users do not keep their machines up to date with security patches and workarounds, do not run current anti-virus software, and do not exercise caution when handling email attachments. Intruders know this, and we have seen a marked increase in intruders specifically targeting home users who have cable modem and DSL connections.

Most of the subscribers to the CERT Advisory Mailing List and many visitors to our web site are technical staff responsible for maintaining systems and networks. But all of us know people who have home computers and need advice about how to secure them. We recently released a document on our web site providing some basic security information and references for home users. The document, "Home Network Security," is available on our web site at

http://www.cert.org/tech_tips/home_networks.html

We encourage the technical readers of our mailing list to reach out to your parents, children, and other relatives and friends who might not be as technically oriented, point them to this document and help them understand the basics of security, the risks, and how they can better defend themselves. We have a long road to travel in educating home users on the security risks of the Internet. But all of us working together to educate home users will improve the security of the Internet as a whole.

Worms and DDoS Tools

The CERT/CC is currently tracking the activity of several large-scale incidents involving new worms and distributed denial-of-service (DDoS) tools. Some of these worms include a command and control structure that allows the intruder to dynamically modify the behavior of the worm after it has infected a victim system. In some cases, the command and control structure allows the intruder to issue a single command to all the infected systems without needing to know which systems have actually been infected. This ability to change the behavior of the worm (including wholesale replacement), makes it substantially more difficult to develop "one size fits all" solutions to the problem. Additionally, many of these worms have targeted home users as victims.

With these facts in mind, and the large number of hosts involved in these incidents, it is imperative for everyone to take precautions to patch the vulnerabilities involved and recover compromised systems.

W32/Leaves worm

The W32/Leaves worm, described in IN-2001-07 primarily affects systems that have been previously compromised by the SubSeven Trojan horse program. We have received reports that over 23,000 machines have been compromised by this worm. This worm includes functionality that allows a remote intruder to control the network of compromised machines.

"Code Red" worm

The "Code Red" worm, described in CA-2001-19 exploits a vulnerability in the Indexing Service on systems running Microsoft IIS. Current reports indicate that over 250,000 hosts have already been compromised by this worm.

"Power" worm

A worm, known by the name of "Power" is also compromising systems vulnerable to the IIS Unicode vulnerability described in VU#111677. It uses the Internet Relay Chat (IRC) as a control channel for coordinating compromised machines in DDoS attacks. Based on reports that we have received, over 10,000 machines have already been compromised by this worm.

"Knight" distributed attack tool

An attack tool known as "Knight" has been found on approximately 1,500 hosts. This tool appears to be a DDoS tool and also uses IRC as a control channel. It has been reported that the tool is commonly being installed on machines that were previously compromised by the BackOrifice Trojan horse program. So far, there has been no indication that this tool is a worm; it does not contain any logic to propagate automatically.

Protective Measures

For all of these problems, the deployment and maintenance of some these simple defenses are relatively effective:

1. Install and Maintain Anti-Virus Software

The CERT/CC strongly recommends using anti-virus software. Most current anti-virus software products are able to detect and alert the user that an intruder is attempting to install a Trojan horse program or that one has already been installed.

In order to ensure the continued effectiveness of such products, it is important to keep them up to date with current virus and attack signatures supplied by the original vendors. Many anti-virus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

2. Deploy a Firewall

The CERT/CC also recommends using a firewall product, such as a network appliance or a personal firewall software package. In some situations, these products may be able to alert users to the fact that their machine has been compromised. Furthermore, they have the ability to block intruders from accessing backdoors over the network. However, no firewall can detect or stop all attacks, so it is important to continue to follow safe computing practices.

For additional information about securing home systems and networks, please see the "Home Network Security" tech tip at

http://www.cert.org/tech_tips/home_networks.html

If these protective measures reveal that the machine has already been compromised, more drastic steps need to be taken to recover. When a computer is compromised, any installed software could have been modified, including the operating system, applications, data files, and memory. In general, the only way to ensure that a compromised computer is free from backdoors and intruder modifications is to re-install the operating system from the distribution media and install vendor-recommended security patches before connecting back to the network. Merely identifying and fixing the vulnerability that was used to initially compromise the machine may not be enough.

Often, these worms rely on Trojan horses to initially compromise a system. For more information on Trojan horses, see

http://www.cert.org/advisories/CA-1999-02.html

Additionally, these worms often spread by exploiting vulnerabilities in systems. For information on vulnerabilities affecting popular products, please see

http://www.kb.cert.org/vuls

Author(s): Jeff Carpenter, Chad Dougherty, Shawn Hernan

This document is available from: http://www.cert.org/advisories/CA-2001-20.html

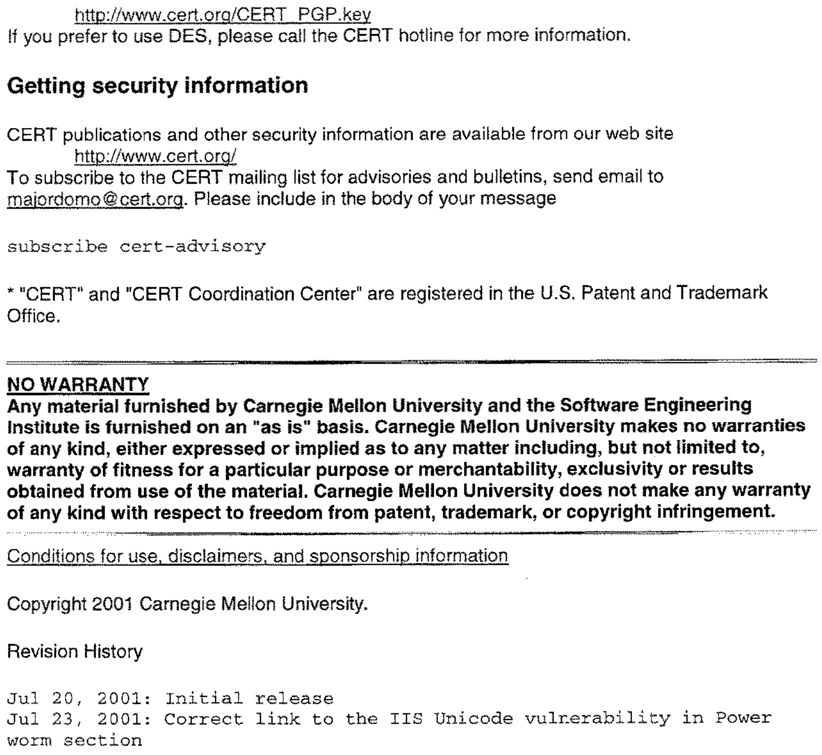
CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from



http://www.cert.org/CERT_PGP.key
If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site
http://www.cert.org/
To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
Jul 20, 2001: Initial release
Jul 23, 2001: Correct link to the IIS Unicode vulnerability in Power
worm section
```

CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL

Original release date: July 19, 2001
Last revised: August 16, 2001
Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed
- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)
- Unpatched Cisco 600 series DSL routers

Overview

The CERT/CC has received reports of new self-propagating malicious code that exploits IIS-enabled systems susceptible to the vulnerability described in CERT advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. Other systems not directly vulnerable to this exploit may also be impacted. Reports indicate that two variants of the "Code Red" worm may have already affected more than 250,000 hosts.

A translation of this advisory into Polish is available at http://www.cert.pl/CA/CA-2001-19-PL.html.

I. Description

The "Code Red" worm is self-replicating malicious code that exploits a known vulnerability in Microsoft IIS servers (CA-2001-13).

Attack Cycle

The "Code Red" worm attack proceeds as follows:

1. The "Code Red" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found. Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Indexing Service described in CERT advisory CA-2001-13
2. The same exploit (HTTP GET request) is sent to each of the randomly chosen hosts due to the self-propagating nature of the worm. However, depending on the configuration of the host which receives this request, there are varied consequences.
    - **IIS 4.0 and 5.0 servers with Indexing service installed** will almost certainly be compromised by the "Code Red" worm.

- **Unpatched Cisco 600-series DSL routers** will process the HTTP request thereby triggering an unrelated vulnerability which causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
- **Systems not running IIS, but with an HTTP server listening on TCP port 80** will probably accept the HTTP request, return with an "HTTP 400 Bad Request" message, and potentially log this request in an access log.

3. If the exploit is successful, the worm begins executing on the victim host. In the earlier variant of the worm, victim hosts with a default language of English experienced the following defacement on all pages requested from the server:

```
4.    HELLO! Welcome to http://www.worm.com! Hacked By
   Chinese!
```

Servers configured with a language that is not English and those infected with the later variant will not experience any change in the served content.

Other worm activity on a compromised machine is time senstive; different activity occurs based on the date (day of the month) of the system clock.

- *Day 1 - 19*: The infected host will attempt to connect to TCP port 80 of randomly chosen IP addresses in order to further propagate the worm.
- *Day 20 - 27*: A packet-flooding denial of service attack will be launched against a particular fixed IP address
- *Day 28 - end of the month*: The worm "sleeps"; no active connections or denial of service

System Footprint

The "Code Red" worm activity can be identified on a machine by the presence of the following string in a web server log files:

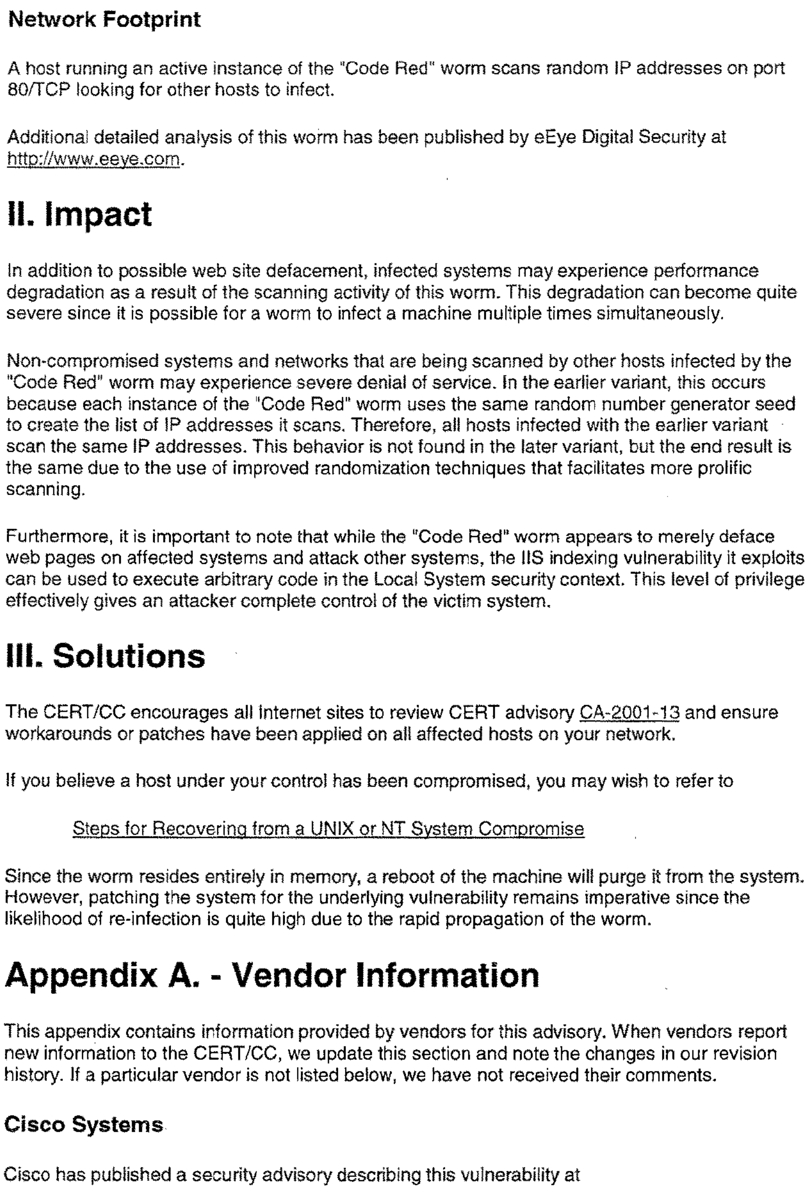
```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u
6858%ucbd3%
u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003
%u8b00%u531
b%u53ff%u0078%u0000%u00=a
```

The presence of this string in a log file does not neccessarily indicate compromise. Rather it only implies that a "Code Red" worm attempted to infect the machine.

Additionally, web pages on victim machines may be defaced with the following message:

```
HELLO! Welcome to http://www.worm.com! Hacked By Chinese!
```

The text of this page is stored exclusively in memory and is not written to disk. Therefore, searching for the text of this page in the file system may not detect compromise.



Network Footprint

A host running an active instance of the "Code Red" worm scans random IP addresses on port 80/TCP looking for other hosts to infect.

Additional detailed analysis of this worm has been published by eEye Digital Security at http://www.eeye.com.

II. Impact

In addition to possible web site defacement, infected systems may experience performance degradation as a result of the scanning activity of this worm. This degradation can become quite severe since it is possible for a worm to infect a machine multiple times simultaneously.

Non-compromised systems and networks that are being scanned by other hosts infected by the "Code Red" worm may experience severe denial of service. In the earlier variant, this occurs because each instance of the "Code Red" worm uses the same random number generator seed to create the list of IP addresses it scans. Therefore, all hosts infected with the earlier variant scan the same IP addresses. This behavior is not found in the later variant, but the end result is the same due to the use of improved randomization techniques that facilitates more prolific scanning.

Furthermore, it is important to note that while the "Code Red" worm appears to merely deface web pages on affected systems and attack other systems, the IIS indexing vulnerability it exploits can be used to execute arbitrary code in the Local System security context. This level of privilege effectively gives an attacker complete control of the victim system.

III. Solutions

The CERT/CC encourages all Internet sites to review CERT advisory CA-2001-13 and ensure workarounds or patches have been applied on all affected hosts on your network.

If you believe a host under your control has been compromised, you may wish to refer to

> Steps for Recovering from a UNIX or NT System Compromise

Since the worm resides entirely in memory, a reboot of the machine will purge it from the system. However, patching the system for the underlying vulnerability remains imperative since the likelihood of re-infection is quite high due to the rapid propagation of the worm.

Appendix A. - Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Cisco Systems

Cisco has published a security advisory describing this vulnerability at http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

Microsoft Corporation

The following document regarding the vulnerability exploited by the "Code Red" worm is available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#36881]".

Author(s): Roman Danyliw and Allen Householder

This document is available from: http://www.cert.org/advisories/CA-2001-19.html

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

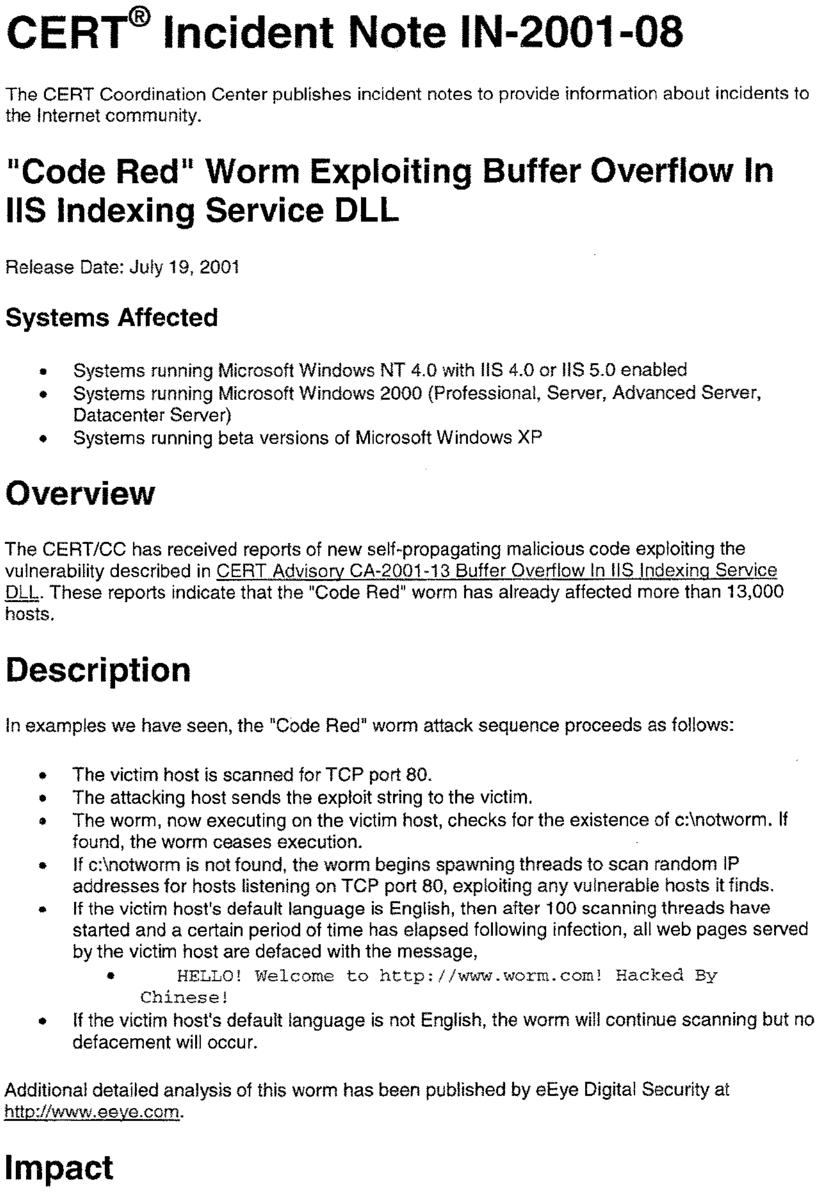
* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
Jul 19, 2001: Initial release
Jul 20, 2001: Multiple variants, vendor information
Jul 30, 2001: Clarification of systems affected, attack cycle; addition
of link to Polish translation
Aug 16, 2001: Updated link to Microsoft cumulative patch
```



CERT® Incident Note IN-2001-08

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

"Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL

Release Date: July 19, 2001

Systems Affected

- Systems running Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled
- Systems running Microsoft Windows 2000 (Professional, Server, Advanced Server, Datacenter Server)
- Systems running beta versions of Microsoft Windows XP

Overview

The CERT/CC has received reports of new self-propagating malicious code exploiting the vulnerability described in CERT Advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. These reports indicate that the "Code Red" worm has already affected more than 13,000 hosts.

Description

In examples we have seen, the "Code Red" worm attack sequence proceeds as follows:

- The victim host is scanned for TCP port 80.
- The attacking host sends the exploit string to the victim.
- The worm, now executing on the victim host, checks for the existence of c:\notworm. If found, the worm ceases execution.
- If c:\notworm is not found, the worm begins spawning threads to scan random IP addresses for hosts listening on TCP port 80, exploiting any vulnerable hosts it finds.
- If the victim host's default language is English, then after 100 scanning threads have started and a certain period of time has elapsed following infection, all web pages served by the victim host are defaced with the message,
  - `HELLO! Welcome to http://www.worm.com! Hacked By Chinese!`
- If the victim host's default language is not English, the worm will continue scanning but no defacement will occur.

Additional detailed analysis of this worm has been published by eEye Digital Security at http://www.eeye.com.

Impact

In addition to web site defacement, affected systems may experience performance degradation as a result of this worm.

Each instance of the "Code Red" worm uses the same random number generator seed to create the list of IP addresses it scans. Therefore, each victim host begins scanning the same IP addresses that previous instances have scanned, which could result in a denial of service against the IP addresses earliest in the list.

Furthermore, it is important to note that while the "Code Red" worm appears to merely deface web pages on affected systems and attack other systems, the IIS indexing vulnerability it exploits can be used to execute arbitrary code in the Local System security context, effectively giving an attacker complete control of the victim system. It is therefore imperative to apply the remedies described in the Solutions section of this document.

System Footprint

The "Code Red" worm can be identified on victim machines by the presence of the following string in IIS log files:

```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u
6858%ucbd3%
u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003
%u8b00%u531
b%u53ff%u0078%u0000%u00=a
```

Additionally, web pages on victim machines may be defaced with the following message:

```
HELLO! Welcome to http://www.worm.com! Hacked By Chinese!
```

Network Footprint

A host running an active instance of the "Code Red" worm will scan random IP addresses on port 80/TCP looking for other hosts to infect.

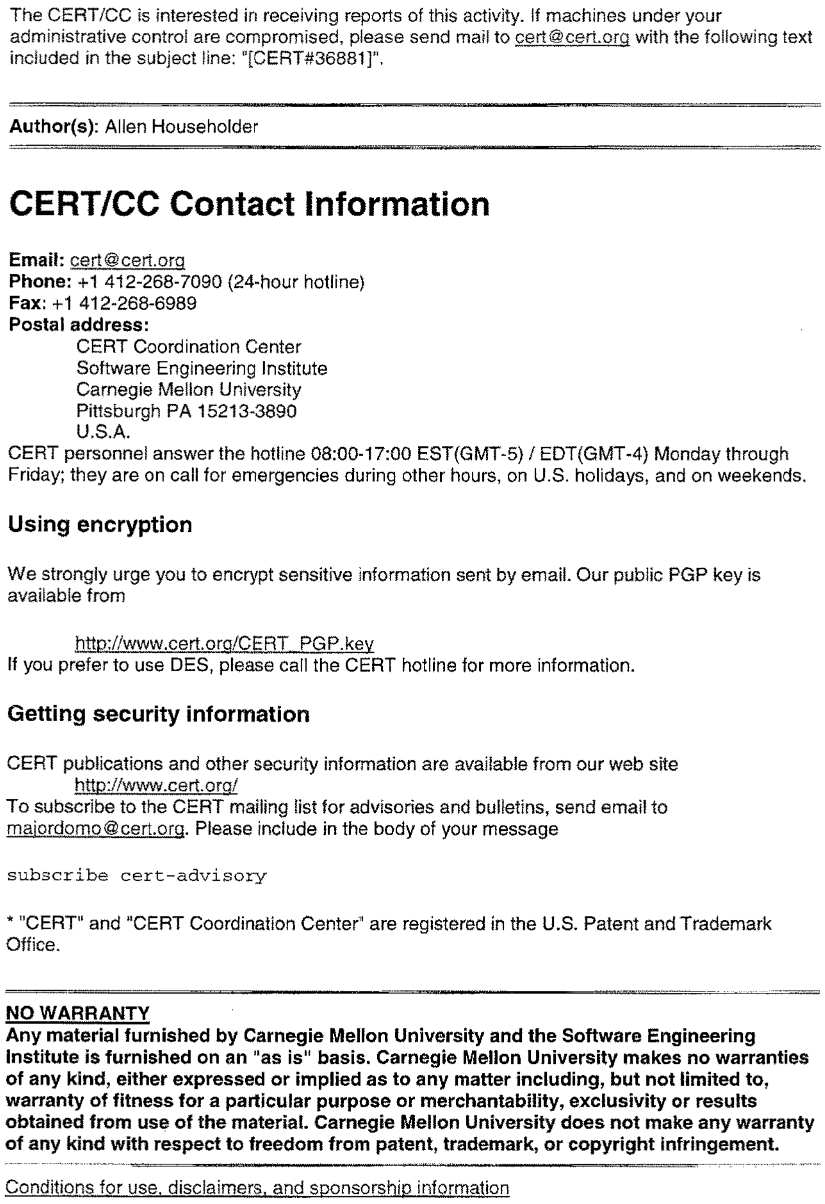
Solutions

The CERT/CC encourages all Internet sites to review CERT Advisory CA-2001-13 and ensure workarounds or patches have been applied on all affected hosts on your network.

If you believe a host under your control has been compromised, you may wish to refer to

> Steps for Recovering from a UNIX or NT System Compromise

Reporting



The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#36881]".

