AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

YOU'VE GOT MAIL—BUT IS IT SECURE? AN EXAMINATION OF INTERNET VULNERABILITIES AFFECTING BUSINESSES, GOVERNMENTS AND HOMES

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

OCTOBER 16, 2003

Serial No. 108–95

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

★ 91–445 PDF WASHINGTON : 2004

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

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

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

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

BERNARD SANDERS, Vermont (Independent)

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

CONTENTS

	Page
Hearing held on October 16, 2003	1
Statement of:	
Evans, Karen, Administrator, Office of Electronic Government, Office of Management and Budget	23
Leighton, Dr. F. Thomson, chief scientist, Akamai Technologies, Inc., professor of applied mathematics, MIT; and Kenneth Ammon, president and co-founder, government solutions, NETSEC, Inc.	33
Letters, statements, etc., submitted for the record by:	
Ammon, Kenneth, president and co-founder, government solutions, NETSEC, Inc., prepared statement of	73
Cummings, Hon. Elijah E., a Representative in Congress from the State of Maryland, prepared statement of	20
Davis, Chairman Tom, a Representative in Congress from the State of Virginia, prepared statement of	4
Evans, Karen, Administrator, Office of Electronic Government, Office of Management and Budget, prepared statement of	26
Leighton, Dr. F. Thomson, chief scientist, Akamai Technologies, Inc., professor of applied mathematics, MIT, prepared statement of	40
Sanchez, Hon. Linda T., a Representative in Congress from the State of California, prepared statement of	14
Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of	9

YOU'VE GOT MAIL—BUT IS IT SECURE? AN EXAMINATION OF INTERNET VULNERABILITIES AFFECTING BUSINESSES, GOVERNMENTS AND HOMES

THURSDAY, OCTOBER 16, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 10:02 a.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis (chairman of the committee) presiding.

Present: Representatives Tom Davis of Virginia, Ose, Platts, Turner, Blackburn, Waxman, Cummings, Tierney, Watson, Van Hollen, Sanchez, Ruppersberger, and Norton.

Staff present: Peter Sirh, staff director; Melissa Wojciak, deputy staff director; Ellen Brown, legislative director and senior policy counsel; Randall Kaplan, counsel; David Marin, director of communications; Victoria Proctor, senior professional staff member; Drew Crockett, professional staff member; Teresa Austin, chief clerk; Brien Beattie, deputy clerk; and Corinne Zaccagnini, chief information officer; Michelle Ash, minority counsel; Nancy Scola, minority professional staff member; Earley Green, minority chief clerk; Jean Gosa, minority assistant clerk; and Cecelia Morton, minority office manager.

Chairman TOM DAVIS. Good morning. A quorum being present, the Committee on Government Reform will come to order. I would like to welcome everybody to today's hearing on Internet vulnerabilities and the threat they pose to our national security, public health and safety, and economy.

Citizens, businesses and governments rely on the Internet for a variety of activities: business transactions, acquisition of goods and services, and the collection and dissemination of information, to name just a few. This morning the committee will review what steps these disparate groups are taking to create a more secure cyber-environment, with particular attention to the Federal Government's response to this growing cyber-threat.

My primary goal today is one of public education. Computer security can no longer be relegated to the back benches of public discourse, or remain the concern solely of governments or corporate technology experts. Think of electronic tax filing or online license renewals. The fact that we are all ever-more "interconnected" means we are all in this battle together. What affects one system

could very well affect all of us, and the unfortunate reality is that the Internet is inherently a breeding ground for malevolent actors.

Congress has taken some strides to help Federal agencies protect their information systems from security breaches. I sponsored FISMA, the Federal Information Security Management Act of 2002, which was enacted last year as part of the E-Government Act of 2002. FISMA provides a strong framework for information security in the Federal Government by requiring Federal agencies to use a risk-based management approach to secure their information systems.