Author(s): Allen Householder

CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

http://www.cert.org/

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

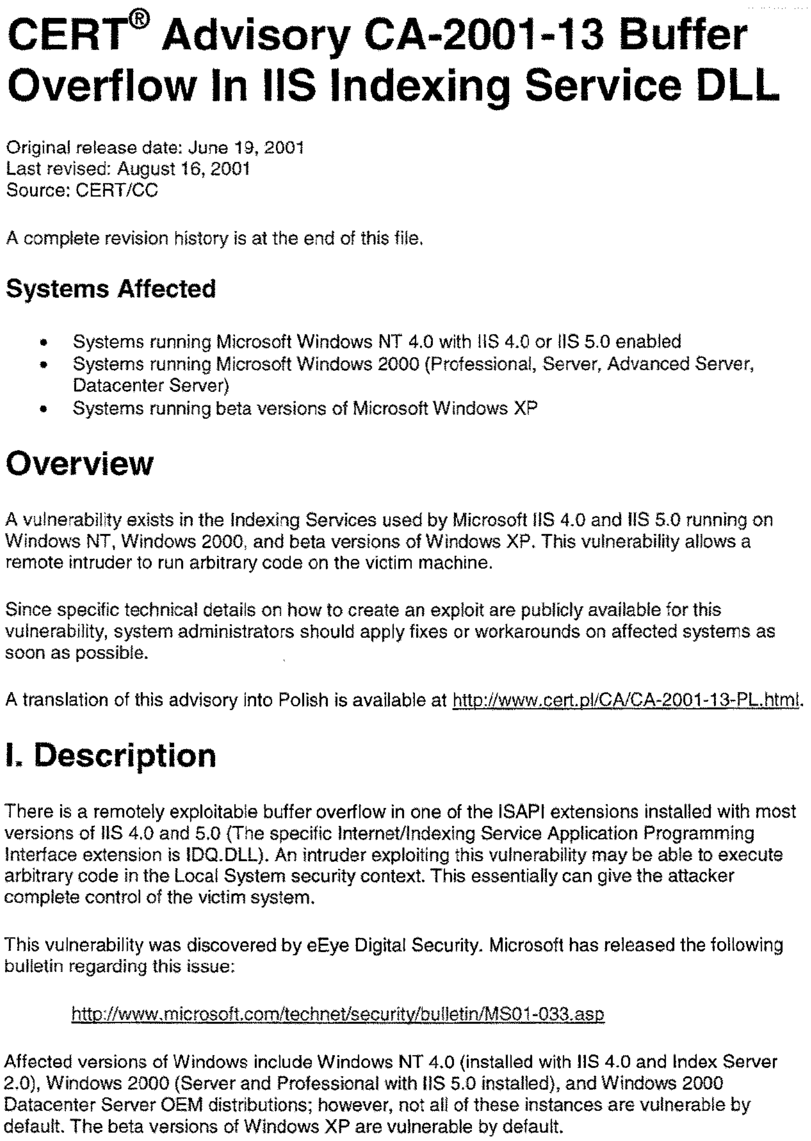
* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
July 19, 2001: Initial Release
```



CERT® Advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL

Original release date: June 19, 2001
Last revised: August 16, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled
- Systems running Microsoft Windows 2000 (Professional, Server, Advanced Server, Datacenter Server)
- Systems running beta versions of Microsoft Windows XP

Overview

A vulnerability exists in the Indexing Services used by Microsoft IIS 4.0 and IIS 5.0 running on Windows NT, Windows 2000, and beta versions of Windows XP. This vulnerability allows a remote intruder to run arbitrary code on the victim machine.

Since specific technical details on how to create an exploit are publicly available for this vulnerability, system administrators should apply fixes or workarounds on affected systems as soon as possible.

A translation of this advisory into Polish is available at http://www.cert.pl/CA/CA-2001-13-PL.html.

I. Description

There is a remotely exploitable buffer overflow in one of the ISAPI extensions installed with most versions of IIS 4.0 and 5.0 (The specific Internet/Indexing Service Application Programming Interface extension is IDQ.DLL). An intruder exploiting this vulnerability may be able to execute arbitrary code in the Local System security context. This essentially can give the attacker complete control of the victim system.

This vulnerability was discovered by eEye Digital Security. Microsoft has released the following bulletin regarding this issue:

> http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

Affected versions of Windows include Windows NT 4.0 (installed with IIS 4.0 and Index Server 2.0), Windows 2000 (Server and Professional with IIS 5.0 installed), and Windows 2000 Datacenter Server OEM distributions; however, not all of these instances are vulnerable by default. The beta versions of Windows XP are vulnerable by default.

The only precondition for exploiting this vulnerability is that an IIS server is running with script mappings for Internet Data Administration (.ida) and Internet Data Query (.idq) files. The Indexing Services do not need to be running. As stated by Microsoft in MS01-033:

> The buffer overrun occurs before any indexing functionality is requested. As a result, even though idq.dll is a component of Index Server/Indexing Service, the service would not need to be running in order for an attacker to exploit the vulnerability. As long as the script mapping for .idq or .ida files were present, and the attacker were able to establish a web session, he could exploit the vulnerability.

This vulnerability has been assigned the identifier CAN-2001-0500 by the Common Vulnerabilities and Exposures (CVE) group:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0500

II. Impact

Anyone who can reach a vulnerable web server can execute arbitrary code in the Local System security context. This results in the intruder gaining complete control of the system. Note that this may be significantly more serious than a simple "web defacement."

III. Solution

Apply a patch from your vendor

Apply patches for vulnerable Windows NT 4.0 and Windows 2000 systems:

For Windows NT 4.0:

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833

For Windows 2000 Professional, Server, and Advanced Server:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800

Users of Windows 2000 Datacenter Server software should contact their original equipment manufacturer (OEM) for patches. A list of OEM providers may be found here:

http://www.microsoft.com/windows2000/datacenter/howtobuy/purchasing/oems.asp

Workarounds

Users of beta copies of Windows XP should upgrade to a newer version of the software when it becomes available.

All affected versions of IIS/Indexing Services can be protected against exploits of this vulnerability by removing script mappings for Internet Data Administration (.ida) and Internet Data Query (.idq) files. However, such mappings may be recreated when installing other related software components.

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS01-033.asp
http://www.microsoft.com/technet/security/bulletin/MS01-044.asp
http://www.microsoft.com/technet/support/kb.asp?ID=Q300972

References

1. *VU#952336: Microsoft Index Server/Indexing Service used by IIS 4.0/5.0 contains unchecked buffer used when encoding double-byte characters* CERT/CC, 06/19/2001, https://www.kb.cert.org/vuls/id/952336
2. Additional advice on securing IIS web servers is available from

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp
Feedback concerning this document may be directed to Jeffrey S. Havrilla.

This document is available from: http://www.cert.org/advisories/CA-2001-13.html

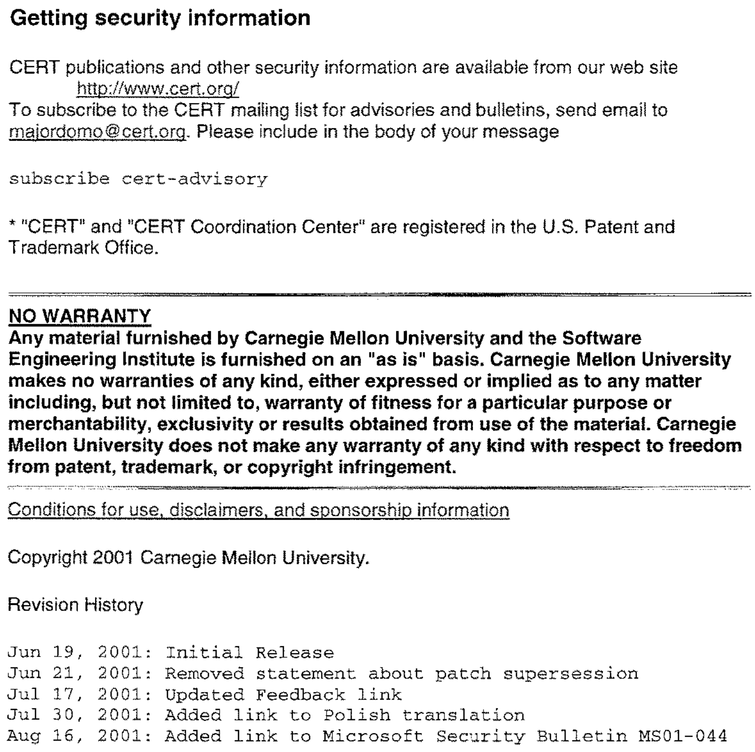
CERT/CC Contact Information

Email: cert@cert.org
Phone: +1 412-268-7090 (24-hour hotline)
Fax: +1 412-268-6989
Postal address:
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.
CERT personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key
If you prefer to use DES, please call the CERT hotline for more information.



Getting security information

CERT publications and other security information are available from our web site
http://www.cert.org/
To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

```
subscribe cert-advisory
```

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY
Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Revision History

```
Jun 19, 2001: Initial Release
Jun 21, 2001: Removed statement about patch supersession
Jul 17, 2001: Updated Feedback link
Jul 30, 2001: Added link to Polish translation
Aug 16, 2001: Added link to Microsoft Security Bulletin MS01-044
```

Synopsis of Jeffrey J. Carpenter's Testimony on Computer Security and the "Code Red" Worm August 29, 2001

Jeffrey J. Carpenter is the manager of the CERT® Coordination Center (CERT/CC) at the Software Engineering Institute (SEI), a federally funded research and development Center at Carnegie Mellon University in Pittsburgh, Pennsylvania.

CERT/CC – trusted, neutral, authoritative source of network security information and expertise

- The CERT/CC was established in 1988, after an Internet "worm" became the first Internet security incident to make headline news, serving as a wake-up call for Internet security. The CERT/CC was operational less than two weeks later.
- Since 1988, the CERT/CC has responded to 63,000 computer security incidents and cataloged 3,700 vulnerabilities. In the first half of 2001 alone, it handled 15,000 incidents, indicating an estimated 42% increase from the year before.

The Red Code Worm and Its Implications

- The Red Code worm takes advantage of the fact that many computers on the Internet run vulnerable versions of Microsoft's Internet Information Server. Even after multiple warnings in July 2001, many computer systems remained unpatched, resulting in thousands of compromised machines again in August 2001.
- The worm represents a larger problem with Internet security. The Internet is vulnerable today and will remain vulnerable in the foreseeable future. Attacks will continue.
- Exploitation of vulnerabilities happens faster and more efficiently than in the past. Security experts have little time to analyze exploit scripts and distribute warnings. System administrators and users have little time to implement workarounds and patches.
- Security issues are not well understood and are rarely given high priority by software developers, vendors, network managers, or consumers. Acquisition practices do not adequately support security in products. As a result, many vulnerable computers are available for compromise by attackers.
- The interconnectedness and interdependency of systems on the Internet means everyone must act to address Internet security problems.

Recommended Actions

- To address attacks by malicious code and other security problems on the Internet, changes are necessary in product development, system administration, user knowledge, and acquisition.
- The government should support research and development leading to a safer computing environment and computer systems that are better able to resist, recognize, and recover from attacks with still providing critical functionality.
- Support is also essential for university programs in information security to meet the need for additional experts in the field.

Mr. HORN. Well, we thank you very much and we'll have a lot of questions coming up very shortly.

From the State of California we have Alethia Lewis, deputy director of the Department of Information Technology and Patricia Kuhar, the program manager, Information Security for the Department of Information Technology. You weren't here when we noted that we do swear in our various guests and I believe Ms. Kuhar is the official witness, but Ms. Lewis will be doing the testifying. So if you'll raise your right hands.

[Witnesses sworn.]

Mr. HORN. Clerk will note both witnesses affirmed the oath. So Ms. Lewis, proceed. We've got some of your testimony. It's in the record and if you'd like to submit some more, obviously we'd be delighted to have your thoughts. So go ahead.

STATEMENT OF ALETHIA LEWIS, DEPUTY DIRECTOR, DEPARTMENT OF INFORMATION TECHNOLOGY, STATE OF CALIFORNIA

Ms. LEWIS. Thank you. My name is Alethia Lewis and I'm Deputy Director with the Department of Information Technology responsible for the department's external affairs and liaison to other State agencies in IT matters. As stated, I have with me today Ms. Patty Kuhar, the department's information security program manager and a board certified information systems security professional.

We're here representing the State of California on behalf of the Governor's office and the Department of Information Technology.

I'd like to thank you for inviting us to participate in this hearing. We did prepare a statement which I'll be presenting a slightly condensed version of that statement here as testimony.

California state government has over 100,000 computer work stations and e-mail users and over 1,000 Web servers at hundreds of locations state-wide. With the large number of users, the even larger number of e-mail correspondence and network connections, our systems are often subject to attack and disruption by viruses and worms. The most visible and notorious of these incidents involve mass e-mail viruses and worms. Like many others, the State was hit particularly hard by the Love Bug viruses which interrupted e-mail systems at many departments for periods varying from a few minutes to several days. Melissa, Kournikova and a few others have caused similar but somewhat less wide-spread disruptions. Each time, several hundred hours of work by skilled and scarce technicians was required to get the e-mail systems cleaned-up and back in business.

Over the past few years, we've deployed commercial software products to protect most State work stations and many e-mail servers. We know this has resulted in a big reduction in the amount of impact that worms and viruses might have had by comparing the impact of attacks on the best protected sites with those that are less protected. Nevertheless, the defense are far from perfect. It is a time consuming and continued effort to ensure that every device and server has software protection from the latest viruses and inevitably, a few systems get missed and are left vulnerable.

Increasingly, the most destructive or at least disruptive malicious software spreads around the world in just a few days or even hours. The fast spreading Melissa was a real wakeup call. We learned that an e-mail virus can span the world in less than 24-hours hitting just about every vulnerable system. We've had to change our approach to system protection from focus on individual desktops out to the perimeters, adding security software to e-mail servers and installing more robust protections at the edges of our networks.

In addition to changing our security architecture to allow us to apply fixes more rapidly, we also have taken steps to make our organization more responsive with the establishment of trained incident response teams and practice recovery procedures. In fact though, we are just holding our own. Generally, we're staying just a bit ahead of, perhaps not falling any further behind, the bad guys. But we should expect this to change for several reasons.

First, the motives of most malicious software authors have heretofore been mostly anarchic. We in government should view the apparent political intent behind some of the worm events this spring with special alarm as the target is likely to be us. Second, unlike the mass e-mail viruses which usually take advantage of human nature to turn otherwise useful software features against us, the most destructive malicious software exploits unintentional flaws in the commercial software we're using.

In the fairly recent past, we and the industry have had several months to find and fix those flaws before the bad guys began to exploit it. Usually, only systems maintained by careless or overworked system administrators were affected. But as we learned with the recent Code Red experience, the attacking community is learning to move faster, too, and a startling number of systems were caught unprepared for this worm which emerged only a few weeks after the vulnerability was discovered.

Third, again exemplified by the Code Red, the worm itself can change quickly making it hard for even the most alert security staff to keep up. The original version of Code Red was fairly innocuous, at least to the system directly attacked, and could be cleared by a simple reboot. Later versions were potentially much more dangerous and required much more time consuming recovery measures.

Fourth, as for both the Code Red worm and the mass e-mail viruses, protecting your own system is not enough. When the Code Red worm hit, every Internet user faced potential disruption due to the sheer volume of traffic generated by the worm's victims. Information security has become a community responsibility. We must maintain robust security measures, not just to protect our systems, but to avoid becoming a nuisance to our peers.

And here we face the most difficult challenge of all, making sure our users understand and perform their role in information security. This is always difficult and is a constantly moving target. Nonetheless, we must move our user communities to a higher-level of sophistication, especially since so many of them now have computers in their homes. These home systems may well be used for after work hours and, while we hate to discourage that, they are new sources of vulnerability. With all this broad band network connectivity, they're a sitting duck for attackers.

So we believe that above all we must place our trust in policy more than technology. We need to stay current with the emerging attack methods and improving security measures. We need to be more organizationally and technically nimble in closing holes and responding to incidents, and we need to educate and keep re-educating our users and technical staff. But ultimately we need to recognize that network-attached resources are vulnerable. Systems that depend on the Internet are going to be disrupted. We need to have effective alternatives for accomplishing critical missions. Sensitive information on network-attached systems is going to be improperly accessed. We need to keep the most critical secrets, including those involving private information, out of harm's way, behind firewalls and properly encrypted.

At the State, we have set standards for information security throughout government that ensure consistent and reliable level of information security throughout State government. We now require that information security requirements are identified and addressed when new systems are planned. We require that implemented security measures are continually checked by information security officers independent of the technology staff to make sure our protections are not allowed to lapse. We have established a level of security performance by State departments that is attainable and is expected by our leaders and the public we serve.

In addition, to make sure everyone in the organization from the chief executive officer to the key data operator is on our security team. We have been sponsoring a continuing series of information security forums and seminars. Presented by independent public and private sector information security experts, these quarterly events are typically attended by over 200 State government decisionmakers, program managers and IT professionals.

This concludes my testimony and, again, I'd like to thank you for inviting us to participate in this hearing.

[The prepared statement of Ms. Lewis follows:]

Ms. Lewis

State of California Department of Information Technology
Testimony for Congressional Field Hearing on Worms and Viruses
August 29, 2001

California state government has over 100,000 computer workstations and email users and over 1,000 web servers at hundreds of locations statewide. With the large number of users, the even larger number of email correspondents and network connections, it's not surprising that we are regularly subject to attack and disruption by viruses and worms.

The most visible and notorious of these incidents involve the mass email viruses and worms. Like many others, the state was hit particularly hard by the Lovebug viruses, which interrupted email systems at many departments for periods varying from a few minutes to several days. Melissa, Kournikova, and a few others have caused similar, but somewhat less widespread, disruptions. Each time, several hundred hours of work by skilled and scarce technicians was required to get the email systems cleaned up and back in business.

Every day, however, much more time—and often, valuable information—is lost due to less well-known, but more destructive, viruses and worms. The mass email viruses that have received media attention generally caused no more damage than the loss of email services for a day or so. Hundreds of viruses, some infecting only a few systems, a few hitting a thousand or so, each require several hours of technician work to correct. Each also costs the user at least a few hours of access to their system, and sometimes the loss of incalculable amounts of work. The recovery of damaged systems is a constant workload and adds significantly to the cost of ownership of computer workstations.

Over the past few years, we've deployed commercial software products to protect most state workstations and many email servers. We know this has resulted in a big reduction in the amount of impact that worms and viruses might have had by comparing the impact of attacks on the best-protected sites with those that are less protected. Nevertheless, the defenses are far from perfect. It is a time-consuming and continuing effort to ensure that every device and server has software protection from the latest viruses, and inevitably, a few systems get missed and are left vulnerable.

Increasingly, the most destructive, or at least disruptive, malicious software spreads around the world in just a few days or even hours. We've had to change our approach to system protection from a focus on individual desktops out toward the perimeters—adding security software to email servers, and installing more robust protections at the edges of our networks. We simply can't get the software necessary to protect against a new virus out to every desktop fast enough. The difference between a site that comes through a Melissa event unscathed and one that goes without email for a week is only a couple of hours of reaction time. The system operators who are alert to the emerging event, and who have the ability to place the necessary protections in place very quickly, are often able to avoid any user impact at all.

The fast-spreading Melissa was a real wakeup call; we learned that an email virus can span the world in less than 24 hours, hitting just about every vulnerable system. In addition to changing our security architecture to allow us to apply fixes more rapidly, we also have taken steps to make our organization more responsive, with the establishment of trained incident response teams and practiced recovery procedures.

In fact, though, we are just holding our own. Virus protection software is best at protecting us from last week's virus. So far, the most destructive viruses, such as Magistr, tend to be fairly slow in spreading, so the virus protection software developers have time to get us a fix, and we have time to get it installed, before much damage is done. And generally, we're staying just a bit ahead of (or perhaps not falling any further behind) the bad guys. But we should expect this to change, for several reasons.

First, the motives for most malicious software authors have heretofore been mostly anarchic—a desire to do damage, but without a particular target in mind. We in government should view the apparent political intent behind some of the worm events this spring with special alarm—the target is likely to be us.

Second, unlike the mass email viruses, which usually take advantage of human nature to turn otherwise useful software features against us, the most destructive malicious software exploits unintentional flaws in the commercial software we're using. In the fairly recent past, we and the industry would have several months to find and fix those flaws before the bad guys began to exploit it. Usually, only systems maintained by careless or overworked system administrators were usually affected. But as we learned with the recent Code Red experience, the attacking community is learning to move faster too, and a startling number of systems were caught unprepared for this worm which emerged only a few weeks after the vulnerability was discovered. Moreover, Code Red moved so quickly that every vulnerable system was probably attacked—and infected—repeatedly with a few days of its release into the wild.

Third, again exemplified by Code Red, the worm itself can change quickly, making it hard for even the most alert security staff to keep up. The original version of Code Red was fairly innocuous—at least to the system directly attacked—and could be cleared by a simple reboot. Later versions were potentially much more dangerous, and required much more time-consuming recovery measures.

Fourth, as for both the Code Red worm and the mass email viruses, protecting your own system is not enough. The White House, which avoided the Code Red's specific intent through a combination of quick response and a flaw in the worm, and perhaps every other internet user, faced potential disruption due to the sheer volume of traffic generated by the worm's victims. Information security has become a community responsibility; we must maintain robust security measures not just to protect our systems, but to avoid becoming a nuisance to our peers.

And here we face the most difficult challenge of all: making sure our users understand and perform their role in information security. This is always difficult—most people with a computer on their desks have only the vaguest notion about what goes on in an around those machines—and is a constantly moving target. It seems we just finished getting the majority to suspect email from strangers, and to avoid running executable attachments, when the next round of viruses and worms came directly from their most trusted correspondents—sometimes even as responses to emails they have sent!

Nonetheless we must move our user communities to a higher level of sophistication, especially since so many of them now have computers in their homes. These home systems may well be used for after-hours work—and of course we hate to discourage that—yet they are new sources of vulnerability. With always on, broadband network connectivity, they're a sitting duck for attackers, but the teleworkers often have full rights to our innermost networks, and may even store critical or sensitive work information on their hard drives.

So we believe that above all, we must place our trust in policy more than technology. Yes, we need to stay current with emerging attack methods and improving security measures. Yes, we need to be more organizationally and technically nimble in closing holes and responding to incidents. And yes, we need to educate and keep reeducating our users and technical staffs.

But ultimately, we need to recognize that network attached resources are vulnerable. Systems that depend on the Internet are going to be disrupted; we need to have effective alternatives for accomplishing critical missions. Sensitive information on network attached systems is going to be improperly accessed; we need to keep the most critical secrets, including those involving private information, out of harms way, behind firewalls and properly encrypted.

We have set standards for information security in California state government that ensure a consistent, and reliable, level of information security throughout state government. We now require that information security requirements are identified, and addressed, when new systems are planned. We require that implemented security measures are continually checked—by information security officers independent of the technology staff, to make sure our protections are not allowed to lapse. We have established a level of security performance by state departments that is attainable, and is expected by our leaders and the public we serve.

To make sure everyone in the organization, from the Chief Executive Officer (CEO) to the Key Data Operator (KDO), is on our security team, we have been sponsoring a continuing series of information security forums and seminars. Presented by independent public and private sector information security experts, these quarterly events are typically attended by over 200 state government decision makers, program managers, and IT professionals. Starting from a series of in-depth technical sessions, we found that we were missing the real opportunity, to educate the broader state workforce. And they, after all, are the ultimate key to success.

Glossary:

What is the difference between a computer virus and a computer worm?

Viruses are computer programs that are designed to spread themselves from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer, or slowly infect the documents on that computer, but it does not intentionally try to spread itself from that computer to other computers. In most cases, that's where humans come in. We send e-mail document attachments, trade programs on diskettes, or copy files to file servers. When the next unsuspecting user receives the infected file or disk, they spread the virus to their computer, and so on.

Worms, on the other hand, are insidious because they rely less (or not at all) upon human behavior in order to spread themselves from one computer to others. The *computer worm* is a program that is designed to copy itself from one computer to another over a network (e.g. by using e-mail). The worm spreads itself to many computers over a network, and doesn't wait for a human being to help. This means that computer worms spread much more rapidly than computer viruses.

Mr. HORN. Well, thank you very much, and we will now go to questions. Some of them will be the same that we'll give the second panel. The first one that comes to mind is do you feel we have appropriate laws to deal with this problem and what would you suggest? I'll ask Mr. Rhodes. We'll just go right down the line.

Mr. RHODES. I do believe the laws are appropriate. There's enough laws on the books for anybody to exercise prosecution. The struggle that I see in working with law enforcement is not that the law is inadequate. It's trying to present highly technical evidence in a court room. Having been an expert witness in legal cases, I can tell you that there's nothing more confusing than an engineer standing up in front of jury trying to explain a denial of service attack and then, just as our associate here, Mr. Castro, pointed out, if I show you this cloud and at one point the actual attacker is here but it looks like the apparent attacker is here and the victim is here, how do we convey that in a way of making ceratin that the laws are enforced? It's not really a question of law. It's a question of forensic analysis and being able to present cogent argument in a courtroom.

Mr. RHODES. Mr. Castro.

Mr. CASTRO. From the NSA perspective, we wouldn't offer anything ourselves but I do believe there's an issue that Mr. Wiser will address that he mentioned in his testimony with regard to having to seek warrant authority from different jurisdictions. Clearly, the key to getting to some sense of attribution is to be able to move very, very quickly once an attack begins, and it would be in that area that I suspect Les will talk about the need for being able to move faster in that regard.

Mr. HORN. Thank you, Larry. Mr. Wiser representing the Federal Bureau of Investigation. They're the ones that are going to be following this up.

Mr. WISER. Sir, time is of the essence in conducting computer intrusion investigations, and we find that logs are perishable and we depend upon those logs to trace back through Internet service providers the trail that an intruder uses. What we're required to do because the Federal rules of criminal procedure mandate this is that we obtain court orders in the judicial district in which the place to be searched exists. When an intruder uses several different hot points, those different ISPs, we have to obtain in serial fashion a number of separate orders and, of course, this is a timely process that could threaten an investigation and one in which a life may depend upon it in a manner that is different from a simple intrusion investigation. So that is one of our primary concerns that we're interested in.

I echo what Assistant Attorney General Cherkoff mentioned in earlier testimony before another committee about penalties where, despite the large dollar amount of damage that can be done, there seems to be disproportionately low maximum penalties for computer intrusions and viruses.

The last point that I would mention would be that in my discussions with members of the private sector, one of the reasons—and I expect that there are many reasons—but one of the reasons that they are sometimes reluctant to come forward with information to us is that they fear that the Freedom of Information Act does not provide adequate protection for proprietary information that they provide to us and so they've asked for a clarification of the law enforcement exception or another exception to be created in FOIA. This is something which there's a continuing dialog about when we've discussed this with the Judiciary Committees as well.

Those are the three things that I would point to and, of course, there are others that I'd be happy to speak with you at another time about.

Mr. HORN. Mr. Carpenter, manager of the CERT Coordination Center, Carnegie Mellon.

Mr. CARPENTER. I would just echo Mr. Wiser's comment on FOIA. From our perspective and our discussions with industry as well as government, that has been probably one of the largest issues that has been raised to us is issues regarding what sensitive information regarding incidents be exposed to FOIA requests. So that would be the only comment we would have on that.

Mr. HORN. Ms. Lewis, what does the State of California have with regard to laws that can relate to this damaging of the computer infrastructure?

Ms. LEWIS. Actually, at the State we work on policy that relates directly to the IT computers and stuff that we actually use. I really don't have any comments with respect to that particular issue.

Mr. HORN. I'm delighted to have one of my colleagues. He's fought the traffic between Sacramento and San Jose. Michael Honda is the representative right in the middle of Silicon Valley, and we thank you for coming. He'll have to go to another appointment shortly, but I'd like him to pose a few questions if he wishes to.

Mr. HONDA. Thank you, Mr. Chairman, and thank you for having this hearing. I know that from my visits with Symantec and other organizations and companies in this area that security is a critical area, not only in government, but also for personal uses and for commercial uses. I don't have any questions since I did not hear most of the testimony. I've been briefly going through the written testimony. So I wouldn't be able to ask any intelligent questions, but I do understand that the issues around security, from my visit with Symantec, is that we have a variety of issues and circumstances that we have to be particularly cognizant of. It's not only related to hardwire security and accessing our security information that we have, but also the wireless issue is a very important area that we're not keenly aware of and I think that the commercial uses that I've been exposed to and schooled in poses even greater concern on my part as far as government uses of similar kinds of techniques that we have in place.

So I'll be listening and I'll be reading the materials, but I'll be back following-up with Mr. Horn on issues of security. But I think that the issue of wireless and things that we don't see and don't realize and are not cognizant of is one top priority for me.

And then also for public policy folks for the schools and educated in the basic things that you all understand so that as policymakers we'll be able to understand how to work with you in developing policies on secure systems. I know that Dr. Neumann is here and he's testified quite a few times, and so I think the other concern I have that I'm sure is shared by Mr. Horn and that is how quickly do we move and with whom do we move and how will we be able to put the system together. So I appreciate all of you being here and sharing your information and your thoughts.

Thank you, Mr. Chairman.

Mr. HORN. Thank you.

Let me ask Mr. Castro. I'm quoting from your written testimony. "In taking out a computer network, the single hacker has the cyber destructive power normally associated with a nation state." If that's the case, what can be done technologically to address this problem?

Mr. CASTRO. Well, there are a wealth of things and I suspect in the industry panel you'll hear from some of the industry folks. But within the National Security Agency in cooperation with the National Institute of Standards and Technology, we jointly administer a program called the National Information Assurance Partnership. It's through this partnership that there have been a number of independent laboratories established. Think of them if you will as the underwriter laboratory's equivalent for cyber products.

What we have now set up is a process whereby industry can bring security and security-related products to these laboratories and, at their expense, at the industry's expense, can have these products evaluated against what is now being called the international common criteria. This is a criteria for specifying the five characteristics I showed you there earlier in my testimony specifying how those characteristics can be achieved and graded for achievement.

It's referred to as the international common criteria because all the English speaking partners have signed up to this criteria and it's now being moved out even for further international acceptance. So the goal would be to have a set of standards by which security and security-related products can be certified as doing what it is that they are advertised to do. These could range from firewalls in one case to public key infrastructure arrangements in other cases.

So I think the short answer, sir, is that there are a variety of defensive measures. We refer to them within the Department of Defense as defense in depth. They certainly in every case include well-trained people at the very, very frontend of that defensive posture but then backed-up by the appropriate software and hardware configurations.

The other thing I'd like to add is I really appreciate Congressman Honda's concern about wireless security. That is an area that at NSA we're working very, very closely with industry, some in this area, to produce secure versions of cellular telephones and other wireless devices. This is, quite frankly, the threat of the future as more and more of our Nation will be moving to this wireless technology. So your point is well taken, sir, and we're right on it.

Mr. HORN. We do need to look at this from a broader perspective that you've laid out there and I would suggest we're talking about a computer NATO. I wonder to what degree is the National Security Agency and the FBI—I know you've worked with foreign people here. Are they listening to us and are they hoping that you're helpful to them?

Mr. CASTRO. Maybe we can take it in two parts and I'll defer to Mr. Wiser on the cooperation on what we call attack sensing and warning. But certainly in the area of cooperating to produce secure products and to ensure that that security is inter-operable within both the NATO and other coalition environments, I think the answer to your question, sir, is that the allies are very, very well engaged. Again, we have a number of both bilateral and multilateral arrangements that will attempt to introduce the secure operability within our defensive posture.

And then I would ask if Mr. Wiser could answer the question on cooperation with regard to sensing and warning of attacks.

Mr. WISER. Sir Congressman, Mr. Chairman, the NIPC is unique because inside it we have the three disciplines represented. That would be law enforcement, intelligence and defense. In fact, NSA is represented at the NIPC and so we have a tremendous coordination and cooperation on a number of levels within the defense community and the NIPC and, therefore, the FBI.

But also in the center we have representatives from foreign governments. We have presently the U.K., Canada and Australia represented. And we find that this is very important in our links with those important allies. But in addition to that, we have connectivity with similar centers around the world, and I mentioned earlier the U.K., Canada and Australia as well as New Zealand and Sweden, and we're working now with Germany to establish that kind of a relationship as well.

So with those relationships and with the relationships that our legal attaches stationed in 44 countries around the world are engaged in, we are working toward that global security, and we find that our allies and those countries with whom we work are extremely interested in pursuing this objective.

Mr. HORN. Mr. Neumann's testimony is coming up on panel two, but I want to get your ideas on it. He raises the point that despite U.S. laws to prevent or punish hackers, given the international aspect of this problem, little can be done. Do you agree with that and how do we deal with it?

Mr. WISER. We've been, just as I mentioned in the testimony, very successful with the Leave worm case. It's just the latest example. That threat is now over. A number of people I don't think realized the danger that the Leave worm represented, but those of us that were working on this problem—I know that Mr. Castro, as he mentioned, is very familiar with this—know that it presented a great potential for danger. But the investigation itself solved this problem, and we've been successful on a number of different investigations.

For example, the Love Bug virus was solved quickly. I mean we had an FBI agent within 24-hours standing outside the door of the person responsible, along with the Philippine officials, Mr. Menses's group. So we are establishing these relationships with countries and as long as we can trace the trail back, many of the countries have been cooperative. Another example would be the Bloumberg case in Kazekstan where we have a league in Amate who worked with Kazekstani authorities to bring people that threatened the Bloumberg financial network to London where we did a sting operation there and individuals have been extradited to the United States to stand trial in that case.

So we have examples of success. I would say that there's a way to go, but we're optimistic that other countries will become more sophisticated with their statutes, with skilled investigators, and we take part in the training of those investigators and I think their growing awareness will create the will to cooperate with us.

Mr. HORN. In looking at the originator of the Codes Red, do you think that man or whoever will be apprehended?

Mr. WISER. Yes, sir. I do. I'm confident about those kinds of things. I'm an optimist and I believe that we'll be able to eventually find the person responsible.

Mr. HORN. Is there anything we should be promoting with the people in Silicon Valley, either in software, hardware where some of this can be headed off?

Mr. CASTRO. If I could comment on that, sir, and I'm sure others will, too. Anything that can be done to really demonstrate the commitment of the U.S. Government to ensuring the security of our ability to work on the Net and then to translate that into meaningful action would be helpful.

As I said, from the Department of Defense's point of view, we are not a dominant, although a very large customer for information technology. In today's market place, we are not a dominant customer. So if someone is going to make the argument only on the economics of what DOD can provide, it's not going to make it. The case is going to have to be made on a very much larger scale that it is critical to our Nation's total infrastructure that vendors start thinking security in their products from the very, very point of inception. The lesson that we have learned over NSA's 50 year history is that if you try to go in after the fact and improve a product, it sometimes doesn't work and, if it does work, it can be a very costly venture.