This year, Chairman Putnam and his subcommittee will closely oversee implementation of FISMA, including new OMB guidelines, and the establishment of agency testing and evaluation plans, and the development and promulgation of information security standards. FISMA is a step in the right direction for Government, but the threat is still great.

As we have seen in recent months, computer viruses and worms can cause significant damage to home and work computers. Loss of files and data can cause irreparable financial damage, mar a business reputation and even shut down operations in a private or Government enterprise. Furthermore, hackers are able to divert traffic from Web sites and steal information, including personally identifiable information, patients' medical records, and financial details. The financial impact of such attacks is estimated to range from hundreds of millions into the billions of dollars. Other intentional threats include electronic eavesdropping or scanning to uncover passwords and other data.

But there are also unintentional threats that can be caused by flaws in computer software. From chief information officers to students to small business owners, everyone needs to know how to respond to cyber attacks. When a new flaw is identified in ubiquitous software like Microsoft operating systems, users need to take preemptive action to minimize damage from the inevitable hacker attacks. For example, security patches released by software manufacturers can be installed in systems to correct these flaws. When patches are announced, one has to act quickly to install them. So does the average computer user know what software he is running? Does he know if the alert applies to him? If so, does he know where to find the patch and how to apply it? The committee is examining these questions as part of the information security effort in the Federal Government.

The aggressive push to implement e-government initiatives means that Federal computer systems are communicating with computers in homes and businesses. If non-Federal computers are not adequately secured, there is an added risk to our Federal system. The challenge for the Federal Government is to promote electronic government initiatives while ensuring the integrity of its systems.

Educating all computer users about cyber security is critical. It is a matter of public safety, and our outreach needs a sense of urgency. When you connect to another computer, you are connecting to every computer that computer has ever connected to. Now, for most computer users, security is an issue that they may address at work, but most people are lax about securing a home computer

that is connected to the Internet. The average user needs to understand the full range of threats. For example, how software such as peer-to-peer file sharing applications leave computers defenseless against cyber attacks. For instance, the recent Swen worm circulating in Europe purports to be a Microsoft security alert and enters computers as an e-mail attachment on an e-mail "delivery failure" notice. Then it tries to spread to other computers through the Kazaa peer-to-peer file-sharing network. Because of the interconnectivity of the information systems and the increased reliance on computers for transactions via the Internet, this type of worm has the potential to cause significant damage to home computers as well as those in businesses, financial institutions, and governments.

Even our Nation's critical infrastructure sectors depend on information systems to protect the Nation's water supply, oil and gas pipelines, electrical grids, and other critical infrastructure. Significant damage to these systems could have a devastating impact on our national security, public health and safety, and economy. In fact, terrorists have already expressed their intent to attack our critical infrastructure, prompting the GAO to include cyber critical infrastructure protection on its high-risk series for the first time in January 2003.

We have three distinguished witnesses with us this morning to help shed some light on this important issue. On our first panel, the committee will hear from Ms. Karen Evans, the Administrator of the Office of Electronic Government at OMB. This is her maiden testimony before this committee. She will testify about the Federal Government's response to this growing cyber threat. Welcome, Karen. We are happy to have you here. You come here with a great reputation from the Department of Energy, so we are pleased to hear what you say and look forward to working with you.

Our second panel is Dr. Tom Leighton, the co-founder and chief scientist of Akamai Technologies, and Mr. Kenneth Ammon, president and co-founder of NetSec. Akamai will give a demonstration of the "Slammer" worm's effect in elapsed time and its estimated impact on individual computers and networks. A presentation from NetSec will show the ease with which the average computer user can obtain names, Social Security numbers, and other sensitive information through popular search engines like Google.

I would like to thank all of our witnesses for appearing before the committee. I look forward to their testimony. I now yield to Mr. Waxman for his opening statement.