So again, fora like this where for industry we demonstrate the government's desire to really keep security in the forefront and the Congress's intent to back that desire are things that are needed.

Mr. HORN. Can you tell us how many government servers were compromised by Code Red and Code Red II? How much damage was made at this point?

Mr. CASTRO. I can speak for the Department of Defense. Others will have to speak for the rest of the government. Within the Department, General Brian, the commander of the Joint Task Force on Computer Network Operations, made the decision on the evening that it was clear that bad things were going to happen that the Department would go to what we call Info Con Alpha. Info Con Alpha is the first step where we normally are in, which is normal Info Con. This Info Con gradation is meant to match in some way DefCon and ThreatCon status that are already well-established within the Department. In doing that, then we raise the awareness of system administrators throughout the Department.

He also directed the blocking of all port 80. Again, without getting into a lot of that, and it was already mentioned in previous testimony, what we basically did is to disable anybody's ability to come in and exploit the one particular port on which the vulnerability was being exploited.

I believe that what we're saying now, with the Department still at Info Con Alpha and we are gradually getting ourselves back to a normal state. You may be aware that there are some finite number of places where the Department's portion of the Internet, which we refer to as the NipperNet, connects to the Internet. There are 13 such gateways currently in existence and we've opened up now 9 of those 13. I can't give you the specifics on what we have taken down, but I believe it's safe to say the Department is slowly recovering and we will probably lift the conditions on Info Con Alpha within the next 2 weeks.

Mr. HORN. I believe Mr. Rhodes, you and your team in the General Accounting Office, have gone through security, various designs, at various of the domestic parts of the government. Have you ever had fun with the Defense Department and CIA and knock them a little and gone through their systems?

Mr. RHODES. No. Well, yes, we've done it with the Department of Defense. I guess one point that I would make is the latest estimate that we have on total number of servers that have been taken down is 975,000. Those aren't government servers though. That was the total estimated number.

I guess one point I would make is that you asked about what could be done for Silicon Valley. What can be done to make the developers change their mind? I have to echo what Mr. Castro said. The U.S. Government has to take the point that you've made continually during your membership in the House and say they have to be able to manage. Silicon Valley is not going to make a decision that's not based on economics. They're in business, and we can't expect them to do it any other way.

If we as the U.S. Government do not manage from a security standpoint, why in the world should they? If we can't make it economically feasible for them, either by building systems specifically for us or putting the security in, we're going to continue to be in the same position we are now which are down stream testers of released software that hasn't been fully tested because they're trying to get their product to market and they're testing it well enough to get to market, not well enough to withstand a Code Red virus or something like that.

Mr. HORN. We will have the majority and minority staff give you a few questions that we simply can't get to because I want to get to the second panel. If some of you can stay, we'd certainly appreciate it to go into questioning on panel two. So let's move now to panel two. I think most of you saw the routine. We thank you very much for coming and we do swear in all witnesses and those that support the witnesses. Get them all to stand up and we don't have to keep making changes.

[Witnesses sworn.]

Mr. HORN. Let the record note that five members took the oath, and we will proceed. We now start with an old friend of this committee and a very knowledgeable person, not only in the United States but throughout the world on behalf of his colleagues in the Information Technology Association of America. So Harris Miller, president of that fine group, let's start with you.

STATEMENT OF HARRIS MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Mr. MILLER. Thank you, Mr. Chairman. Thank you for inviting me to the heart of Silicon Valley to testify about what practices, policies and tools are being deployed to reduce the impact of computer security threats to government at all levels. I commend you for your continued leadership on information technology issue.

IPA is proud to be the leading association on cyber security issues representing over 500 corporate members. These are companies that have a vested economic interest in assuring that the public feels safe in cyber space to conduct electronic commerce and, in a developing era of e-government, that their information will be secure and transactions reliable.

Though the official title of today's hearing focuses on government information security, I submit to you that security challenge is ultimately a government and business challenge that must be addressed at the highest levels of all organizations, whether public or private. We must do more than just recognizing the challenge, however, though that is an important first step. We must work together to find ways to enable solutions, solutions to threats that will likely become more significant as the Internet becomes more pervasive.

As a witness during the Code Red situation, if cyber security receives the kind of prioritization needed at senior levels, government and industry can mobilize quickly and effectively to combat common and significant threats to the Internet. Those efforts during the Code Red situation helped to reach users of vulnerable systems on a massive, unprecedented scale that prevented the further spread of the worm. Over a million copies of the patch were downloaded and, since that patch can be downloaded and installed to any number of machines, the number of systems that are actually patched is no doubt higher.

Few of the major Web sites were affected by the Code Red worm because many took action after the industry/government announcement on July 30. The public awareness of information security issues increased significantly during the Code Red situation. This cooperative, proactive response by industry and government that Mr. Rhodes addressed in his comments could be used as one model for more meaningful and effective cooperation on cyber security issues in the future.

If industry and government do not collaborate, then the impact of such threats on the Internet users will be much greater in the future.

Chairman Horn, I know from working together with you closely on Y2K and cyber security issues that you are fond of report cards and grading which you issued in your previous life as a leading academic political scientist. Today I would like to offer my own report card in six separate categories and an overall grade on industry and government handling of computer security threats. This is my own grading system, I tell you, and I look forward to suggestions from you and others about ways to improve it.

The first area is the government organization. In addressing the challenges and developing structures that can adequately address cyber security challenges, the Federal Government has moved from what had to be a failing grade just a few years ago to a passing grade or C today. I base my C grade on four factors: the priority for this issue for the Federal Government, internal cooperation within the government, mechanisms for liaising with stakeholders, particularly in the private sector, and response time.

The national plan for cyber security and Presidential Decision Directive 63 help provide a framework for government organization. However, the alphabet soup of government agencies charged with some aspect of cyber crime prevention makes it easy to see why progress has been slow in the government. We credit the National Infrastructure Protection Center under the leadership of Ron Dick to forge ahead with programs such as InfoGard which was described in Mr. Wiser's testimony. Because of his efforts and joint efforts between ITAA and the Department of Justice, we've increased the cooperation between law enforcement and the industry.

According to numerous press reports, President Bush will sign soon after Labor Day an Executive order that will establish the critical infrastructure and protection and continuity board. As that draft Executive order has been explained to us, it should be a major step forward creating substantially more coordination within government and less duplication among the plethora of government departments and agencies involved in InfoSec. Should this new board result in a centralized, coordinated cyber security effort based in the White House, I think the government grade could be moved from a C to a B.

Let me talk about a second area related to government. Government funding for information security. Here the story is not so positive, Mr. Chairman. The grade for government funding at best has moved from a D- to a D. Mr. Chairman, while you and some of your colleagues such as Representative Greenwood have done a valuable service in scrutinizing computer security policies and practices in U.S. Government agencies and departments, that is not enough. As that well-known philosopher Yogi Berra would say, this is deja vu all over again. During Y2K you pointed out in a series of hearings that government agencies had neither the plans nor the funds for Y2K remediation. Under your prodding, they came up with a plan but they still didn't have the funds. We seem to be seeing the same thing today InfoSec. Agencies seem to be knowing much more about what they need to do, but the funding is not there.

A GAO office report issued earlier this month strongly criticized the Department of Commerce for InfoSec failures internally, and that carried the clear implications report that additional financial resources are needed. Every Federal CIO with whom I speak privately tells me they are in desperate need of additional funding for their InfoSec activities. There is a long way to go before the government is going to get a passing grade here.

For example, President Bush requested an e-government fund of $20 million this year but, as you know, the House Appropriations Committee and the Senate Appropriations Committee only provided $5 million for even that. So we're going to have to work together, Mr. Chairman, under your leadership to convince your colleagues in Congress that government agencies they need to really address the InfoSec challenges.

Area No. 3. How about industry? Where is their focus in information security? I think one of the good news stories from Y2K is that issue elevated the whole issue of information technology from a back room to a front office issue. The CEOs, the members of the board began to understand how important information technology was to their businesses. Similarly, they've come to understand how important information security is to their businesses if they're going to get continuity.

Yet, at best, I only give corporate America a B- because we have a lot of variations. Some industries such as financial services, telecommunications, are doing very well but others are frankly far behind and particularly small businesses and mid-size businesses as under Y2K are far behind. I commend the FBI for its InfoCar program because that reaches small businesses. But we have a long way to go. Organizations must be willing to invest in development of comprehensive security procedures and to educate all employees continuously. We have to practice sensible cyber hygiene and Internet users have to be vigilant about it.

The next area I wish to give a grade is industry/government cooperation. The Ad Hoc Coalition on Industry and Government that was formed to provide a public service message to counter the Code Red worm is a major operational success, as Mr. Rhodes remarked. It illustrates just how far players have come. A few years ago, industry cooperation would have received an F or maybe a D. However, through hard work on both sides, progress has been made. The efforts to stand up the Information Sharing and Analysis Centers, ISACs, by the telecommunications industry, financial services industry, electric industry, transportation and now the IT industry have helped to bring us up to a C grade and, in fact, Code Red may get us up to a B-. But in order to get to an A, the remaining industry sectors will need to stand up and operationalize the ISACs and the ISACs will need to share confidential information.

Equally important, if maybe not more important, is sharing information between industry and government on sensitive information in both directions. We strongly support the bill that was referred to by the previous panel introduced by Congressmen Tom Davis and Jim Moran and soon to be introduced by Senator Bennett and Senator Kyl in the Senate to remove legal obstacles related to the Freedom of Information Act and Senator Feinstein from the State of California is in a position as chairwoman of the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information to move that bill through the Senate under her leadership.

The next area is industry to industry cooperation. Let me emphasize that while government has a critical role to play, not just in the United States but internationally, vertical industries also have an obligation to communicate on cyber security issues, again, similar to the obligation they had under Y2K. Progress has been made. We've moved from maybe a D- a few short years ago to a C+/B- today. How so?

Critical to this has been the Partnership for Critical Infrastructure Security which was begun in December 1999. This created a cross-sectoral dialog with collaboration from government, particularly the Critical Infrastructure Assurance Office, to address risks to the Nation's critical infrastructures and assure delivery of essential services over the Nation's critical infrastructures in the face of cyber threats. The Partnership is run by companies and private sector associations and is effectively meeting the industry dialog challenge.

But much more needs to be done globally. I have advocated creation of an international InfoSec cooperation center, analogous to the highly successful International Y2K Cooperation Center that you supported very strongly, Mr. Chairman, during that challenge to our global economy.

Let me next address international cooperation. Again, I think the best I can do here is a C-. Some areas are working well, others not so well. Let me tell you briefly about an area well-intended that seems to have gone a little bit awry, and that's the work of the Council of Europe to establish a cyber crime convention. The principle here is great. We need to have laws in every country around the world, not just in the United States, to fight cyber crime. As we saw in the example of the Philippines at the time that incident occurred that was referred to in the previous panel, they didn't have laws at that time to prosecute the people even though they identified them. Fortunately, the Philippines has since updated their laws.

The Cyber Crime Convention, if we could get it adopted around the world, in theory is a good idea. Unfortunately, the Cyber Crime Treaty has some flaws in it because it was developed by law enforcement officials without adequate input from industry and economic ministries. So we think with some changes in it, that might be a model law that could be adopted in many countries around the world.

To sum up, there is much work to do. In addition to improving our letter grades in information security, both industry and government need to strive to have the teacher commend us for playing well with others. Cooperation, communication and sharing sensitive information are the keys to moving from today's overall grade, which is a C-, to an A+.

Summer vacation is ending, Mr. Chairman, and we are about to begin a new school year. By working together to build meaningful and effective relationships that recognize the bottom line impact of InfoSec on our businesses and government operations, both domestically and globally, we can all move to the head of the class on cyber security issues. Thank you very much.

[The prepared statement of Mr. Miller follows:]

Testimony of Harris N. Miller
President, Information Technology Association of America (ITAA)

Field Hearing by the
House Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

August 29, 2001

"What can be done to reduce the threats posed by computer viruses and worms to the workings of government?"

Introduction

Chairman Horn, thank you for inviting me to the heart of Silicon Valley to testify about what practices, policies, and tools are being deployed to reduce the impact of computer security threats to government at all levels. I commend you for your continued leadership on information technology issues. My name is Harris N. Miller, and I am President of the Information Technology Association of America (ITAA), now celebrating its 40th Anniversary. I am proud that ITAA has emerged as the leading association on cyber security issues. ITAA represents over 500 corporate members. These are companies that have a vested economic interest in assuring that the public feels safe in cyberspace to conduct e-commerce and that in the developing era of e-government, their information will be secure and transactions reliable. As surveys ITAA has conducted demonstrate, concerns about security by citizens and consumers are major inhibitors to e-commerce and e-government.

Though the official title of today's hearing focuses on government, I submit to you that security is ultimately a government AND business challenge that must be addressed at the highest levels of all organizations, whether public or private. We all must do more to go beyond recognizing that cyber security is a challenge -- which is an important first step. Government and industry need to work together to find ways to enable solutions, solutions to threats that will likely become more significant as the Internet becomes more pervasive, and eventually ubiquitous in our society.

As we witnessed during the recent "Code Red" situation, if cyber security receives the kind of prioritization needed at senior levels, government and industry can mobilize quickly and effectively to combat common and significant threats to the Internet. Representatives from the private and public sector -- some are here today -- stood together on one stage on July 30th in Washington, DC and warned the world about the need to take precautionary steps to stop the spread of the Code Red computer worm. Those efforts helped to reach users of vulnerable systems on a massive, unprecedented scale that prevented the further spread of the worm:

- Over a million copies of Microsoft's security patch have been downloaded, and since the patch can be downloaded once and installed to any number of machines, the number of systems that were actually patched is no doubt higher;

- Microsoft observed a dramatic increase in the number of downloads during the week of July 30th, which suggests the industry-government effort to heighten user awareness and fend off the worm before it could significantly impact the Internet, worked;

- Few of the major Web sites were affected by the "Code Red" worm, because many took action after the industry-government announcement on July 30th; and

- The public's awareness of Information Security issues -- and about the specific kinds of cyber threats out there -- increased significantly during the "Code Red" situation.

This cooperative, proactive response by industry and government could be used as one model for more meaningful and effective cooperation on cyber security issues in the future. If industry and government do not collaborate to minimize impact of threats such as the "Code Red" worm -- which we were able to do in a timely and effective way in this situation -- the impact of such threats on the Internet and users could be much greater in the future. Trust is a key factor here and building relationships on trust will not happen overnight; however, industry and government collaboration on "Code Red" certainly provided a helpful boost in the right direction while our joint actions limited the number of "Code Red" infected machines.

Chairman Horn, I know from working together on Y2K and cyber security issues that you are fond of report cards and grading, which you issued in your previous career as a leading academic political scientist. Today I would like to offer a report card in six separate categories and an overall grade on industry and government handling of computer security threats. This is my own grading system, and I look forward to suggestions from you and others about additional areas requiring grading and whether I am grading based on the correct factors.

I think we can all agree that progress is being made. However, our foes in the Internet underworld are moving in Internet time, and unless we take a hard look at the effectiveness of our efforts, they may beat us at every stroke of the keyboard in the future.

A Cyber Security Report Card

Government Organization

In recognizing the challenges and developing structures that can adequately address cyber security challenges, the Federal Government has moved from a failing grade in the mid-1990s to a passing grade or "C" today. I base my grade on four factors: 1) priority for the Federal government, 2) internal cooperation, 3) mechanisms for liaising with other stakeholders, and 4) response time.

The National Plan for Cyber Security and Presidential Decision Directive (PDD) 63 helped provide a framework for government organization and thinking about information security that helped to raise the government's grade. However, the alphabet soup of government agencies charged with some aspect of cyber crime prevention makes it easy to see why progress has been slow in government. To his credit, Ron Dick, Director of the National Infrastructure Protection Center (NIPC) has forged ahead and has been successful with programs such as InfraGuard. Because of his efforts and others that ITAA has initiated with the U.S. Department of Justice and other law enforcement agencies—including two major national events with the previous Attorney General--industry is becoming more comfortable with law enforcement efforts in cyber security. The Department of Commerce also plays a critical role for government organization, since industry often feels most comfortable working with the Department of Commerce and the Critical Infrastructure Assurance Office (CIAO) there. For example, both John Tritak, CIAO's Director, and Dan Hurley, Director of the Communication and Information Infrastructure Assurance Program at NTIA, have done an outstanding job reaching out to industry during the ongoing development of the President's National Plan Version 2.0.

According to numerous press reports, President Bush will soon sign an Executive Order that will establish the "Critical Infrastructure and Protection and Continuity Board. As that draft Executive Order has been explained to us, it should be a step forward, creating substantially more coordination and less duplication among the plethora of government departments and agencies involved in InfoSec. But I continue to believe that an InfoSec Czar position similar to the role played by John Koskinen during the Year 2000 date rollover would be more effective, on the "one throat to choke" principle. With minimal overhead and resources, but strong backing from the President, Mr. Koskinen was able to have substantial influence on both the governmental and private sector efforts to address the Y2K challenge. Should the new Board result in a centralized, coordinated cyber security effort based in the White House, this grade has a chance from moving from a "C" to a "B."

Government Funding for Information Security

The grade for government funding for information security has gone from a "D-" to a "D." Mr. Chairman, while you and some of your colleagues such as Representative Greenwood have done a valuable service in scrutinizing computer security policies and practices in U.S. government agencies and departments, that is not enough. As that well-known philosopher Yogi Berra would say, "This is déjà vu all over again." As you pointed out through your invaluable oversight hearings during the early days of Y2K, government agencies had neither plans nor funding for Y2K remediation. Due to your prodding, plans were developed, but funding was not. Until finally, thanks to your efforts and those of so many of your Congressional colleagues, additional appropriations were provided that enabled departments and agencies to become Y2K compliant.

That pattern is being repeated with InfoSec. Agencies now know much more about what they need to do. But the funding is still not there. A General Accounting Office (GAO) report issued earlier this month strongly criticizing the Department of Commerce for InfoSec failures internally carries the clear implication that additional financial resources are needed. Every Federal CIO with whom I speak tells me privately they are in desperate need of additional funding for their InfoSec activities.

The Federal Government needs to make information security a part of every manager's responsibilities, authorize and appropriate new money for agency information security enhancements, fund advanced information security research, and invest in the training and development of more skilled information security workers. There is a long way to go before government receives a passing grade here. For example, when Congress did have a chance to act and make a small investment in deploying and securing e-government by providing funding for the President's E-government Fund, it only provided $5 million of the $20 million requested this year. Government needs to move beyond the rhetoric and invest real funds in this important issue in order to boost its grade.

Corporate Focus and Spending for Information Security

When corporate America addressed the Y2K challenge, information technology was elevated from a back-office, MIS sideshow to a Boardroom-level, center stage mission critical component of most businesses. A corollary of this intensive focus was an understanding by more CEO's that the security of their IT systems is critical. Yet, at best, I give corporate attention a "B-."

One reason for the lower grade is the huge variations between industries and between companies of different sizes. As usual, the financial services industry, so dependent on IT, is leading the charge, with a clear focus—and related dollar commitments—on InfoSec. Telecommunications is also doing reasonably well. But many others, including manufacturing, retail, and health care are much more problematic and uneven. And as we found with Y2K, larger companies are much more understanding of the importance of InfoSec, than medium and small companies.

One of the reasons the major alert on Code Red was necessary was the evidence that many mid-sized and smaller firms were not paying attention to the need to implement the patch, though information about the patch had been widely available for some time. The July 30 press conference was designed to reach what I call the second and third tier IT users, not the first tier users and the IT specialists who had already remediated the problem because they are so focused on it.

But even in corporations that are paying attention to the issue, too many times, the incorrect assumption is made that improving cyber security and fighting cyber crime can be done with technology alone. That is wrong. Just as the best alarm system will not protect a building if the alarm code falls into the wrong hands, a network will not be protected if the passwords are given out freely. Failures in the "process and people" part of the cyber crime solution may, in fact, be the majority of the problems we see. From a strategic point of view, the challenge is to make cyber security a top priority issue. Moving from platitudes to practical action requires the sustained commitment of senior management. The position of "Chief Information Security Officer" should be added to every corporate roster, in my opinion, in order to get this grade to an "A".

Organizations must be willing to invest in the development of comprehensive security procedures and to educate all employees--continuously. We call this practicing sensible cyber hygiene and Internet users have to be vigilant about it.

The primary focus of improving processes and changing behaviors is inside the enterprise. However, the scope of the effort must also take into account the extended organization—supply chain partners, subcontractors, customers, and others that must interact on a routine basis.

Industry-Government Cooperation on Cyber Security Issues

The ad hoc coalition of industry and government representatives that was formed to provide a public service message to counter the Code Red worm this summer is an operational example of successful industry and government cooperation on cyber security. It illustrates just how far the players have come.

A few years ago, industry-government cooperation would have received a "D" in my grade book. Through some hard work on both sides, progress has been made and the dialogue has increased. ITAA worked with the United States Justice Department in 1999 and 2000 to host high-level national industry and law enforcement meetings to share information and begin to open the lines of communications. We also established the Cybercitizen Partnership, a public-private partnership with DOJ to help parents and educators teach children about ethical online behavior and provide "rules of the road" to help protect the Internet from kids who have the skills to threaten the Internet, but not necessarily the guidance to know it is wrong to hack. I think these and the efforts to stand up Information Sharing and Analysis Centers (ISACs) by the Telecommunications, Financial Services, Electric, Transportation, and IT industries have helped to bring us to a "C" grade, and the Code Red coalition raised our grade to a "B-".

In order to get to an "A", the remaining industry sectors will need to stand up and operationalize the ISACs, and all ISACs will need to share confidential information with the government. Equally important and as much of a challenge, government and law enforcement agencies will need to share threat information with the ISACs. In short, we must develop trust in each other; to develop relationships between law enforcement and the private sector that are built on meaningful cooperation. That will not happen overnight. Improved information sharing between government and industry will be a step forward.

In order to solidify that trust, a bill introduced by U.S. Representatives Tom Davis and Jim Moran in the House -- and a bill soon to be introduced by U.S. Senators Robert Bennett and John Kyl in the Senate -- to remove legal obstacles to information sharing should be passed and signed into law this year. Regarding the latter, we hope that Senator Dianne Feinstein, in her key role as Chairman of the Judiciary Committee's Subcommittee on Technology, Terrorism, and Government Information, will take the lead in moving this important bill through the Senate.

Industry-to-Industry Cooperation on Cyber Security Issues

Let me emphasize that while the government has a critical role to play, not just in the U.S. but the government of every nation, vertical industries also have an obligation to communicate on cyber security issues. I think progress has been made in this arena. I believe the grade has moved again from a "D-" a few short years ago to a "C+ / B-" today. How so? The Partnership for Critical Infrastructure Security, begun in December, 1999, has created a cross-sectoral dialogue with collaboration from government to address risks to the Nation's critical infrastructures and assure the delivery of essential services over the nation's critical infrastructures in the face of cyber threats. The Partnership is run by companies and private sector associations and is effectively meeting the industry dialogue challenge. The Critical Infrastructure Assurance Office (CIAO) provides support for the Partnership. Government officials are invited to participate in Partnership meetings on a collaborative basis, and the group is becoming more effective with each meeting.

The Partnership for Global Information Security <http://www.pgis.org> provides a forum for executives from both the public and private sector in economies around the world to share information about InfoSec topics. PGIS members are focused on five areas for collaboration: sound practices, workforce, research and development, cyber crime and law enforcement and public policy. This Partnership arose from the first Global Information Security Summit organized by ITAA in October, 2000 in conjunction with our sister IT associations around the world, collectively known as the World Information Technology and Services Alliance (WITSA).

But much more needs to be done globally. I have advocated creation of an International InfoSec Cooperation Center, analogous to the highly successful International Y2K Cooperation Center, that I know you supported very strongly, Chairman Horn, that would help address the global InfoSec challenge, particularly in developing countries.

International Government Cooperation on Cyber Security Issues

In the area of international governmental cooperation, I give an average grade of a "C-" with the explanation that some portions of international government cooperation are working quite well, while others at the same time are forgetting that the main owners and operators of the information infrastructure around the world are the private sector.

The Council of Europe Cybercrime Convention is one such example of good and bad news mixed. The countries involved in drafting this treaty were able to coordinate their law enforcement efforts and interests reasonably well, so they get high marks. Unfortunately, their grade gets docked substantially for neglecting the commercial sectors in their countries when establishing treaty objectives.

The Council of Europe Cybercrime Convention has improved in many respects through the efforts of the U.S. delegation. Though the US is not a member of the Council of Europe, it does have observer status. However, we were disappointed to learn that several changes of critical importance to industry, privacy groups and noncommercial interests were not adopted in the final version of the Convention. For example, the Convention does not address adequately several important issues, including data retention and surveillance technology mandates, lack of reimbursement for compliance with surveillance mandates, lack of standard privacy protections for law enforcement requests, and potential liability for complying with requests. Therefore, we are concerned that implementation of the Convention will produce a patchwork of costly and inconsistent requirements worldwide that create significant market access barriers for companies, and undermine user privacy.

One important area of particular concern in implementation of the treaty is proposals by foreign governments to mandate that Internet and telecommunications companies maintain, for between one and seven years, massive logs reflecting every innocent user's communications over their networks, or to mandate that companies install new surveillance technologies.

The Council of Europe Cybercrime Convention that the U.S. Government helped to negotiate neither requires nor prevents such mandates.

The data retention mandates would require communications companies to retain enormous amounts of data that they do not retain in the ordinary course of business. Data would have to be retained about every user, without any showing that these users were suspected of engaging in illegal activity. The mandates would compromise user privacy, create costly barriers to entry for U.S. companies seeking to enter foreign markets, and threaten the security of user data by creating a ripe target for hackers. In some countries, such as Holland, service providers are subject to unique surveillance technology standards requirements, which create barriers to deploying international networks in those countries.

Overall Grade

To sum up, there is much work to be done. In addition to improving our letter grades on information security, both industry and government need to strive to have the teacher commend us for playing well with others. Cooperation, communication, and sharing sensitive information are the keys to moving from today's grade, a "C-", to an "A+". Summer vacation is ending, and we are about to begin a new school year in America next week. By working together to build meaningful and effective relationships that recognize the bottom line impact of InfoSec on our businesses, government operations -- and the global economy -- we can all move to the head of the class on cyber security issues.

Thank you and I welcome any questions from the Committee.

Mr. HORN. Thank you very much.

We now have a rather well known person in the whole computer evolution and that's Peter Neumann, the principal scientist, Computer Science Laboratory, SRI International which used to stand for Stanford Research Institute, but you don't say that any more, I gather. Delighted to have you here.

STATEMENT OF PETER G. NEUMANN, PRINCIPAL SCIENTIST, COMPUTER SCIENCE LABORATORY, SRI INTERNATIONAL, MENLO PARK, CA

Mr. NEUMANN. Thank you. Thank you for your very kind introduction.

SRI, I should point out, is a not-for-profit research institute. I would like to believe that what I have to say is motivated, not by any corporate need or any allegiance to any particular ideas.

I think the message that I want to give you is pretty well taken care of in my written testimony. I'm going to summarize it very briefly.

The bottom line here, I think, goes back to September 19, 1988 when Robert Morris, who was at the time chief scientist of the Computer Security Center at NSA, said, "To a first approximation, every computer in the world is connected to every other computer in the world." That was 13 years ago. The situation is much worse now. The number of computers that are connected to the Internet is enormous.

A month and a half later, it was his son who, in a research experiment that went awry, created the Internet worm which, in some sense, was the beginning of all of this nonsense that we have going on relating to worms, viruses, trojan horses, and so on. Letter bombs coming through e-mail.

I would like to take a broader view of the problem and make the very bold statement that what we're really talking about is not viruses, worms and related subjects but the fact that the computer security and information security infrastructure, including all the networking, is riddled with so many security flaws that it is virtually impossible to expect that we can have any meaningful sense of security, given the infrastructure that we have today, and I want to elaborate on that to some extent.

Larry Castro mentioned the classical DOD mantra which is defense in depth. What we have is weakness in depth. There are vulnerabilities essentially everywhere, in the mass market desktop systems, in the server systems, in the networking, in the embedding of even some of the cryptography in the world into platforms that are again riddled with security vulnerabilities. So let me very briefly go through what I've called a set of seemingly dirty truths that remain largely unspoken and under-appreciated in my written testimony.

The first is that what we have today is a far cry from what is straightforwardly possible. Back in 1965 I was part of an ARPA, Advanced Research Project Agency, project in MIT in Bell Labs which developed a commercial operating system that had enormous research advances in it. If we look at what's happened in the last 36 years, many of those research advances and other similar advances have not found their way into the mainstream. What this leaves us with, especially me as a researcher, is the very gnawing feeling, annoying and gnawing, that the good stuff that should be coming out of research is not finding its way into the market place.

One of the great adages of our society is that the market place is supposed to drive everything. Unfortunately, the market place seems to be much more interested in whiz bang features and rush to market place than it is in having systems that are truly reliable, secure, and available in high degrees and survivable in the face of all sorts of problems.

The problems that we're addressing today in terms of worms, viruses and so on are really the tip of the iceberg. If in fact it is possible to penetrate systems from anywhere in the world, irrespective of what the laws are in this country, we have a fundamental problem. Whereas the laws are important and the laws are in fact useful in many respects, the comment that you quoted earlier was based on the fact that if you cannot trace back to find out where the problem is coming from because of network weaving and the lack of accountability and the lack of identity and authorization and authentication, then the laws may be absolutely worthless except as a possible deterrent for the people who believe that those laws are applicable to them.

So we have a situation in which the Internet provides the opportunity for attacks from essentially anywhere in the world, and many of those attacks can be created by individuals for which it is almost impossible to trace them back. I appreciate the optimism stated in the previous panel, but I believe that one of the most important things here is finding ways of incentivizing the improvement in the systems that we're dealing with.

The previous panel dealt primarily with the methodology of patching. Patching is extremely limited. If you start with something that is fundamentally insecure, you add patches, you may or not remove a vulnerability and, in fact, you may introduce new vulnerabilities. But because there were so many vulnerabilities in the original products, you merely transfer the attacks to new vulnerabilities.

If you look back at the Internet worm of 1988, essentially all of the vulnerabilities that existed at that time—and there were four of them—are still present today in one form or another. They may not be the specific flaws in the specific code that was used at that time, but the characteristics of those four flaws are all present in systems today. This suggests that we are not progressing as we should be progressing. So let me very briefly go through some of my seemingly dirty truths.

I don't really need to go into detail to you on the President's Commission on Critical Infrastructure which found a great many vulnerabilities. The Internet, being enormous and relatively uncontrollable, and being international is not really the culprit itself. It's all of the systems that are attached to it. The presence of these almost trivial to perpetrate Internet mail bombs, for example, are the result of the fact that there is very little inherent security in the systems that we're dealing with. I mentioned the education problem indirectly, but I think I should mention it very specifically.

The difficulties in developing very secure systems are enormous. They require a great deal of education. They require good software engineering practice, which is not very widely found in this country or in other countries, as well. To develop systems that are very secure, life critical, ultra-reliable takes an enormous amount of effort and, although there has been enormous research in those areas in the past 40 years or so that I've been involved in this area, the research is not finding its way into the market place.

Another dirty truth is this outsourcing thing, and you may remember from the Y2K business the fact that the air traffic control remediation was done by foreign nationals, essentially unbeknownst to the technical people at the FAA. That was rather startling when it was uncovered. The notion that DOD would like to outsource all of its critical functionality—for example, system administrators, is startling. If you can't have a trustworthy system, then you outsource the management of it to somebody who might be even less trustworthy than the system itself. This does not sound like a good way to run a ship.

In general, simple systems and simple solutions are not very effective. This gets us into the laws, to some extent. One of the simple solutions that Congress has come up with is the Digital Millennium Copyright Act which has a chilling effect on the research community and which, in fact, is seriously hindering, in my opinion, the development of systems that are more secure because somebody who points out that a particular system is not secure is immediately threatened as in the case that occurred last week of somebody who pointed out that his local newspaper had its Web site totally available to anybody in the world and anybody could do anything to it with essentially no authorization. He was threatened with 5 year felony charge for having pointed out that this problem existed. We're shooting the messenger in many cases in the enforcement of the Digital Millennium Copyright Act.

The Uniform Computer Transactions Act, the UCITA legislation which is working its way through many States, has a chilling effect as well. It allows the vendor or the developer to declare absolutely no liability for anything that goes wrong. This is a very strange business. I remember in the Y2K era there was legislation that said the remediators for Y2K should be absolved of their liability and should be able to have a certain freedom in that respect. I believe that when we get to the issue of what the laws can do, the area of liability is going to be a very important one.

There has been legislation in the past and directives from the government that have dumped down security. Examples of that include the use of good crypto. There's one example that is extremely important to me. I was at a workshop yesterday and the day before on electronic voting systems. Here's an example where there's a mad rush to replace the punch card ballots after Florida with all electronic voting systems. This is an example where the simple solution of rushing into an electronic voting system does not solve the problem at all because every existing system today has essentially no assurance that the vote as cast is actually the vote as counted. The vendors say trust us. We have proprietary software. We can't show anybody the software because it would diminish the security of the system which is actually nonsense in many cases and that we just have to trust them that they're going to do everything right because they know what they're doing. This is an example of an apparently simple solution that in fact has very serious implications.

Another example is the use of legislation to insist on filters to solve the spam problem. This doesn't work, and we've had cases where the Bible and the encyclopedias and all sorts of things are banned or where people's Web sites are banned because their name happens to include the string S-E-X like Essex and Sussex.

Now, my conclusions are very simple. We need to address technological problems with technological solutions. We need to address legal problems with legal solutions. We need to address all of the problems of computer security, computer reliability, with a combination of these approaches. Laws by themselves do not solve the problem. Technology by itself does not solve the problem. We need a combination of socio-economic and political, technological and other approaches. So at the very minimum, we need what I think would be radically improved security reliability and availability in the systems that we are using, not only in our critical infrastructures, but in our Internet conduct of normal business.

As I said several times, it is really unfortunate that many of the important research advances of the last 45 years or so have not found their way into the market place. I don't know how you can incentivize that more effectively, but I think you've got to find ways to do it. There are roles that NIST can play. In the former session, the common criteria was mentioned. NIST has been involved for many years in the elaboration of the common criteria. If those were systematically used in an effective way, it would be tremendously valuable.

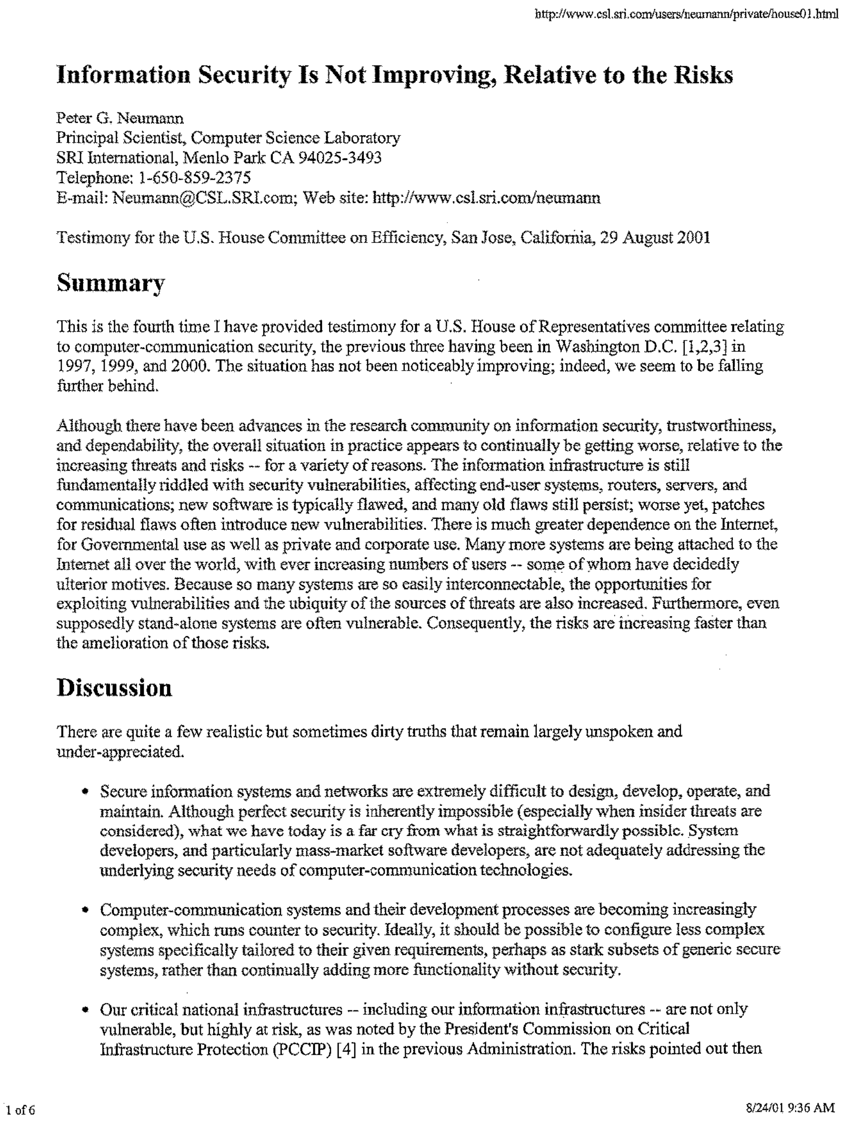
One of the examples. One of my doctoral students has just written a thesis on applying the common criteria to the electronic voting problem and demonstrates that even if all of those criteria that she's constructed were satisfied, it's still not enough, but it's a major, major step forward. So I recommend strong endorsement of that approach.

I'm very concerned about liability issues. I believe that liability legislation could go a very long way. The idea that a vendor can disclaim all of its liability is a joke, although it's good marketing. I believe that Federal legislation that imposes strict liabilities on end consequential damages for gross negligence in not only system development but corporate misbehavior would be very valuable. There's a proposal today that I saw about making Web site and system purveyors liable for not using best practices when it comes to security, for not installing the patches that have been given to them and, in some cases, they've been told that they were critical. In some cases, they weren't told at all.

So in my final comment, there is some wonderful research and development out there and it really needs to be worked into the development of systems that are substantially more secure, more reliable. Along with that goes the education and the training and everything else that's needed to make it work. But if I look around the country, I do not see the adequate attention to software engineering, to security, to reliability in even graduate programs and certainly not in undergraduate programs.

Thank you very much.

[The prepared statement of Mr. Neumann follows:]



Information Security Is Not Improving, Relative to the Risks

Peter G. Neumann
Principal Scientist, Computer Science Laboratory
SRI International, Menlo Park CA 94025-3493
Telephone: 1-650-859-2375
E-mail: Neumann@CSL.SRI.com; Web site: http://www.csl.sri.com/neumann

Testimony for the U.S. House Committee on Efficiency, San Jose, California, 29 August 2001

Summary

This is the fourth time I have provided testimony for a U.S. House of Representatives committee relating to computer-communication security, the previous three having been in Washington D.C. [1,2,3] in 1997, 1999, and 2000. The situation has not been noticeably improving; indeed, we seem to be falling further behind.

Although there have been advances in the research community on information security, trustworthiness, and dependability, the overall situation in practice appears to continually be getting worse, relative to the increasing threats and risks -- for a variety of reasons. The information infrastructure is still fundamentally riddled with security vulnerabilities, affecting end-user systems, routers, servers, and communications; new software is typically flawed, and many old flaws still persist; worse yet, patches for residual flaws often introduce new vulnerabilities. There is much greater dependence on the Internet, for Governmental use as well as private and corporate use. Many more systems are being attached to the Internet all over the world, with ever increasing numbers of users -- some of whom have decidedly ulterior motives. Because so many systems are so easily interconnectable, the opportunities for exploiting vulnerabilities and the ubiquity of the sources of threats are also increased. Furthermore, even supposedly stand-alone systems are often vulnerable. Consequently, the risks are increasing faster than the amelioration of those risks.

Discussion

There are quite a few realistic but sometimes dirty truths that remain largely unspoken and under-appreciated.

- Secure information systems and networks are extremely difficult to design, develop, operate, and maintain. Although perfect security is inherently impossible (especially when insider threats are considered), what we have today is a far cry from what is straightforwardly possible. System developers, and particularly mass-market software developers, are not adequately addressing the underlying security needs of computer-communication technologies.

- Computer-communication systems and their development processes are becoming increasingly complex, which runs counter to security. Ideally, it should be possible to configure less complex systems specifically tailored to their given requirements, perhaps as stark subsets of generic secure systems, rather than continually adding more functionality without security.

- Our critical national infrastructures -- including our information infrastructures -- are not only vulnerable, but highly at risk, as was noted by the President's Commission on Critical Infrastructure Protection (PCCIP) [4] in the previous Administration. The risks pointed out then are essentially all still present today, and have not substantially diminished. In some senses, the risks may be greater because of increased opportunities for exploitation of the vulnerabilities.

- The Internet is an enormous distributed system. It is international in nature. U.S. laws intended to outlaw bad behavior here seem to have relatively little effect in thwarting malicious activities from off-shore. Because of generally weak information security, threats arising from anywhere in the world are often very difficult to trace accurately. Improving the dependability and security of our computer and communication systems would be a good place to start, with sensible uses of cryptography, less easily bypassed user authentication, and meaningful accountability (for example). Laws and law enforcement do have roles, but cannot be the primary means of discouraging misuse.

- Internet-connected systems are especially vulnerable to viruses, worms, Trojan horses, e-mail letter bombs, calendar-time bombs, and other malfeasant attacks, and remain so despite nominal improvements. The long history of relatively simple-minded mail bombs (Melissa, ILoveYou, SirCam) and other attacks such as the recent Code Red variants suggest that much more destructive attacks can easily be conceived and perpetrated. Denials of service and especially widely distributed denial-of-service attacks are easy to mount, and can be quite very debilitating. However, much more serious system subversions are also easy to perpetrate.

- Education relating to computer systems and computer security is woefully inadequate. The technical field has developed very rapidly, and education is always hard-pressed to keep up. But the problems are particularly vital with respect to systems with critical requirements. For example, developers of secure systems, ultra-reliable systems, life-critical systems, and other systems with stringent requirements need to be more than merely competent; extensive backgrounds in dependable software engineering are required. In some cases, an understanding of mathematics far beyond what the average college student receives is necessary. System administrators are generally unprepared for the sophistication required to deal with the flawed system security and weak configurations; the steady flow of security patches attempting to fix earlier flaws often remain uninstalled. Managers often do not have a clue. Legislators need to have a much better understanding of the social and technical implications. Some people have advocated certification of developers and programmers; however, this is a very contentious matter, which if adopted badly could easily create a sense of false security. Overall, much greater emphasis on education is needed, for training would-be experts and illuminating less technical folks as well.

- Outsourcing of critical functionality to people who must be trusted even if they are not trustworthy is a riskful strategy, although it is being increasingly used in various branches of government. Dependence on questionable outsiders for software development, operations, maintenance, and administration presents many additional risks. DoD outsourcing of critical system administration functionality and the recent use of unvetted foreign nationals for the Year-2000 remediation of air-traffic control software (apparently unbeknownst to the technical people at the Federal Aviation Administration) are recent examples of potential risks.

- In general, seemingly simple solutions are often not effective. They are misleading, and tend to offer a false sense of security. Several examples are given here:

    - The existing Federal Digital Millennium Copyright Act (DMCA) and the emerging Uniform Computer Information Transactions Act (UCITA, either passed or under consideration in various states) both seem to be having a chilling effect by seriously impeding the research community from helping to improve security, and by allowing system developers and vendors to hide behind inferior security. Also, genuinely well-intentioned whistleblowers are increasingly finding themselves threatened with prosecution.

- Past government efforts to prevent or impede the use of strong cryptography have seriously retarded progress in security. Cryptography and strong security should have been routinely embedded into our standard protocols and products, but unfortunately this has not happened. Security is extremely difficult to retrofit into systems that are fundamentally flawed. It should not be surprising to anyone that many cryptographically enhanced systems are so easily broken.

- At the moment, there is a mad rush to try to replace punched-card ballots and their vote-counting systems with all-electronic voting systems. However, today's fully electronic voting systems (such as Direct Recording Equipment, DREs) and especially Internet voting software all have a fundamental lack of meaningful accountability. Because of the absence of user-verified independent audit trails, there is typically no assurance whatever that a vote as cast is identical to the vote as counted. Although some people have hope that this serious deficiency could be overcome in the future, it may be possible only at the sacrifice of voter privacy. In addition, Internet voting adds opportunities for election fraud from anywhere in the world, not just locally within a given precinct. Proprietary electronic voting and Internet voting systems are both highly susceptible to insider fraud that can seriously alter the results of elections; in addition, Internet voting is especially susceptible to bogus polling places and fraudulent voting software, plus hacker attacks, viruses, worms, calendar-time bombs, and external denial-of-service attacks (to mention just a few security risks). The proprietary nature of the election software results in voters having to trust software that is seldom subjected to external scrutiny. However, even open examination of the software would not be enough to prevent election fraud. I have grave doubts that fully electronic voting systems will ever be adequately fraud resistant. Interestingly, the problem of attaining high-integrity election systems is a paradigmatic example of the general system security problems, opening up many of the usual problems -- inadequate requirements, lack of adequate standards, unvetted proprietary software, and many unchecked operational problems.

- Attempts to hinder Internet spamming attacks (with potentially huge amounts of unsolicited and often offensive e-mail) by legislation requiring filtering are always going to be of limited effectiveness. Simplistic spam filters are usually counterproductive, as they have often filtered out such content as the Bible, encyclopaedias, valuable Web sites and people's names because they contained some particular character string (Sussex and Essex are common examples), and other generally desirable materials.

Conclusions

One conclusion from the above discussion is very simple: we are not progressing sufficiently in our attempts to achieve acceptable information security. Essentially everything I wrote in my 1995 book [5] about computer-related risks -- and particularly security risks -- still seems to apply today.

A broadly coordinated effort is needed, not just palliative measures. In principle, technological problems need technological solutions, not legal solutions. Legal problems need laws and enforcement, not technological solutions. In general, technologists are better at understanding the technical problems, and similarly for the legal communities. Mismatched solutions tend not to be effective. However, many of our emerging problems require a careful combination of approaches cognizant of the full spectrum of social, economic, technological, legal, and other needs. Nevertheless, at the very minimum, we need vastly improved security, reliability, dependability, and survivability in the face of adversity, in the computer and communication systems on which we critically depend for so many things.

It is unfortunate that many important research advances are not finding their way into practice. In the research community, we have known how to do much better for a long time. For example, many approaches for developing and operating vastly more secure systems and networks can be found in a recent report [6], including system and network architectures that sharply reduce the necessity for trusting potentially untrustworthy components and individuals, while also realizing extensive interoperability and ability to evolve over time while still fulfilling the desired requirements. However, many factors have contributed to our having less information security than we deserve, including (for example) U.S. Government's past restrictions on cryptography policy, the House's predominant concern with the immediate future rather than looking farther ahead, corporations often determined to deliver functionality without regard to security, customers lacking awareness of the risks, and a general lack of commitment to progress.

What Might Congress Do?

- To begin with, Congress should avoid repressive legislation that disincentivizes better security, as has been the case for example with past constraints on the use of cryptography and the implicit sanctioning of weak systems. Unfortunately, on the other hand, leaving progress solely to the marketplace evidently does not work, because there are very few financial incentives to significantly improve security in the absence of serious government and customer demands. The DMCA legislation is already causing enormous grief in dumbing down progress and hampering the research community's ability to inspire improved security; that needs to be revised.

- There are various roles that the National Institute of Standards and Technology (NIST) could play, particularly in the development of relevant interoperable vendor-nonspecific security standards. Although the Common Criteria are emerging as a potential framework for security, there is still much to be done to make that process realistic. For example, NIST (when it was the National Bureau of Standards) was actively involved in election standards; a serious application of the Common Criteria to voting systems would be a major step forward. H.R. 1165 could be a possible step in that direction for security standards of general applicability.

- Another direction to consider would be liability legislation. Emerging one state at a time in state legislatures, UCITA among other things allows information-system developers and vendors to disclaim essentially all liability for failures of their products. Perhaps Federal legislation that imposes strict liabilities and consequential damages for grossly negligent system development and flagrant corporate misbehavior would go a long way toward ratcheting up the dependability, reliability, and security of our information infrastructures.

- Relevant research and development efforts are still needed to provide the basis for dramatically increasing the security and reliability of our computer systems and networks. However, that research also needs to find its way into systems that are procured by the U.S. Government, setting a good example for others.

- Improved computer-related education is an area strongly in need of support, to attempt to overcome many of the problems noted above.

Overall, there are few incentives today for the development, operation, and maintenance of robust, secure, reliable computer-communication systems that are so badly needed as a basis for our future. That needs to be corrected.

References

(Hot links to the references are included in the Web version of this document: http://www.csl.sri.com/neumann/house01.html)

1. Peter G. Neumann, *Computer-Related Risks and the National Infrastructures.* U.S. House Science Committee Subcommittee on Technology, 6 November 1997. In *The Role of Computer Security in Protecting U.S. Infrastructures,* Hearing, 105th Congress, 1st session, No. 33, 1998, pages 64--99, ISBN 0-16-056151-5, 1997, preceded by the oral presentation on pages 61--63. Oral responses to oral questions are on pages 101--118, and written responses to subsequent written questions are on pages 148--161. (Written testimony at http://www.csl.sri.com/neumann/house97.html and written responses to written questions at http://www.csl.sri.com/neumann/house97.ans)

2. Peter G. Neumann, *Melissa is Just the Tip of a Titanic Iceberg.* Written testimony, for the U.S. House Science Committee Subcommittee on Technology, hearing on 15 April 1999. (Written testimony at http://www.csl.sri.com/neumann/house99.html)

3. Peter G. Neumann, *Risks in Our Information Infrastructures: The Tip of a Titanic Iceberg Is Still All That Is Visible.* Written testimony, for the U.S. House Science Committee Subcommittee on Technology, hearing on 10 May 2000, introduced into the record by Keith Rhodes of the General Accounting Office on my behalf. (Written testimony at http://www.csl.sri.com/neumann/house00.html)

4. Tom Marsh (ed), *Critical Foundations: Protecting America's Infrastructures,* President's Commission on Critical Infrastructure Protection, October 1997. (CIAO Web site at http://www.ciao.org and PCCIP report information at http://www.ciao.org/PCCIP/index.htm)

5. Peter G. Neumann, *Computer-Related Risks,* Addison-Wesley, 1995.

6. Peter G. Neumann, *Practical Architectures for Survivable Systems and Networks,* SRI report for the U.S. Army Research Laboratory, 30 June 2000. (html, PostScript, and pdf versions available at http://www.csl.sri.com/neumann)

Mr. HORN. Thank you. We appreciate those comments. They're stimulating, to say the least.

Scott Culp is the lead security program manager for the Microsoft Corp. We're glad to have you with us.

STATEMENT OF SCOTT CULP, MANAGER, MICROSOFT SECURITY RESPONSE CENTER, MICROSOFT CORP.

Mr. CULP. It's a pleasure to be here. Thank you for the opportunity to appear today at this hearing. My name is Scott Culp. I'm the manager of the Microsoft Security Response Center. I'd like to commend the chairman and the committee for leadership on government computer security. It's a matter that we take with great seriousness, not only because the U.S. Government is one of our largest customers but also as an issue of civic duty. Mobile hostile code such as viruses and worms pose an ongoing threat to the security of our network systems. Every vendor's platforms can be affected and countering worms and viruses is a challenge that the entire IT industry must address.

As an industry leader though, Microsoft has a number of ambitious programs designed to combat hostile code and to safeguard our networks. The good news is that the basic design and architecture of the systems that we all use is sound. Viruses and worms only succeed when they can bypass the security these systems provide. Some say to do this is for the virus or worm to exploit a security vulnerability, a hole in the system's armor.

To reduce the occurrence of security vulnerabilities and out products, Microsoft has had an ambitious program under way for over 18 months called the Secure Windows Initiative which has as its goal nothing less than a generational improvement in the development practices that we use. We're providing advanced security training to our developers, we're building leading edge tools that dramatically improve how we test our software and we're using innovative techniques like penetration test teams in which we intentionally try to break into our own products. At the same time, we're increasing our use of independent third party experts, both inside and outside the government, to validate our work.

But software is and always will be a human activity subject to human frailties. No piece of bug-free software has ever been developed and none ever will be. To root out any security vulnerabilities that may have slipped through our development and testing processes, Microsoft has assembled a Security Response Center which even our critics acknowledge to be the best in the industry. We investigate every claim of a security vulnerability affecting one of our products. When one is found, we quickly develop updated software and we deliver it through a well-publicized Web site, a free mailing list with over 200,000 subscribers and automated sites like our Windows Update Web site.

Last year alone, we received over 10,000 reports. We investigated every single one of them. Of these, a grand total of 100 security vulnerabilities in all Microsoft products was found.

The other way that viruses and worms typically succeed is through social engineering, tricking the user into undermining his or her own security. To combat viruses and worms that use these techniques, Microsoft announced in April of this year a war on hostile code. One outcome of this campaign is something called the Outlook E-mail Security Update which blocks e-mail viruses. To the best of our knowledge, the number of customers who, after applying this update, have subsequently been affected by an e-mail virus is zero worldwide.

Another element of the war on hostile code is a new feature in Windows XP called Software Restriction Policies which stop viruses and worms from executing on the machine even if the user downloads them and tries to run them.

In addition to improving our products, we work collaboratively with our colleagues throughout the security community. Microsoft senior executives are also fully engaged in the U.S. government's security policy initiatives. For example, Bill Gates, Microsoft's chairman and chief software architect, received a Presidential appointment to a National Infrastructure Assurance Council and Craig Monday, Microsoft's senior vice president and chief technical officer for strategy and policy, received a Presidential appointment to the National Security Telecommunications Advisory Council.

But technology is not a panacea. Breaking into computers and writing viruses and worms to damage them is a crime and it's important that we not lose sight of that fact. Just as we can never realistically expect the threat of burglary or bank robbery to end, we should realize that cyber crime will always be a fact of life and, accordingly, Microsoft strongly supports enforcing our society's cyber crime laws and we work closely with domestic and international authorities and we strongly support increased funding for computer crime enforcement.

In sum, Microsoft takes its responsibilities as an industry leader very seriously and we believe that the efforts of Microsoft and its colleagues in the industry will improve the security of the U.S. government's networks, the Nation's, and the world's. Thank you, Mr. Chairman.

[The prepared statement of Mr. Culp follows:]

Prepared Testimony of Scott Culp
Manager, Microsoft Security Response Center
Microsoft Corporation

Before a field hearing of

The Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations
Committee on Government Reform
U.S. House of Representatives

August 29, 2001

Mr. Chairman and Committee Members, thank you for the opportunity to appear today at this hearing on reducing the threats posed by computer viruses and worms to the workings of the U.S. Government. My name is Scott Culp, and I am the Manager of the Microsoft Security Response Center at Microsoft Corporation. I wish to commend the Chairman and the Committee for leadership on the issue of government computer security. It is a matter we take with grave seriousness, not only because the U.S. Government is one of our largest customers but also as a matter of civic duty.

I. INTRODUCTION

Mobile hostile code, which includes computer worms and viruses, poses an ongoing threat to the security of Internet-connected systems. The recent Code Red virus is the latest reminder of the widespread damage that worms and viruses can cause. Indeed, the danger posed by mobile hostile code has long been recognized – the Morris Worm disabled portions of the Internet as long ago as the late 1980s and caused a level of frustration and anger comparable to the publicized viruses and worms of the past year.

Countering worms and viruses is a challenge that the entire information-technology industry must address. We know that every vendor's platforms can be affected. The Code Red virus was aimed at Microsoft's programs, and we are one of its victims as well as one of its targets. Concomitantly, our colleagues and peers from other software platforms, both proprietary and open source, have been victimized by worms such as Lion, Ramen, and SADmin.

As a society, we must recognize that hostile code is, ultimately, a human activity and, in particular, a criminal activity. To counter this threat, we are doing innovative work on several fronts that we believe will make our software significantly more resistant to worms and viruses and thus will benefit the U.S. Government – and all of our customers. We also support the responsible handling of vulnerability information by the software industry itself.

II. MICROSOFT'S EFFORTS TO IMPROVE COMPUTER SECURITY

Microsoft is an industry leader, and we take this responsibility seriously in all its aspects and especially regarding security. Our efforts to improve computer security cover a wide array of security considerations. I will discuss four of these today: (1) improving software development practices at Microsoft; (2) our state-of-the-art Microsoft Security Response Center (MSRC); (3) Microsoft's "war on hostile code" initiative; and (4) our senior executives' leadership in the Nation's critical infrastructure protection policy.

A. Improving Software Development Practices

To limit the number of vulnerabilities, we recently announced an ambitious program called the Secure Windows Initiative with the goal of nothing less than a generational improvement in our development practices. The Secure Windows Initiative includes several elements, as follows.

First, we are providing advanced training to our own developers so that they better understand the most current threats and vulnerabilities.

Second, we have developed superior code analysis tools that root-out subtle flaws that may result in vulnerabilities. These tools can perform a level of inspection and analysis that far exceeds what human reviewers could perform. The initiative is also helping to assure the quality of our products by broadening the use and scope of automated testing tools that we apply to our own software code. In other words, we have developed more innovative tools to test our own software with far greater complexity and depth than ever before.

Third, we have expanded the use of non-traditional testing methods to test our software, including "penetration test-teams" which intentionally attempt to break into our own products. We also recently created an organization outside of Microsoft's normal development framework that provides independent testing.

Finally, we work closely with third-party experts including NAI Labs and the International Computer Security Association as well as with security experts in the U.S. Government and the British Government as part of their respective security evaluation processes. Indeed, Microsoft has a source-licensing program with over 100 different non-governmental review organizations that have access to our source code and the ability to review it for vulnerabilities. Through these tools and techniques, we believe our future products will have significantly fewer security vulnerabilities, although we know the number will never be zero.

B. Microsoft's Security Response Center

Software engineering is a human activity and is subject to human frailties. No software firm has yet built a product without "bugs," and none ever will. Some of these "bugs" take the form of security vulnerabilities that could be subsequently exploited by criminals. Because our customers' security is a paramount concern for Microsoft and in order to counter this criminal activity, Microsoft has developed a security response mechanism.

Although some other software companies have security response organizations, we believe, with all due humility, that the Microsoft Security Response Center (MSRC) is the industry's state of the art. The MSRC thoroughly investigates all reported vulnerabilities and then builds and disseminates any needed security updates. In 2000, for instance, we received over 10,000 reports from our customers, every one of which we investigated, culminating in a grand total of 100 confirmed vulnerabilities across the full Microsoft product line. When we do find a bona fide vulnerability in one of our products, we deliver updated software through a well-publicized web site, a free mailing list with over 200,000 subscribers, and automated sites like WindowsUpdate which provide consumers with current security information.

Despite our state-of-the-art security response process, we recognize that – as Code Red illustrated – further improvements are needed. The vulnerability that was eventually exploited by Code Red was reported to us in June of 2001. We developed a patch in roughly ten days and publicized the patch for over six weeks prior to Code Red's appearance. We believe that our initial efforts spared many of our customers from being significantly affected by the worm. But clearly, our efforts to protect all of our customers met with less success than we hoped for. We have a number of initiatives underway, with the goal of making it easier for customers to know which updates they need and simplifying the process of keeping their systems secure.

C. Combating Hostile Code

While we must find and fix vulnerabilities, we must also provide protection against the other typical avenue of attack used by viruses and worms – namely, using "social engineering" to trick users into allowing them to operate. Microsoft announced a "war on hostile code" at the

RSA Data Security Conference in April of 2001, with the goal of providing new product features that provide this protection. This broad-ranging initiative includes the following components.

First, the Microsoft Outlook Email Security Update, which we released as a stand-alone update over one year ago, is now built into the recently-released Outlook 2001. This directly addresses threats like the "Melissa" or "I Love You" viruses that trick end-users into undermining their own security and then manipulate functions within the users' email system. To the best of our knowledge, not a single customer who applied the Update has been affected by an email virus.

Second, we integrated a personal firewall into Windows XP that helps avoid attacks against home-users who utilize DSL or cable connections with the Internet.

Third, we added software restriction policies in Windows XP that allow a systems administrator to configure exactly what software can and cannot run on the system. In other words, even if hostile code gets on a particular machine, these restrictions defang it and prevent it from running.

D. Microsoft's Executive Leadership

Our involvement in computer security begins with the leadership of our senior executives. Microsoft's senior executives are fully engaged in the U.S. Government's security policy initiatives, international outreach, and creation of a vision for a more secure computing infrastructure.

For example, Bill Gates, Microsoft's Chairman and Chief Software Architect, received a presidential appointment to the National Infrastructure Assurance Council (NIAC). The NIAC is intended to advise the President and encourage cooperation between the public and private sectors to address physical threats and cyber threats to the Nation's critical infrastructure.

Craig Mundie, Microsoft's Senior Vice President and Chief Technical Officer for Advanced Strategies and Policy, received a presidential appointment to the National Security Telecommunications Advisory Council (NSTAC). The NSTAC advises the President on policy and technical issues associated with telecommunications.

In addition, Steve Lipner, Microsoft's Lead Program Manager for Security, serves on the Congressionally-mandated Computer Systems Security and Privacy Advisory Board.

Finally, Howard Schmidt, Microsoft's Corporate Security Officer, is deeply involved in G8 and United Nations initiatives and serves on the Board of the Partnership for Critical Infrastructure Security, a cross-sector, cross-industry effort supported by the National Security Council and the U.S. Department of Commerce. He recently participated in a U.S.-Australia bilateral meeting on critical infrastructure protection led by the U.S. Departments of State and Commerce. Moreover, he is the first president of the information technology industry's Information Sharing and Analysis Center to coordinate information-sharing among information-technology companies and with the U.S. Government.

Our senior executives care passionately about security. They drive our thinking on what we need to do in the decades ahead to create a more secure Internet infrastructure, and they simultaneously play a leading role in shaping the general U.S. technological and policy environment.

III. LARGER COMMUNITY EFFORTS TO IMPROVE COMPUTER SECURITY

In this digital age, we have all been awed by what technology can do to facilitate communication, productivity, commerce, and learning. Yet technology is not a panacea that by itself will defeat hostile code written by criminals. To be perfectly clear: This is a battle of good versus evil. We employ innovative and intelligent software developers, but there are also tremendously innovative computer criminals who have as their mission the penetration and stealing of digital information. Just as no one has built a truly impenetrable house or car, no one has produced impenetrable software. We will always face online criminals just as we always face home burglars or car thieves, and we will never see the end of the battle for computer security.

Our society does not tolerate people breaking into brick-and-mortar homes and businesses, but our society inexplicably seems to have more tolerance for computer break-ins. Yet breaking into computers is just as much a crime as breaking into brick-and-mortar homes and businesses, and both types of break-ins harm innocent people and weaken American businesses. Computer attacks need to be treated as the criminal activities that they most assuredly are.

Accordingly, Microsoft strongly supports enforcement of our society's cybercrime laws. To this end, Microsoft works closely with domestic and international law enforcement. We actively participate in U.S. Government efforts to increase critical infrastructure protection, such as our support for legislation that facilitates information-sharing between industry and government. And we strongly support increased funding for computer crime enforcement. As an example of our close relation with law enforcement, we reported our knowledge of the "I Love You" virus to the U.S. Government within minutes of learning of it, and the U.S. Government acted on the report shortly thereafter. We welcome the continuation, expansion, and improvement of these collaborative efforts. And we support the bolstering of cybercrime law enforcement by the U.S. Government.

Furthermore, Microsoft believes that consensus is needed within the IT community concerning the handling of vulnerability information. We have very strong relations with many third-party security entities, and both Microsoft and the larger community benefit greatly from their expertise. Most security researchers handle security vulnerabilities responsibly; they report such vulnerabilities to the vendor and then work with the vendor to develop a fix. When the remedy is completed, they assist in notifying the user community about the vulnerability and the available solution in a way that denies information that could be used by criminals to exploit the vulnerability. This process produces a net gain in online security, and Microsoft is working to build a consensus in support of this paradigm.

In sum, Microsoft takes its responsibility as an industry leader and as a technology provider to the U.S. Government, to the Nation, and to the world very seriously. We demonstrate this through Microsoft's Secure Windows Initiative, the Microsoft Security Response Center, our efforts to combat hostile code, and our executive leadership's involvement in governmental initiatives. While we engage in state-of-the-art work to improve computer security, violations of computer security are ultimately criminal activity. We are proud of our active support of and close collaborative relationship with law enforcement in its efforts to investigate and prosecute these criminals and to deter them from committing their crimes in the first place. We believe that the efforts of Microsoft and its colleagues in the industry will improve the security of the U.S. Government's networks, the Nation's, and the world's.

###

Mr. HORN. Thank you very much. Our second to last witness is Stephen Trilling, senior director of advanced concepts from the Symantec Corp.

STATEMENT OF STEPHEN TRILLING, SENIOR DIRECTOR OF ADVANCED CONCEPTS, SYMANTEC CORP

Mr. TRILLING. Thank you, Chairman Horn and members of the subcommittee for giving me the chance to testify today about the growing threat of computer worms to our national and economic security.

Mr. Chairman, I'd also like to commend you and your subcommittee for your leadership in examining cyber security issues and for releasing the report card on computer security in the Federal Government.

My name is Stephen Trilling. I'm here representing Symantec Corp. We're a world leader in Internet security technology, providing solutions to government, individuals, enterprises, and Internet service providers. At Symantec I oversee our Advanced Concepts Team, a group dedicated to studying new security threats and creating new technologies to better protect our electronic frontiers.

Prior to this role, I directed our Anti-Virus Research Group, a worldwide team responsible for analyzing and creating fixes for computer viruses and other malicious threats.

I'd like to first discuss the difference between computer viruses and worms such as Code Red. Traditional viruses, while potentially very damaging to individual computers, spread only very slowly to other computers. Users can inadvertently spread traditional viruses when they share infected files with one another. For example, through user-initiated e-mail. Again, since viruses rely on humans to spread, they spread only very slowly between different computers.

I'd like to direct your attention to the screen to show a short simulation of how traditional viruses spread. In the simulation, each large circle represents an individual organization and each of the small dots inside the large circle represents a computer. What we're going to do is hypothetically plant the virus in the left hand organization shown as a single red dot—although I know from trying this out earlier the dots look black on that screen—and watch how it spreads over time. You can go ahead and start.

So what we're looking at is at the concept virus. It's a simple virus that spreads when people exchange infected documents with each other and, as you can see, viruses spread over days or even weeks at about the rate that people exchange information. This picture is how the world looked to us up until the Melissa threat was released just over 2 years ago.

In contrast to traditional viruses, computer worms—as has already been mentioned today—are designed specifically to spread over networks to as many computers as possible. Most worms, such as Melissa and LoveLetter, hijack e-mail systems to spread themselves automatically and, because worms spread largely or completely without human interaction, they can infect new users at an exponential rate without regard to borders or boundaries.

So I'd like to go back to the simulation and watch how a single worm infection can ravage an organization. You can go ahead and start that. As you can see, computer worms have completely changed the rules of our game. Looking ahead, there are three factors that increase the potential for future damage from worms. No. 1, our global economy is clearly becoming more dependent on the Internet. Computers connected to the Internet now control e-commerce sites, power generation, electronic business supply chains, government transactions, and numerous other operations. A properly targeted computer worm could hobble any of these systems, threatening our national security.

No. 2, as more home users move to high-speed broad-band Internet connections through cable modems or DSL, the potential for a devastating attack grows further. A Code Red type worm could spread to tens of millions or more home computers within hours. A denial of service attack then launched from tens of millions of infected machines could decimate the on-line business to business transactions of all Fortune 500 companies as well as all business to business and government to government electronic transactions. A large part of our economy would simply grind to a halt.

Finally, No. 3, the demographics of on-line attackers are changing. Until now, most computer worms appear to have been created by amateurs with no specific targets. However, with more business and government functions occurring on-line, we expect to see an increase in professional attacks from organized crime, corporate spies, terrorist groups, and other organizations targeting specific systems on the Internet.

Today industry research shows that the public and private sector have been reasonably successful in taking the first step in cyber defense through deployment of anti-virus software and firewalls. The same research has shown that government entitles rank among the earliest adopters of anti-virus technology and are also among the most effective at fighting computer viruses in a timely fashion.

Moving forward, it will be increasingly important for both the government and private sector to share as much information on cyber attacks as possible. Harris Miller on this panel has already spoken to you about the formulation of the ISACs, a good step in encouraging such cooperation.

Symantec is a founding board member of the IT-ISAC and I would like to commend Harris Miller for his efforts in helping to create this important organization.

Now I'd like to move to some recommendations. A good lesson learned from the private sector is the need to appropriately prioritize potential security solutions according to their cost/reward tradeoff. Deploying effective security is not an all or nothing procedure. Rather, it is an evolutionary process where each successive step further reduces risk.

We sometimes refer to an 80/20 rule for security. By applying the most important 20 percent of potential security solutions, one can likely prevent 80 percent of possible attacks. Based on our experiences, there are three top recommendations to protect against 80 percent of likely attacks.

No. 1, organizations should deploy properly configured and updated anti-virus software and firewalls. No. 2, organizations need to install appropriate updates for any announced security holes on all systems as soon as these are available. As we've seen, such actions would have disabled the Code Red worm.

And finally, No. 3, organizations should have a specific policy to ensure that computer users' passwords cannot be easily compromised. Beyond these 80/20 rules are there further general recommendations.

No. 1, organizations should consider deploying other types of security software such as vulnerability assessment or intrusion detection software at all appropriate layers of their network.

No. 2, organizations should consider instituting a policy to block all executable programs from flowing into their networks through e-mail attachments. Many corporations have successfully blocked numerous worms through just such procedures.

And finally, No. 3, industries and government agencies deemed essential to our national security, as described in PDD63, should consider using private networks for all critical communications to isolate themselves from worm-based attacks.

In conclusion, Mr. Chairman, over the coming decade, a computer worm could easily devastate our national economy. The time to invest in this problem is now. Both the government and corporations are building their next generation of on-line systems today and all of these systems will be targets tomorrow. Thank you very much.

[The prepared statement of Mr. Trilling follows:]

Testimony of Stephen Trilling

Senior Director of Advanced Concepts, Symantec Corporation

Before the

Committee on Government Reform's Subcommittee on
Government Efficiency, Financial Management and Intergovernmental Relations

Hearing on

What can be done to reduce the threats posed by computer viruses and worms to the workings of the government?

San Jose, CA
August 29, 2001

Introduction

Thank you Chairman Horn and members of the Subcommittee for providing me with the opportunity to testify before you today. Mr. Chairman, I would also like to commend you and your Subcommittee for your leadership in examining the state of cyber-security among federal agencies through previous hearings, and your release of the *Report Card on Computer Security in the Federal Government* last year.

My name is Stephen Trilling and I am here representing Symantec Corporation. Our company is a world leader in Internet security technology, providing a broad range of solutions to government, individuals, enterprises and service providers. We are a leading provider of virus protection, firewalls, vulnerability management, intrusion detection, and security services for enterprises and Internet providers around the world. In addition, Symantec is providing security solutions to numerous federal government agencies, including all four branches of the armed forces and the U.S. Postal Service. Our enterprise-level solutions span all tiers of the network, from desktop computers, to servers, to Internet gateways. Symantec's Norton brand of consumer security products leads the market in worldwide retail sales and industry awards. Headquartered in Cupertino, California, Symantec has approximately 4000 employees, worldwide operations in 37 countries, and over 100 million users.

At Symantec, I oversee our Advanced Concepts team, a research group dedicated to studying new security threats and creating new technologies to protect computers at all levels of the Internet infrastructure. Prior to this role, I oversaw our anti-virus research team, responsible for analyzing and creating fixes for computer viruses and other malicious threats. I am pleased to have the chance today to speak with you about computer worms, a growing threat to our national and economic security.

Computer Viruses and Worms

A traditional computer *virus* is a program designed to spread to many files on a single computer. However, a virus cannot spread from one computer to another without the user performing some manual action. For example, a user could inadvertently copy a virus to a floppy disk, and then transfer the virus to another computer. Or a user could unknowingly attach an infected file to an e-mail message. Again, traditional computer viruses are dependent on user action, spreading only as fast as humans exchange information, on the order of days or weeks.

Computer *worms* are malicious programs designed to spread themselves over networks to as many computers as possible. Worms spread largely without human interaction and can therefore infect new computers at an exponential rate. In some cases, worms can infect hundreds of thousands or even millions of computers in hours, without regard to borders or boundaries.

Recent Computer Worms and their Impact

While there have been some notable computer worms in the more distant past, the release of *Melissa* in March, 1999, marked a significant turning point in fast-moving malicious computer threats. *Melissa* spread itself automatically through e-mail from one computer to the next, across the Internet. Even more damaging, was the *LoveLetter* worm from May, 2000, which infected millions of e-mail messages and is estimated by Computer Economics to have cost our global economy 8.7 billion dollars[i].

Most recently, certain versions of the *Code Red* worm spread, by some estimates, to more than 350,000 computers on the Internet in less than 15 hours, without any user interaction[ii].. According to Computer Economics, *Code Red* has already had a worldwide economic impact of 2.4 billion dollars[i]. Initial versions of *Code Red,* released in July 2001 attempted to launch a denial of service attack on the whitehouse.gov Website. *Code Red* is particularly virulent because it combines two different forms of attacks, first spreading to many computers and then launching a denial of service attack.

A subsequent version of this worm, *Code Red II,* released in early August 2001, again spread to many computers across the Internet and also left behind a "back door" on each infected machine. This back door provides a new security hole in the machine, making it easy for an attacker to compromise the computer still further even after *Code Red II* has been removed and the system has been appropriately updated.

In the future, we could see computer worms moving across the Internet at even greater speeds with an even wider array of hostile capabilities.

The Dangers Ahead

Our global economy is becoming more dependent on the Internet. Computers connected to the Internet either control or will likely soon control e-commerce sites, stock market trading, power generation, transportation systems, electronic business supply chains, government transactions and numerous other operations. A properly targeted computer worm could hobble any or all of these systems, threatening our national security. This is the price we pay for all of the efficiencies that the Internet brings to our business and government systems.

The potential for such a devastating threat will only grow more likely as home users move in greater numbers to broadband Internet connections through cable modems or Digital Subscriber Lines (DSL). A *Code Red*-type worm could quickly spread, without user intervention, to 50 million or more home computers through broadband "always on" connections. Furthermore, a denial of service attack then launched from 50 million infected machines could decimate the online business-to-business transactions of all Fortune 500 companies, as well as all business-to-government and government-to-government electronic transactions. The Internet would grind to a halt, just as would traffic on a freeway if 50 million stalled cars were suddenly added to the road. In addition, the cleanup effort required to disinfect tens of millions of privately owned computers would be enormous, likely costing far more than for any previous incidents.

The demographics of online attackers are also changing. To the extent that we know of their origin, amateurs—primarily young males, ages 14-24—appear to have created most of the recent computer worms and were not targeting any special victims. Even the most damaging of these threats, such as *LoveLetter* clearly had no particular target in mind. However, with more and more business and government functions conducted online, we expect to see an increase in professional attacks from organized crime, corporate spies, social or political activists, terrorist groups, rogue states, and other organizations targeting specific systems on the Internet.

In March of this year, the National Infrastructure Protection Center (NIPC) issued a release indicating that several organized hacker groups from Eastern Europe had penetrated US e-commerce systems and stolen proprietary customer information including over one million credit cards (NIPC Advisory 01-003). Given the increasing value of information stored on the Internet, we fully expect other targeted attacks from professionals in the future.

Security in the Government and the Private Sector

There is no question that the need for improved security is as much an issue for the private sector as for the United States Government. Research from IDC on North American security trends shows that both the federal government and private sector organizations have been fairly successful in setting up a first line of cyber-defense, through deployment of anti-virus software and firewalls. Furthermore, according to IDC, government entities rank among the earliest adopters of anti-virus technology and are also among the most effective at fighting computer viruses in a timely fashion[iii]. While this initial line of defense can thwart many of today's threats, next steps should be taken if government and industry are to provide a complete security solution to protect against the targeted attacks we may face tomorrow. Should a professional attacker attempt to exploit existing vulnerabilities through a more targeted worm, the costs to American corporations could be astronomical.

Moving forward, it will be increasingly important for the government and the private sector to share as much information on cyber-attacks as possible, to protect our nation's critical infrastructures. Thanks to the support of the government through *Presidential Decision Directive 63* (PDD 63), private industry is in the process of setting up a number of Information Sharing and Analysis Centers (ISACs) that provide formal mechanisms for companies to share information on security attacks, vulnerabilities, solutions, and best practices. This information is, in turn, shared with the government in certain instances.

Symantec is a founding board member of the Information Technology or IT-ISAC. The effort to build an ISAC for the IT community has been spearheaded in large part by Harris Miller, President of the ITAA who is also testifying before you today and I would like to commend his efforts on this project. We hope that the creation of the IT-ISAC will encourage further efforts by both the government and the private sector to work together on cyber-security issues.

We provide further specific security recommendations on the following section.

Recommendations

The key to effective security is a set of well thought out and clearly communicated policies and plans that support the organization's objectives and provide guidance for employees. Successful enforcement comes through a combination of informed people, sound policies, workable procedures, management commitment and appropriate use of technology and services.

One good lesson learned from the private sector is the need to appropriately prioritize potential solutions according to their cost/reward tradeoff. By applying a few simple rules, one can prevent the vast majority of attacks. We sometimes refer to this as the 80/20 rule for security - by applying the most important 20 percent of potential security solutions inside an organization, one can likely prevent 80 percent of possible attacks. Deploying effective security is not an all or nothing procedure. Rather, it is an evolutionary process, where each successive step further reduces risk.

Based on our experiences, the top security recommendations for any organization, public or private, which will likely protect against 80 percent of attacks, are:

1. Organizations need properly configured and regularly updated anti-virus software and firewalls, as a basis for any effective security solution. To use an analogy

from physical security, this is similar to locking your door and having a guard in front of the house. According to the CSI/FBI 2001 Computer Crime and Security Survey, the penetration of both anti-virus and firewalls in the private and public sector is very high[iv].

2. Organizations need to deploy appropriate updates for any announced security holes, on all systems, as soon as they are available. Whenever a new security vulnerability in commercial software is announced publicly, the information becomes accessible not only to legitimate users of the software but also to attackers who can then take advantage of the flaw for their own malicious purposes. This was clearly demonstrated with the recent *Code Red* worm[ii].

3. Organizations should have a specific policy to ensure that computer users' passwords cannot easily be compromised. This will help ensure that none of these computers can easily be co-opted to launch a worm. This also greatly reduces the effectiveness of any worm that attempts to spread in an organization from one computer to the next by cracking user passwords. Such a policy includes making sure that users do not have easily guessed passwords, such as common words, users, names or initials, the word *password* and others. Users should be required to change passwords regularly and use passwords that are sufficiently long. The policy should include a requirement to regularly test that all passwords are adequately strong.

Further general security recommendations, again based on our experiences, are as follows:

1. Organizations should take more proactive steps to deploy vulnerability assessment and vulnerability management software. This type of monitoring can determine, for example, whether appropriate software updates for security holes have been deployed (#2 above) and whether any easily compromised passwords are being used (#3 above). As such, these software solutions can help ensure that organizations are adhering to the key elements of the 80/20 rule. This type of software can also help organizations ensure full compliance with existing security policies in advance of monitoring from outside agencies.

   According to an IDC report, government agencies as a whole tend to be slightly behind some other critical organizations such as banking, communications, financial services, healthcare, and utilities with respect to routine security auditing, and slightly ahead of transportation. However, the federal government is well ahead of most critical industry sectors in this area[iii]. While this survey does not directly address vulnerability assessment software, these results are likely indicative of the level of deployment of this type of solution across different sectors.

2. Organizations should consider blocking all executable programs flowing into the corporation through e-mail attachments. Such a policy will likely stop some

legitimate attachments from entering the organization, but will also vastly reduce the chance of a malicious worm entering via e-mail. Many private corporations are quite willing to make this tradeoff and have successfully blocked numerous worms by instituting such procedures.

3. Organizations should consider installing intrusion detection software to monitor their networks for potential attacks. This software is analogous to alarm systems and motion sensors in a home, alerting on any suspected intrusion. On a computer network, intrusion detection software can provide alerts on attacks and break-ins from numerous threats including worms such as *Code Red.*

   According to the CSI/FBI Computer Crime and Security Survey, deployment of intrusion detection systems is rapidly increasing for large corporations and government agencies, although its overall penetration is still well below that of anti-virus software or firewalls[iv]. According to IDC, the federal government is well ahead of such critical organizations as financial services, healthcare, transportation, and utilities and comparable to banking and communications with regards to deployment of intrusion detection software[iii].

4. Organizations should deploy several layers of security software at all tiers within the enterprise. The following is an example of various different technologies that could have helped stop *Code Red* from infecting a given Web site:

   - Certain firewall products could prevent initial *Code Red* infection.
   - Intrusion detection software could alert on a *Code Red* attack
   - Vulnerability assessment software could alert administrators to update their software to prevent attack
   - Anti-virus software could be used to detect the "back door" left by *Code Red II.*

   Computer worms can potentially attack large servers, desktop computers, and even handheld devices. This emphasizes the importance of having an integrated set of security solutions protecting all tiers of the network. For example, one should consider deploying firewalls not only at the network perimeter, but also on desktop machines to stop threats that have been released inside the organization.

5. Industries and government agencies that are essential to our national security (as described in *Presidential Decision Directive 63*) should consider using private networks for all critical communications. Such private networks could help isolate important transmissions from computer worms or worm-based denial of service attacks.

6. We need continued public/private sector cooperation in sharing information on security issues as well as in providing appropriate security education to both government and corporate entities. The IT-ISAC is a good current example of a cooperative sharing organization for the IT sector. Recent alerts from the public

and private sectors on the need to deploy appropriate security updates to protect against *Code Red* were a good demonstration of educational efforts in this space.

Conclusion

Over the coming decade, a computer worm could easily devastate our economy. As the threats become more dangerous and more sophisticated, we must be vigilant and take necessary steps to better protect our nation's critical infrastructure. The time to address and invest in the problem is now. Both the government and corporations are building the next generation of online systems today, and all of these systems will be targets tomorrow.

By applying the 80/20 rule, organizations can likely prevent 80 percent of potential worm attacks to their infrastructure, by addressing just the top 20 percent of good security practices. This is a very good first step. However, the growth of home broadband connections raises further concerns that a worm could spread rapidly to millions of Internet users and drastically impact the operation of our economy.

We must therefore look for comprehensive solutions to protect against future attacks on our electronic highways. Only through proactive attention to this problem across both the public and private sector, and through greater cooperation between both groups, will we be able to effectively deal with this serious threat.

Thank you.

References:

[i] www.computereconomics.com

[ii] www.caida.org

[iii] *North American Security Technology Adoption Trends: A Vertical Market Segmentation* (IDC Report #23608)

[iv] *Computer Security Issues and Trends*, VOL. VII, No.1

Further Resources

A good further source of general best practices is the list of security requirements for Visa merchants provided by Visa's *Cardholder Information Security Program*. This list is available from www.visabrc.com.

Mr. HORN. Thank you, and we will back to you on a number of questions.

Our last presenter is Marc Maiffret, the chief hacking officer of eEye Digital Security. Welcome. We're delighted to have you here.

STATEMENT OF MARC MAIFFRET, CHIEF HACKING OFFICER, eEYE DIGITAL SECURITY

Mr. MAIFFRET. Thank you. I'd like to thank you for providing me the opportunity to be here today. I hope to bring a real world perspective to some of the issues that are currently affecting the security of our computer networks. My name is Marc Maiffret and I'm the co-founder and chief hacking officer of the eEye Digital Security. I've been in the computer security field for about 6 years now. The first 3 years of my experience was mainly as a hacker and the last 3 years has been as the chief hacking officer of the eEye Digital Security.

The eEye Digital Security was started with the goal of creating software products that would help protect companies against the growing threat of cyber attack. Besides just creating software products, eEye also focuses on vulnerability research as a way to stay on top of the latest security threats. Vulnerability research is the process of analyzing software products to find ways in which an attacker can manipulate software in a malicious way.

I've personally found vulnerabilities within 30 or so different software products and eEye itself has also been responsible for the discovery and disclosure of a few of the largest software vulnerabilities ever. It is a real world experience I have in hacking, vulnerability research and worms which I hope provides you all with an insight into the problems we are currently facing in the world of computer security.

Computer systems and networks are vulnerable to many different types of attacks. The computer worm is one of the most dangerous types of attacks that threaten the Internet today, potentially more damaging than any virus. A virus can only infect systems if the computer user performs a certain action—for example, executing an e-mail attachment—whereas a worm, once planted on the Internet, is completely self-propagating. This functionality allows a worm program to infect a very large number of systems in a very short period of time. Once the worm spreading has begun, the author of the worm could have control over thousands, if not millions, of systems which can then be used to perform attacks against the Internet or specific parts of the Internet.

Code Red represents one of the best modern examples of a worm and the impact they can have on the Internet. Code Red was discovered around July 13 of this year. The first detailed technical analysis of Code Red was actually published July 17. That first detailed analysis of Code Red was done by myself and Ryan Permeh of the eEye Digital Security. Funny enough, we actually named the worm after the type of soft drink we had been drinking while performing our analysis.

For a worm to propagate, it requires a method of entry. In the case of Code Red, it was via vulnerability within Microsoft Internet Information Services Web server or IIS. The vulnerability that the worm used to compromise Microsoft IIS Web servers is a vulnerability called the dot IDA buffer overflow. The dot IDA buffer overflow was actually a vulnerability found by eEye Digital Security. Microsoft and eEye Digital Security released the security advisory a month before Code Red was found in the wild. The advisory gave administrators instructions on how to protect themselves from the dot IDA vulnerability. Therefore, if administrators had installed the Microsoft security patch, then Code Red would not have had the ability to infect any systems and spread itself across the Internet.

Code Red was designed with two goals in mind. The first goal was to infect as many IIS Web servers as possible and the second goal is to attack the White House Web server between the 20th and the 27th of every month. Code Red seems to have been very successful at its first goal while failing at its second goal. The reason it was successful for its first goal is due to the fact that many Web servers were left unpatched against the IDA vulnerability. Code Red failed at its second goal because eEye Digital Security's early analysis of Code Red provided enough information in advance to protect the White House Web server.

The aftermath of Code Red has shown us the devastating effect that worms can have on the Internet. Although the worm only reached one of its two goals, the effects of the first goal had numerous implications. The rapid spreading of Code Red created abnormally high amounts of network traffic causing some networks to go off-line. Certain routers and other network devices experienced crashes unforeseen before Code Red.

Five hundred thousand systems were comprised at the highest level of access and they were broadcasting that fact to the Internet at large. Although preventative measures stopped the second goal of the worm from being achieved, had it occurred, it would have been the largest distributed denial of service attack the Internet has seen today. Code Red has served as a warning shot to grab the attention of the Internet community.

The biggest problem facing security today is that there are too many people talking about what we could do or what the threat is and not enough people doing real work that will result in a mitigating or abolishment of those threats. The Code Red worm was in some ways one of the best things to happen to computer security in a long time. It was a much needed wakeup call for software vendors and network administrators alike. Code Red could have caused much more damage than it did and, if the authors of Code Red had really wanted to attempt to take down the Internet, they could most likely have easily done so.

What made all of this possible and what steps can we take to help prevent things like this in the future? These are the most important questions and, luckily, there is much we can learn from Code Red to improve our current security standing. One of the first areas that needs improvement is the way that software vendors test their code for stability and security. I'm a software engineer so I know that mistakes do happen and programmers will now and then accidentally write vulnerable code. Software vendors, however, are usually not very motivated to take security seriously.

Software vendors are not the only ones at fault here though. Network administrators and managers at various corporations are also to blame for faulty security. Going back to Code Red as our example, we can see that really the largest reason for Code Red's spreading as it did was because a lot of network administrators did not install the Microsoft security patch.

It should also be noted that many companies have a very small budget for an IT staff or do not even have an IT staff. This leads to a lot of problems for administrators when it comes to securing a company's network.

To help get security messages out to the public, there needs to be a centralized organization for vulnerability alerting. There are a few cyber watch organizations, NIPC, SANS, CERT, that currently watch for large scale attacks, i.e., worms, larger vulnerabilities and viruses. However, I feel these organizations would be able to accomplish a lot more if they sent alerts about all vulnerabilities instead of only vulnerabilities deemed serious enough to cover. There should be a Web site or e-mail alert system that administrators could join that would allow them to find out about all vulnerabilities and patches.

Something that was said earlier I thought was pretty interesting from the gentleman from SRI. The reality of the situation right now is that there's a few aspects to security. One of the main things is, of course, vulnerabilities. Really, the type of vulnerabilities that are out there, there's I'd say five to six different classes of vulnerabilities out there. Things like buffer overflows, etc. These classes of vulnerabilities have actually been around, some of them, for 20 years, 15 years. For example, the class of vulnerability that Code Red was exploiting was a buffer overflow vulnerability. The Robert Morris worm itself was exploiting that type of vulnerability.

So I think one thing is that the research has been done about buffer overflows and all these things and a lot of people have given the same speeches about doing more and all this sort of stuff but really, to me, when I got into the security field, I was kind of amazed that still, 15 years later after things like buffer overflows have been covered, that something like that is still actually a problem today. Really, it comes down to software vendors and also IT administrators, etc., but stopping worms, stopping viruses, stopping a lot of the vulnerabilities out there, it is not as hard of a thing to do as some people might say it is. These are vulnerabilities that have been around for a long-time and there's tons of information on them and there definitely is a lot that we could be doing to make sure that software products do not have these types of vulnerabilities. That's all.

[The prepared statement of Mr. Maiffret follows:]

Marc Maiffret
Chief Hacking Officer
eEye Digital Security
One Columbia
Aliso Viejo, CA 92656
Toll Free: 866.339.3732
Tel: 949.349.9062
Fax: 949.349.9538

I would like to thank you for giving me the chance to write this testimony and to share with you some of the knowledge I have gained over the past few years as both a hacker and a security professional.

My first three years in the field of computer security where spent as a hacker. That part of my life allowed me to gain insight into the types of security threats we face, as well as an understanding of what can be done to defend against those threats.

One day, when I was 17, I had a "wake up call" of sorts that motivated me to turn my life around and to put my knowledge towards something that would help people in their quest for security. That something is now what is known as eEye Digital Security.

eEye Digital Security was started a little over 3 years ago by Firas Bushnaq and myself. We formed eEye with the intention of creating software products that would help protect companies against the growing threat of cyber attacks.

In addition to building software, one of the ways that we are able to help keep systems secure is through vulnerability research. Vulnerability research is the process of looking for ways that someone could potentially manipulate a software product or hardware device, in order to gain access to a system or network.

Since its inception, eEye has researched and published some of the largest software vulnerabilities to date. In fact, within the last 3 months alone, eEye has discovered 3 vulnerabilities within software products that are installed on more than 8 million servers around the world. When eEye finds a vulnerability, we work closely with the software manufacture (vendor) in order to help them create a "patch" which is then installed by computer administrators in order to protect their systems from the newly discovered vulnerability.

In May of this year (2001), eEye discovered a vulnerability within Microsoft's Internet Information Services Web Server software. Microsoft IIS is a software product that is installed on roughly 6 million Web servers around the world. The vulnerability allowed an attacker to gain complete control of a Microsoft IIS Web Server within a matter of a few seconds from anywhere in the world. When we discovered the vulnerability (which we termed the .ida buffer overflow) we followed the same process of contacting the software vendor and working with them to have a patch released. eEye and Microsoft worked together to make sure that system administrators were aware of this serious vulnerability and protected themselves accordingly.

In a perfect world, every system administrator would have installed the security patch and all 6 million systems would have been protected from this vulnerability; however, computer security is not perfect, and the consequences resulting from systems remaining unpatched were far worse than anyone expected.

The Creation and Release of the CodeRed Worm.

The CodeRed worm has become a great example of just how fragile the Internet really is. I believe that the CodeRed worm contains many key elements to make for a serious discussion on the current types of threats the Internet and the United States are facing on the digital frontier.

A computer worm is one of the most dangerous types of attacks that threaten the Internet today, often more dangerous than any virus. A virus can only infect new systems if a computer user performs a certain action (e.g.. executing an email attachment) whereas a worm, once planted on the Internet, is completely self-propagating. This ability allows a worm program to infect a very large amount of systems in a very short period of time. Once the spreading has begun, the author of the worm can conceivably have control over thousands if not millions of systems, which can then be used to perform attacks against the Internet or specific parts of the Internet.

As I said earlier the best real world example of all of this is the CodeRed worm.

On Friday, July 13th,eEye Digital Security was contacted by a network administrator that was experiencing a stream of .ida buffer overflow attacks being sent against his computer network. At first the administrator felt that it was simply a few hackers on the Internet attempting to break into his network. Later that day one of his websites' pages was replaced with a message that said "Hacked by Chinese. Welcome to http://www.worm.com". That Web server then proceeded to attempt to connect to other Web servers on the Internet. All of this information was made available to the network administrator because he was running a network intrusion detection system, which was able to detect the .ida, attacks. At this point, when his server started trying to connect to other Web servers, the administrator began to think that someone had possibly written a worm program for the .ida vulnerability. Since eEye Digital Security was the company that discovered the .ida vulnerability, the administrator turned to us for help. On Friday July 13th,he sent us an email containing the details of what he was experiencing. We worked most of Friday evening to try and decipher what was happening, but without the actual code of the worm the work was difficult. On Sunday July 16th a second network administrator, who had been in contact with the first administrator, was able to give us the complete binary capture (attack code) of the worm that was also attacking his network. We then worked through Monday and early Tuesday until we released our initial worm analysis on the morning of Tuesday, July 17th. The initial analysis was sent to various security mailing lists and also to government cyber watch agencies such as NIPC. We named the worm "CodeRed" after the type of soda that Ryan Permeh (the other researcher at eEye that dissected CodeRed) and I were drinking during the late-night hours of work on the worm.

Over the next few days we worked closely with NIPC to explain to them how CodeRed worked and to make sure they had all of the information that they needed to release an alert.

On Wednesday, July 18th, 2001 we released our second and more detailed analysis of the CodeRed worm. In this analysis we outlined that between the 20th and 27th (UTC) of the month, the CodeRed worm was going to stop trying to infect new Web servers and instead start attacking by means of flooding the www.whitehouse.gov Web server with very large amounts of data (much like the yahoo.com DDoS attacks). We then pointed out that on the 28th the worm was suppose to go to "sleep" and never try to infect a new server again. At this point the CodeRed worm had infected nearly 400 thousand systems. That meant that 400 thousand Web servers around the world would be sending terabytes of data through the Internet towards the White House's Web server.

We talked with NIPC between July 18th and July 19th to help them further understand CodeRed and the impact it was going to be having on the White House Web server and the Internet as a whole. Time short since it was the 19th and only a matter of a few hours before infected CodeRed servers were going to stop trying to infect new machines and start attacking the White House Web server.

We received a phone call on July 19th from Erkan Chase of the FBI, whom Vince Rowe (our contact at the time to NIPC), had introduced us too. Erkan Chase asked if I and Ryan Permeh would be able to send his superior an email within 10 minutes that would detail what effect CodeRed would have on the White House's Web server and the Internet itself and what they could do, if anything, to keep the worst from happening.

In our email we outlined that the minor effect of CodeRed would be the White House's Web server going offline. The more significant effect would be that the Internet itself, in some parts of the world, could actually stop working or slow to a crawl because so many hundreds of thousands of systems were going to be pushing large amounts of data through the Internet pipes. We then outlined that the best course of action would be to take the White House's Web server offline because if none of the worms could connect to the server then they wouldn't be able to send the floods of data.

NIPC released their CodeRed worm alert on Thursday July 19, 2001. The conversation with Erkan Chase was probably one of the last communications we had with NIPC for reasons unknown to us.

A few hours later the original IP address of www.whitehouse.gov was "black holed", the website was moved to a new address, and the thousands of infected servers were unable to connect to the old address thus preventing the flood of data from being sent. In the end the Internet was still standing and the aftermath of CodeRed was solely that half of a million Web servers were still infected by the worm.

Between July 20th and July 28th there was not much CodeRed activity, nor were there many organizations actively warning people of what was yet to come.

As stated earlier, the CodeRed worm was written to basically go to sleep on the 28th (UTC) of the month. In a perfect world, CodeRed should have completely died on the 28th and we should have never heard about it again. However, since our original analysis we at eEye had warned that all it would take for the spreading to continue would be one infected system with its internal clock set incorrectly. On such a system the worm would have never gone to "sleep" and on August 1st would start infecting new systems, essentially starting the CodeRed worm all over again.

In a last minute effort, Microsoft, NIPC, FedCIRC, ITAA, CERT, SANS, ISS, ISA got together and released a press release on July 29, 2001 stating that CodeRed was going to return and emphasizing that all vulnerable systems needed to be patched. A large press conference was held and eEye Digital Security, despite significant involvement at the beginning, was not included or recognized.

On Saturday August 4th, 2001 eEye Digital Security was contacted by security firm SecurityFocus.com because they had knowledge of a new worm that had been released. Within the binary data of this new worm was the word "CodeRedII", so it was obviously written after the discovery of the original worm on July 13th. We analyzed this new worm and found that it was much smarter than the original CodeRed. Its method of propagation was done in a way in which it would infect servers at a much faster rate than the first CodeRed. This new CodeRedII worm also installed a backdoor/trojan on infected web servers. This backdoor/trojan program would allow an attacker to be able to remotely break into any server infected with CodeRedII even after an administrator installed the security patch. The speed at which this new version of CodeRed could infect systems and the malicious backdoor that it placed on the systems seemed to indicate that this new worm was written by someone more technically cunning than the original CodeRed worm author.

In the end when the dust the Internet was still standing. There were, however, a total of about half of a million Web servers that were compromised by CodeRed and CodeRedII. Also a few smaller computer networks were disabled intermittently due to the influx of network traffic caused by CodeRed and its variants.

The CodeRed worm was in some ways one of the best things to happen to computer security in a long time. It was a much needed wake-up-call for software vendors and network administrators alike.

CodeRed could have caused much more damage than it did, and if the authors of CodeRed had really wanted to attempt to take down the Internet then they could most likely have easily done so.

Below are a few reasons how CodeRed could have been more devastating.

1. Before CodeRed was released there was information spread throughout the Internet underground which exposed ways in which a worm, like CodeRed, could actually spread itself across the Internet without *any* Intrusion Detection System being able to detect it. This possibility existed because of a design flaw in most IDS systems. If an attacker would have written CodeRed in a way that it exploited this design flaw then CodeRed would have had much more time to spread before being detected, resulting in many more compromised machines under the worm's control that could be used to bring down the Internet.
2. CodeRed and CodeRedII were only able to infect Microsoft Windows 2000 Web servers, which only make up part of the 6 million IIS Web servers on the Internet. The second part of that 6 million servers figure is made up of Microsoft Windows NT 4.0 Web servers. If the attackers wrote the worm to infect Windows NT 4.0 systems then the worm would most likely have at least doubled the number of servers that it was able to infect, bring the number closer to 1 million.
3. The payload of the worm (the code left on a compromised machine) could have been much more devastating. Instead of simply attacking the White House's Web server, the worm could have done something such as a true DDoS (Distributed Denial of Service) attack against various websites or Internet

> backbones. Unlike most DDoS's that have taken place before, this worm could have had close to a million servers at its disposal instead of just a handful.

The scenarios are endless, but the point is that CodeRed was actually not as nearly devastating as it could have been.

What made all of this possible? What steps can be taken to help prevent things like this in the future? These are the most important questions, and luckily there is much we can learn from CodeRed to improve our current security standing.

There were two things that made the CodeRed worm possible: the vulnerability within the Microsoft Internet Information Web Server software and the fact that not nearly enough administrators installed the Microsoft supplied security patch. If the vulnerability had not existed within the software, or if administrators had installed the patch, then CodeRed would have never existed.

One of the first areas that needs improvement is the way that software vendors test their code for stability and security. I am a software engineer; so I know that mistakes do happen and programmers will now and then accidentally write vulnerable code. Software vendors, however, are usually not very motivated to take security seriously.

Most software vendors will take security just seriously enough in order to curb bad PR or news stories about vulnerabilities within their products. When a vulnerability is found within a software product used on millions of servers, then the press will typically write articles to expose the information to a larger audience. Software vendors should not wait until they have been publicly embarrassed in order to take security more seriously. Anything that a software vendor does to make their software more secure, after a PR fiasco, is something that they should have been done before the fact.

Also a lot of times security is the last thing discussed when companies map out a product development cycle. Typically, a company will put more focus on making their products perform better and have more features than how secure they will be in the end. Therefore security is usually made to try to fit around the current architecture of products. Security needs to be of the greatest importance when designing software to be run on thousands of servers. Software products must be made so that security is designed first and then everything else (features/functionality) is made to fit around the security architecture. This is typically a problem for most software development firms because in most product markets there is a race to get new features to market before the competitors do. Usually the race to get those new features out results in new vulnerabilities to exploit.

Software vendors should also be taking a better approach at notifying customers of vulnerabilities and patch releases. Software products should discontinue to run if a critical security patch is missing, and every software vendor should have an email alert system that clients can subscribe to in order to receive email notification anytime a new patch is released.

When it comes to installing patches, many administrators are actually sometimes more afraid of the security patch than of the vulnerability itself. The reason being that some software vendors have had bad track records in releasing security patches, and in fact a lot of vendors have had to re-release security patches numerous times because the original security patch did not function correctly and in some cases broke a system component that had nothing to do with the component that the patch was suppose to be fixing. It is for this reason, because patches can sometimes lead to system instability, that administrators have grown hesitant to install security patches, and sometimes will wait as many as two weeks in order to make sure the patch is safe to install.

Software vendors are not the only ones at fault here though. Network administrators and managers at various corporations are also to blame for faulty security. Going back to CodeRed as our example, we can see that really the largest reason for CodeRed spreading as it did was because a lot of network administrators did not install the Microsoft security patch. Microsoft has an email notification system that will notify administrators anytime Microsoft releases a new security patch. Last time I checked there were roughly two hundred thousand people subscribed to Microsoft's security mailing list. It is completely obvious that that is a *very* small number of people compared to the number of administrators who run Microsoft software within their networks. As an example, there are roughly 6 million Microsoft IIS Web servers on the Internet. Only two hundred thousand administrators being subscribed to Microsoft's security mailing list is unacceptable. Administrators need to be proactive in finding ways to stay up to date with the latest security patch releases of software. Software vendors also need to be more proactive in doing everything possible to let users know what they can do to stay up to date with the latest security patches.

It should also be noted that many companies have a very small budget for an IT staff, or do not even have an IT staff. This leads to a lot of problems for administrators when it comes to securing a companies network. Many administrators are already over-worked with their day-to-day tasks without having to worry about security. Companies need to make sure they have the staff needed in order to maintain the security of their network. Companies must also do their best to provide their IT staff with the budgets they need to be able to maintain the tools that will help them keep their network secure. Also, corporate managers need to understand that security must be taken seriously. For example, administrators are usually caught in the dilemma of not being able to install the newly released security patch, which requires their Web server to go offline for a few minutes, for fear they may get in trouble with management for having server downtime.

To help get security messages out to the public, there needs to be a centralized organization for vulnerability alerting. There are a few cyber watch organizations (NIPC, SANS, CERT) that currently watch for large scale attacks (i.e. worms, larger vulnerabilities, viruses) however I feel these organizations would be able to accomplish a lot more if they sent alerts about all vulnerabilities instead of only vulnerabilities deemed "serious enough" to cover. There should be a website or email alert system that administrators could join that would allow them to find out about all vulnerabilities and patches.

In my opinion, a government run organization, like NIPC, has the best chance of succeeding because it will not have the financial motivations of a corporate entity. Whether it is through the release of security auditing tools for issues such as CodeRed, or initiating a system of notification about all vulnerabilities, these are just a couple of small things that would make an organization very useful to the average administrator trying to keep his systems secure.

Also an organization, such as NIPC, could perform real-world technical research on a regular basis. One example of how such an organization could discover and alert about worms almost as soon as they are released is if they setup a large scale "honeypot." A honeypot is a term that security professionals use to describe a dummy network that has been setup to typically trap and study hackers. If an organization were to own a large enough block of IP addresses (computer internet addresses) from various Internet providers from around the world, then they could build and maintain specifically designed honeypots that are able to detect new worms/viruses almost as soon as they are released, or at least much faster than they are detecting them right currently.

I referenced the CodeRed worm heavily in this document because I feel by analyzing it closely we can learn a lot about what went wrong and what we can do to in the future to prevent things like CodeRed from taking a major toll on security and the Internet.

In conclusion, the biggest problem facing security today is that there are to many people talking about what we could do or what the threat is, and not enough people doing real work that will result in the mitigating or abolishment of those threats.

References:
Initial CodeRed Analysis –
http://www.eeye.com/html/Research/Advisories/AL20010717.html
CodeRedII Analysis -
http://www.eeye.com/html/Research/Advisories/AL20010804.html

Mr. HORN. Thank you very much. Let me ask you a question and we'll start going this way. You heard the testimony of Mr. Castro of the National Security Agency and the ease with which hackers can learn their trade. Do you agree?

Mr. MAIFFRET. Yes. Definitely. To write something like Code Red would take probably an hour or two. It's a very trivial thing to do. To launch something like Code Red to the Internet in a way where you're not going to be tracked, you're not going to be detected, is very simple to do. Even sometimes finding the vulnerabilities of these worms exploiting stuff is also actually rather trivial. Some of the most talented people out there happen to be on the side of the hackers and what not. Really, the thing is it's like that sort of knowledge, as the gentleman from SRI was saying, has not really been transferred into a lot of the corporate companies that are actually developing these products and what not. A lot of them have started to do some very good things recently. Microsoft would be a perfect example that's made a lot of improvements lately. However, the majority of software vendors out there still, it's a race for do I have the same features as this other software company.

Really, one of the things, security is not going to necessarily change until enough administrators are actually demanding for better security and that's what the market is actually asking for rather than new features being released.

Mr. HORN. What are the disincentives that you can think of that governments might have to stem the hacker behavior, or do you think it's a problem?

Mr. MAIFFRET. There's a lot of talk about having laws that are a little bit more scary or whatnot but coming from the hacker past and stuff, really when you're in that like mindset and when you are that teenager breaking into systems and whatnot, even though you read something in the newspapers about Kevin McNeff being in jail for 5 years and this sort of thing—which is definitely serious—you usually think you're above that and you're not going to get caught, etc. So laws, I don't really think, are necessarily going to scare people into not doing it and whatnot. I mean it really comes down to stopping the vulnerability in the first place.

And actually, it's not an easy task to get vendors and whatnot to actually start looking at security first and then designing the product around security. It's usually design the product and then design the security around it, which is not necessarily the best thing to do.

Mr. HORN. Let me try an analogy out on you and see if it makes any sense in the electronics of software, hardware, so forth. A lot of people look for marks on pistols and the bullet goes out and you've got usually, as the FBI knows, you can find and relate what happened on that barrel as the projectile went. The other one is the use of gun powder in terms of shot guns and people are talking about well, gee, why can't we have in that one on the shot gun in particular, you can put in types of things that have a pattern that no other shot gun shell does that. So is there any way that something like that can be in the electronics and all of the ones that are into software and maybe even hardware?

Mr. MAIFFRET. I guess the question is basically kind of like the attackers and the hackers, whatever you want to label them, performing the attacks if there's something that can be kind of resident or left to be able to help track them. Would that be correct?

Mr. HORN. Could be.

Mr. MAIFFRET. Basically, dealing with software and whatnot, it's not really an easy thing to put anything in there like that. I mean people have tried to put in kind of bug type devices or things. Different software products have like unique identifiers for each computer which has actually led to the capture of a couple of different e-mail virus authors. However, all of those things, if you're smart enough, it really just is software and it's bytes of information and that is all easily manipulable. So it's not necessarily where you're going to track a hacker that way.

There are a lot of things that could be done as far as on the network layer with things like intrusion detection systems and actually being able to detect an attack coming over the network and you'll at least have some sort of starting point of where they came from. Even intrusion detection systems, which is one of the more popular ways of creating logs to track attackers, even IDS systems themselves are vulnerable to attacks. Either yesterday or sometime today eEye Digital Security is releasing another security advisory on which we basically illustrate a technical way where you could bypass any commercial intrusion detection system to be able to attack IS Web servers.

What that means is that if somebody would have had that knowledge—in fact, somebody did have that knowledge at the time of Code Red—they could have used that knowledge to basically change around the Code Red attack in a way where intrusion detection systems would not have actually detected it, which is what led to the early analyses and the information getting out. So it could have potentially given Code Red and things of that nature another week head start on attacking the systems and what not.

One of the things I was covering in my written testimony is I think that there's a lot that could be done as far as trying to detect some of these worms earlier in the process, to be able to get the word out and having a sort of system. They call it a honey pot in the security field. But you basically have a set of dummy servers that look vulnerable and whatnot and they're really watching. Typically they're used to monitor attackers and how they work. However, you could adapt something like that for worms and, if you did own a large enough block of IP addresses or computer network addresses, you could actually detect a worm and be able to get the analysis out much earlier than we have been right now.

Mr. HORN. Mr. Trilling, you want to comment on that dialog?

Mr. TRILLING. Yes, with regard to tracing back?

Mr. HORN. Right.

Mr. TRILLING. Certainly a lot of these threats, e-mail threats and so on and Code Red, as they move through the Internet, they do leave traces, whether it's in logs or whether it's in the actual e-mail. Sometimes they use the analogy as a letter goes from one city to the next, each post office will put a local stamp on that envelope and eventually, if you want to trace back through all the stamps, you can find the origin. But the extent to which you're likely to be successful at that is very much related to how much effort you want to take and, as has been mentioned earlier, there are over

50,000 known computer viruses and worms right now. It's not likely to be practical for law enforcement officials to be able to trace back to the origin of all of them.

So certainly, as we've seen with Melissa, as we saw with LoveLetter, it is possible and certainly when effort is placed, when there's a high-profile attack that does a lot of damage, it's absolutely possible to trace back to the origin, but it's time consuming, it requires money and resources and proper prioritization.

Mr. HORN. Mr. Culp, how about it? What's your feeling for Microsoft?

Mr. CULP. Well, trying to make changes in the software that's going to run on a hacker's machine to identify the hacker is ultimately going to be futile. The hacker owns that machine and, as Mr. Maiffret put it, it's just software. If a vendor installs tracking software into the operating system, a person who installs it on their machine and has administrative control can simply take it off. They can patch it with something that nulls out the functionality.

Just the same, what Mr. Trilling was saying about improved forensics as the information transits the network is a much more interesting idea. The flip side though is that there could potentially be privacy concerns. But the real issue here is not so much the technology as much as human behavior.

I want to sketch a scenario for your consideration. Suppose we lived in a world where I could come home today and find out that on my way out to work this morning I accidentally left my back door unlocked and when I came into the house, I found all my furniture gone with a sign that said, "I've taken all your furniture in order to teach you about the importance of locking your doors." Now, suppose that I knew who did it and the general opinion of society was, well, he's done you a favor. He's shown you how insecure your home was. Does anybody believe that our homes would be secure?

The reason that we don't tolerate this kind of behavior in our physical lives is because we know what it would lead to. Cyber crime is crime. There's nothing new about it. It's the same old type of crime we've had for generations. It's breaking and entering. It's robbery. It's burglary. It's destruction of property. We focus on the cyber part of cyber crime and we lose track of the fact that this is just crime. What keeps us safe in our insecure physical world is the deterrent value of law enforcement. To a certain extent, that's missing in cyberspace and that's one reason why we have the problems that we do. Adding tracking information is fine, but it presupposes that there's going to be effective law enforcement.

Mr. HORN. Mr. Neumann.

Mr. NEUMANN. Thank you. There's a huge confusion between leaving your front door open and leaving your computer system accessible from anywhere in the world. Recently, Abby Rueben, who works at AT&T Labs, one of the old Bell Lab spin-offs, was sitting in the Morristown Memorial Hospital and all of a sudden the green light on his laptop goes off and he discovers that he's instantaneously connected to the wireless network of the hospital with no security, no authentication, no protection whatsoever.

As I mentioned earlier, we had this case in Oklahoma where a guy let his newspaper know that their Web site was open and he's now up for 5 year felony charge. Abby did not do anything within the Morristown Memorial Hospital, but he noted this and I published it in my risk forum and I fear that all of a sudden people are going to be going after him because he has exceeded authority.

In the Robert Morris case, Morris was accused by the Federal prosecutor of exceeding authority. In the four mechanisms that he used in the Internet world, not a single one of them required any authority. There was no authentication required, there was no access control required. The startling thing about this is the law that we're dealing with says you must exceed authority. If there's no authority required, then somebody who happens to access your system from afar is obviously intending to break into your system. But the law as it is written does not say that he's doing anything wrong if he's being accused of exceeding authority and there's no authority required.

One of the most fundamental problems we have is that fixed passwords are being used. Fixed passwords are flying around the Internet unencrypted. They're trivial to sniff. There's lots of software you can get that will enable you to pick off essentially any Internet traffic.

The fact that somebody breaks into your system should be a violation of the law and yet, as the law says, if he's exceeding authority, there's something fishy here. So I think we have to be a little bit careful if the laws are not saying what they're supposed to be saying. If there is no authentication and there exists zombie machines all over the place that people can jump into and use as springboards for attacks with no trace back possible because they've broken in masquerading as someone else and you have no idea who they are or where they're coming from because of the way they come in, there's something fundamentally wrong here.

I mentioned the idea of malicious code. You have to realize that the malicious code, once it's in your system, is executing as if it were you. So the challenge is to keep it from getting in there in the first place. The laws do not help in that respect. So yes, we need better laws, I think, but we also need better systems.

I will just mention the Advanced Research Project Agency of the DOD which has at the moment a set of 10 contracts—I happen to be lucky enough to have one of them—on what's called composable high assurance trustworthy system. This is an effort to radically improve the security/availability/ reliability of the computer operating systems that we deal with, and I'm hoping that research will inspire some of our computer vendors and developers to use some of the better techniques to come out of that research program.

But again, I say I don't have much hope because I've seen the research that we did back in 1965 which is widely ignored. Thank you.

Mr. HORN. Harris Miller, president, Information Technology Association of America. How do you look on this?

Mr. MILLER. I think the idea of the unique identifier, I would agree with what Mr. Culp said. The problem with the technology is that technology can be over-ridden, No. 1. No. 2, the privacy advocates would go absolutely ballistic. They've gone crazy when they've accused companies like Intel and others of trying to plant identifiers in their computers, even though Intel is doing it purely to protect the consumer. The consumer privacy advocates say that this is an attempt to install big brother. So I think the negative reaction sociologically, in addition to the technological obstacle that Mr. Culp outlined, really don't make that a very good alternative solution.

I would like to comment on two other things that you addressed earlier though, Mr. Chairman. One is about the behavior of cyber citizens. We're not foolish enough to believe that simply saying be good will solve all of our cyber problems. However, we're sort of at the other extreme right now where we don't teach young people at all about good cyber ethics.

In fact, there is still a tendency to revere hackers as if somehow this is a positive element of our society. It's good to be able to say I brought down the Defense Department Web site or, even worse, Johnny and Susie's parents say, isn't Johnny or Susie clever? They brought down the Defense Department Web site as if it's a mark of admiration. They wouldn't be proud if Johnny or Susie burned down the Pentagon or burned down an office building, but somehow they're proud if they can figure out a way to show that they're technologically more sophisticated than the people who developed the software.

That's why ITAA has worked with the Department of Justice and now Department of Defense on our cyber citizen program. We think that there needs to be education built into the classrooms all the way K–12 and higher education and even beyond to teach people good cyber ethics. Again, it's not going to solve all the problems but the previous panel mentioned that 24,000 attacks occurred on DOD last year. DOD will tell you that a huge percentage of those, 80, 90, 95 percent, is what they call script kitties. People just fooling around because they think it's cute or clever. Doesn't mean most of those attacks succeed but it does mean that it's harder for DOD as the object of attack to identify the serious problem because there's so much chaff coming at them in the form of people playing games. So I think that we do need to focus more on cyber education.

The last point I'd like to make is I enjoy Doctor Neumann. He's obviously a lot smarter than all of us, but he does somehow take statements and run a little bit to the extreme. For example, he says that the Y2K legislation totally protected software vendors. As you know as one of the authors of the legislation, that was not the objective. The objective was to try to make the point that if a remediation could be found, that should be the first choice before you run off to the courts. That was a system that worked reasonably well.

I would just disagree candidly with Doctor Neumann's assessment that the market place does not provide incentives for cyber security. I think the market place provides tremendous incentive to cyber security but, just as with automobiles, people want it both ways. They want to be able to do speedy business, but they want to be able to do secure business. So the challenge for industry is to balance those two interests off. We could all drive HumVees and armored personnel carriers down the road and probably wouldn't have 42,000 Americans die on American highways. But we'd go a lot slower, they'd be a lot more expensive to run, they'd ruin the highways. We'd have to replace them a lot more often. So we try to come up with a balance: cars that are safe but also are fairly inexpensive and can move quickly.

That's the challenge for the IT world. Companies, customers, individual consumers, both domestically and globally, want new products. They want products that work quickly. They want to be able to get their e-mail instantly if not faster. They want to have wireless access but at the same time they want security. So the challenge for all of us, both as producers of these products and as consumers, is to reach that balance. I think that clearly the good news is there's a lot more focus on cyber security. Mr. Maiffret said quite correctly the Code Red virus was a wakeup call. An even bigger wakeup call was the February 2000 distributed denial of service attacks which led to the creation of the IT-ISAC. So these incidents are good in a way. Fortunately, there's never been what Dick Clark and others have referred to as an electronic Pearl Harbor where it really has destroyed the Internet it's been so bad. But I think there have been enough serious incidents that people are paying more attention. I think we are making progress.

Mr. HORN. When a symptom of being a virus or a worm or whatever you want to call it, is there a way to sort of think about that software side? Can you get all this bombardment away into another part within a computer and that would then divert the group that's making the attack?

Mr. MILLER. I'll defer more to the experts. Again, I don't think it's possible to say that somehow you know intrinsically that these are good guys and bad guys. What technology has tried to do is separate that as much as possible. Mr. Maiffret mentioned the idea of this honey pot concept where you create a lot of IP addresses that are basically out there just to lure bad guys hoping that because security experts or government officials are watching those IP addresses, they would catch earlier warnings of these problems before they become widely diffused through the real government and the real private sector. But I don't know that there's any way of saying at the end of the day we're going to know every bad guy that walks into the bank any more than we're going to know every bad piece of code that comes in. I don't think there's any way of saying that in advance.

Clearly, the tradeoff—and I think I discussed this before another hearing you had, one of your colleagues said, well, can I get to a situation where I never get an e-mail virus on my computer? I said to the Member of Congress, you could. You'd have someone else get all your e-mail and let him or her be the guinea pig, in a sense, and he or she would screen it. But, of course, you're giving up your privacy because that means someone else gets all your e-mail. You're giving up the time sensitivity because someone else would have to filter it and make sure it was all done. So that's a tradeoff. You could say, OK, I as an individual don't want to get any viruses but what kind of tradeoffs am I going to make then?

Mr. HORN. Let me just ask a few closing questions here. Mr. Maiffret, you've been criticized for giving a blueprint of the exploit to malicious programmers. Could you tell us how you believe this is an important way to provide details of threats to the on-line community?

Mr. MAIFFRET. Yes. The first thing would be the wording on that would be it's not necessarily a blueprint. The main criticism came with Code Red and people said that we gave out enough details where somebody took our details and then actually wrote Code Red from those details.

In the case of Code Red, the actual techniques that they used were far superior to anything that we talked about. In every advisory on software that we do, we always give out enough details where a vulnerability scanning type tool or an intrusion detection system or administrators themselves will have enough technical information where they can either test the vulnerability to make sure that the patch is working themselves or that they can actually update their intrusion detection systems to be able to monitor for potential people trying to exploit the vulnerability.

It is a double-edged sword because yes, there is the information that's there and somebody could take that and try to write an exploit program with it, as they call it. However, the thing people need to understand is that even without any information at all, it's actually rather trivial to actually figure out where the vulnerability lies and exploit it. This has happened in the past before. One example of that would be Code Red itself was actually based off of another worm that was released back in April of this year and the vulnerability that worm exploited, there was actually no technical details ever released on it.

So what happened from that was that some hackers did figure out the technical details, did write an exploit for it, did write a worm for it. However, since there was no public technical details released about it, no security software tools or anything out there were actually updated to be able to look for that specific signature. So back in April when Code Red was actually first attempting to go around the Internet, since there was no details, nobody was actually able to detect that it was going on. There just happened to be a couple of administrators at Sandia Labs that were lucky enough to see it.

Mr. HORN. Recently the editorial editor of the Washington Post, Meg Greenfield, had her computer and people wondered what her password was and so when they found out, she simply said password, and I began to think that's so obvious, maybe people would leave her alone. No one would obviously think password for the password.

Mr. MAIFFRET. One of the most common.

Mr. HORN. That's right. Well, since some of you have teaching backgrounds, I guess I'd be interested in the fact that even Microsoft who warned the users of the newly discovered vulnerability and issued the patch to protect against the exploit did not protect all of its own systems, illustrative of the day-to-day challenge that system administrators face in maintaining the security of their systems. Any thinking on that?

Mr. MAIFFRET. Sure. Let's walk back through. As you noted, when the initial patch was released, we did extensive publicity. Let me run through a couple of things that we did. As always, we released a security bulletin on our Web site. It's one of those heavily traveled Web sites on the Internet. We mailed it to over 200,000 subscribers to our mailing list.

We also took the unusual step, because of the severity of the vulnerability, of engaging our worldwide support organization, particularly several thousand employees known as technical account managers who have direct relationships with customers and we asked them, call your customer and tell them you need to put this patch on now, read the bulletin later.

We also proactively contacted the media and asked for help in getting information out. This was without a doubt the most widely publicized security bulletin in history. It's in keeping with how we have traditionally handled security vulnerabilities. Our goal at the end of the day is to get as many patches on machines that need them and, if the way to do that is to air the fact that we've made a mistake worldwide, we're going to do that.

But as you mentioned, we neglected to fully protect our own networks. We did have a few machines, scattered machines here and there, that didn't get patched and this is illustrative of a problem that's inherent in a patch-based protection scheme. Applying patches is a management burden. Takes time. Certainly takes less time to apply a patch than it does to rebuild a machine after the machine has been compromised, but just the same, there's a management burden associated with this. We've invested quite a bit of time and effort, even starting before the worm, into trying to make our patches as simple as possible to get onto the machines that need them.

Let me give you a couple of examples. Starting in May, we inaugurated a practice in which every IIS patch, patches not only whatever the vulnerability is we're discussing here now, but includes every previous patch for IIS. So if you just apply the most recent patch, you're protected against everything. No other vendor in the industry does that.

We've also taken some steps to do some technology development to make it easier to get the patches onto the machines. Specifically, not requiring the machines to reboot. It turned out when we talked with our customers we found that was a significant impediment to a lot of them. So we did some technology development. We rolled out no reboot patches. And just recently we've rolled out some tools that have been in the works that have been under development since earlier this year that we believe will help ensure that customers have fully patched machines.

The first one is something called the Microsoft Personal Security Advisor. It's a Web site. You navigate to the Web site and it downloads some software to your machine that allows it to scan itself with reference to a data base that we keep up to the minute on our site to find out whether your machine is configured securely and to determine whether or not you're missing any patches. We released a companion tool that server farm administrators can use so that if you're, for instance, an administrator with 100 machines, from a single console you can tell which patches each one of those machines is lacking and keep them up to date. But just the same, the fact that we didn't have perfect compliance ourselves illustrates that there's more work to be done and we're certainly committed to making improvements as we go forward. We have some new features in our upcoming products that we believe will make it even easier to stay up to date on patches, including some technologies that will allow you to stay up to date automatically.

Mr. HORN. That's very interesting and Mr. Trilling, I was intrigued by your testimony. Applying a few simple rules. One can prevent the majority of attacks on your systems. More specifically, you detailed three top security recommendations that would likely protect against 80 percent of the attacks. In your opinion, should these rules be made mandatory for government agencies? That's a good probability.

Mr. TRILLING. Right. It's an interesting question. I think a little outside my area of expertise. I certainly feel like security rules and security policies really ought to be decided on by security companies rather than necessarily by the government. The other thing to point out is that security really is different for everybody. One of the things we often say is that it's important to secure your systems in such a way that the cost of breaking into that system is greater than the value of information you could get out of that system. So the effort to protect information for the Department of Defense is going to be very different than for a home user's individual Web site. I think each of those decisions needs to be made individually by individual organizations in consultation in many cases with security experts.

I'd have to sort of understand a little bit the framework of what you're talking about but I think in general it would be difficult to sort of mandate across all agencies that these certain laws ought to be applied because the needs of security for different agencies and different organizations are really different depending on the value of what they're trying to protect.

Mr. MILLER. Mr. Chairman, the Federal CIO Council is trying to deal with this kind of a challenge and IT has been somewhat involved. It's basically led by the Federal CIO Council, particularly Mr. John Gilligan who's now the Deputy CIO at the Department of the Air Force and previously was CIO at the Department of Energy. What they're trying to do is establish best practices across agencies and it is complicated for the reasons Mr. Trilling suggested because there's no one size fits all. But by sharing information within the Federal CIO Council and then between industry and government, that's the role ITA has played by bringing to the government CIOs some of the best practices applied in commercial settings. We think there has been some progress there.

Your staff might want to get a debriefing from the Federal CIO Council about how their best practices are coming along. They're trying to achieve in practice what Mr. Trilling has outlined in theory would be a good idea.

Mr. TRILLING. If I could just make one quick point just to take an example. If you were to mandate inside an organization every user inside the organization needed to change their password every 5 minutes, clearly that would reduce productivity enormously to the extent that most companies would never make that tradeoff. But there may well be some organization, some government organization where security is so critical that you're willing to make that tradeoff, and you see this over and over again, the tradeoff between convenience and security. More convenience often means less security and people need to, again, appropriately protect themselves depending on the value of their information stored on their computer networks.

Mr. HORN. Mr. Neumann.

Mr. NEUMANN. A couple of comments. One is that this 80/20 business is a moving target. I go back to my tip of the iceberg analogy. You chop off the top very small percentage of the iceberg and there's still exactly the same size of the iceberg there. You may get rid of the 80 percent but there's an escalation effect here in that the attackers are advancing faster than the developers which means that no matter how much there is visible of the iceberg, you still have a very serious problem.

You mentioned education. Let me just speak to that. I've taught in a bunch of different universities. Most recently I taught a course based on work that I've done for the Army Research Lab on how to build reliable, secure, highly survivable systems. All of the notes for that course are on my Web site and I think when you talk about how do you set principles and try to get people to enforce them, a good place to start is to read a document like that and discover what the principles are and see which ones of them are applicable.

The most important thing is the architecture, as I've mentioned. I don't have a virus problem. I can read e-mail with all kinds of attachments but it never bothers me. I'm not running a Microsoft operating system. I'm running a Lennox system. Lennox has its own security violations and vulnerabilities. But the point is that if you focus on an architecture in which your system protects itself against itself—and again I go back to the research that we did in 1965 which pretty much solved that problem—then a lot of the problems that you see in malicious code don't happen because the malicious code is executing with all of your privileges and you're giving it freedom to do whatever it wants.

So all of the stuff about Trojan horses is ignoring one fundamental thing. That once somebody has broken into your system with a virus or a worm or whatever it is, you don't know that there's a residual Trojan horse there. There might be something nasty just sitting waiting for something else to happen. The Trojan horses are really the ultimate problem here. We're talking a lot about viruses and worms, but the real problem is the fact that systems are not designed with adequate architectures to protect themselves against themselves and to protect themselves against outsiders as well as, of course, insiders.

Mr. TRILLING. May I make a very quick comment to respond to Mr. Neumann. I think you're quite correct in saying that it is a moving target and that more of the iceberg is always showing when you cutoff the top. But again, it's about reducing risk. As we pointed out here, most of these crimes, most of these worms that we talked about today, were not targeted attacks. They were crimes of opportunity. Code Red simply went from machine to machine checking somebody's door knob. It would be like somebody walking through a neighborhood seeing if each door was open. If the door was open, they'd walk in and attack. If not, they'd keep moving. You could break into that home but you might as well keep walking down the block because you'll find another home that's open down the road.

Most of these attacks such as Code Red are crimes of opportunity. They're going from machine to machine seeing if they can break in and so, again, it's all about reducing risk. By taking a small number of steps, we believe you can reduce your risk a lot. Certainly, to reduce your risk further to get that next part of the iceberg is going to be a big step for some organizations is more cost effective and more needed than others. But you want to make sure that the person just trying to walk into your door or come in through your basement, which is how most attacks are occurring today, you want to make sure you're stopping that. That's for government machines as well as home machines.

Mr. HORN. Mr. Maiffret, any thoughts on this?

Mr. MAIFFRET. I guess beyond just like it's really something where I think they're kind of talking like if you like patch the current top 10 vulnerabilities, you're making the best effort. But I think what Mr. Neumann was saying is when you patch the ranked top 10 right now, then hackers move on to the next top 10 and the next top 10. It's really something where the biggest vulnerabilities, they're just that and if you fix them, then the things that were not necessarily the biggest vulnerabilities the week before, now they are. It's really something where you do have to try to eliminate all of them. It's not something about doing the top 10 checklist or something of that nature.

Mr. TRILLING. I think that's also a really good point which is that you never get to the point where you are now secure. Security is a moving target. The value of the information on your network could suddenly change tomorrow as your business changes, as you acquire a new organization. So companies, organizations, government entities should never be stopping and saying, well, because we've gone through these top 10 lists, we're now done. Security is an evolving thing in much the same way that physical security is also.

Mr. HORN. One of my colleagues who sat near me in our investigation of the White House e-mails which went on for dozens of hours and he said to me, he said, I'm just going to get rid of e-mail. The heck with it. They had the most stupid conversation. It was not great political theory or great policy and all this. They were darned stupid crazy things. Everything from every joke on Arkansas and everything else. He said, enough is enough. If they want to see me, they can walk through the door.

Panel one has been very gracious listening to this dialog and if you have any thoughts that we haven't explored, feel free to get to the microphone or we can just send it back, I think, and put it in the front row there whereas they're in the orchestra pit. I've got a number of questions here and if you're on the way home or something or dictating into whatever your little thing is, we would welcome. Both the Democratic staff and the Republican majority staff have a number of questions. So we appreciate any helpfulness you could give in answer.

We will keep the hearing over and out and open for probably 2 weeks and then any thoughts you have going back. I want to thank all of you. You're very able in your whole firm of computers and enhancing computer security in the public and private sectors is a priority of this subcommittee and must become a priority, we think, for governments at all the levels because as we get from enhancing computer security, we're also talking about helping to have privacy for the citizen. Their records should not be used without their access or whatever the law reads on that.

We'll issue a second report card on computer security within the Federal Government shortly. Attention to and action on this important issue must occur at the highest levels. It took them 2 years in the previous administration to wake up to Y2K and we're hoping that the current administration will take this very seriously, and I think they will. Today's hearing is a part of that process and we thank you very much for coming here, some of you for 3,000 miles.

The staff I'd like to thank for this hearing is to my left, J. Russell George, the staff director/chief counsel of the subcommittee. Bonnie Heald is here out in the audience. She's working with the press, professional staff member, director of communications. And then Elizabeth Johnston, as a lot of you know, is a detailee with us and very knowledgeable on all sorts of issues. Scott Fagan is assistant to the subcommittee. Scott, this is his last hearing because he's going into the American Foreign Service. So you might see him in embassies throughout the world and maybe one of these days he'll be an ambassador and will be nice to us in congressional delegations. Hopefully you've been around us enough to know that Congress is trying to help you. We're not from the government alone.

David McMillen, professional staff for the Democrat group and the San Jose Council Chamber's contacts that really helped us here tremendously. Judy Lacy, Ross Braver and the court reporters and Mark Johnson is the clerk for the majority. Mark, you're still around. You're not going to go in the foreign service or anything, are you?

Mr. JOHNSON. I'm here as long as you want me.

Mr. HORN. And the court reporter is George Palmer. It's tough when you go as long as we have, and we thank you, Mr. Palmer, for doing a good job on this, and that it'll be a good transcript.

So now this hearing will be in other parts of the United States on a number of questions. So we thank you all. Adjourned.

[Whereupon, at 12:58 p.m., the subcommittee was adjourned, to reconvene at the call of the Chair.]

○