[The prepared statement of Chairman Tom Davis follows:]

Opening Statement
Chairman Tom Davis
Committee on Government Reform
You've got mail – but is it secure?
Internet Vulnerabilities Affecting Businesses, Governments, and Homes

Good morning. A quorum being present, the Committee on Government Reform will come to order. I would like to welcome everyone to today's hearing on Internet vulnerabilities and the threat they pose to our national security, public health and safety, and economy.

Citizens, businesses, and governments rely on the Internet for a variety of activities: business transactions, acquisition of goods and services, and the collection and dissemination of information, to name a few. This morning the Committee will review what steps these disparate groups are taking to create a more secure cyber-environment, with particular attention to the Federal government's response to this growing cyber-threat.

My primary goal today is one of public education. Computer security can no longer be relegated to the back benches of public discourse, or remain the concern solely of governments or corporate technology experts. Think of electronic tax filing, or online license renewals. The fact that we are all ever-more "interconnected" means we are all in this battle together. What affects one system could very well affect us all, and the unfortunate reality is that the Internet is inherently a breeding ground for malevolent actors.

Congress has taken some strides to help federal agencies protect their information systems from security breaches. I sponsored FISMA (the Federal Information Security Management Act of 2002), which was enacted last year as part of the E-Gov Act of 2002. FISMA provides a strong framework for information security in the federal government by requiring federal agencies to use a risk-based management approach to secure their information systems.

This year, Chairman Putnam and his subcommittee will closely oversee implementation of FISMA, including the development of new OMB guidance, the establishment of agency testing and evaluation plans, and the development and promulgation of information security standards.

FISMA is a step in the right directions for the government. But the threat is still great.

As we have seen in recent months, computer viruses and worms can cause significant damage to home and work computers. Loss of files and data can cause irreparable financial damage, mar a business' reputation, and even shut down operations in a private or government enterprise.

Furthermore, hackers are able to divert traffic from websites and steal information, including personally identifiable information, patients' medical records, and financial details. The financial impact of such attacks is estimated to range from hundreds of millions to billions of dollars.

Other intentional threats include electronic eavesdropping or scanning to uncover passwords and other data.

But there are also *unintentional* threats that may be caused by flaws in computer software. From Chief Information Officers to students to small business owners, everyone needs to know how to respond to cyber attacks. When a new flaw is identified in ubiquitous software like Microsoft operating systems, users need to take preemptive action to minimize damage from the inevitable hacker attacks.

For example, security patches released by software manufacturers can be installed in systems to correct these flaws. When patches are announced, one has to act quickly to install them. So, does the average computer user know what software he is running? Does he know if the alert applies to him? If so, does he know where to find the patch and how to apply it? The Committee is examining these questions as part of the information security effort in the federal government.

The aggressive push to implement e-government initiatives means that federal computer systems are communicating with computers in homes and businesses. If non-federal computers are not adequately secured, there is added risk to our federal systems. The challenge for the federal government is to promote electronic government initiatives -- while ensuring the integrity of its systems.

Educating all computer users about cyber security is critical. It's a matter of public safety, and our outreach needs a sense of urgency. When you connect

to another computer, you're connecting to every computer that that computer has ever connected to.

For most computer users, security is an issue they may address at work, but most people are lax about securing a home computer connected to the Internet. The average user needs to understand the full range of threats – for example, how software such as peer-to-peer file sharing applications leave computers defenseless against cyber attacks.

For instance, the recent Swen worm circulating in Europe purports to be a Microsoft security alert and enters computers as an e-mail attachment or an e-mail "delivery failure" notice. Then it tries to spread to other computers through the Kazaa peer-to-peer file-sharing network. Because of the interconnectivity of information systems and the increased reliance on computers for transactions via the Internet, this type of worm has the potential to cause significant damage to home computers as well as those in businesses, financial institutions, and governments.

Even our nation's critical infrastructure sectors depend on information systems to protect the nation's water supply, oil and gas pipelines, electrical grids, and other critical infrastructures. Significant damage to these systems could have a devastating impact on our national security, public health and safety, and economy. In fact, terrorists have already expressed their intent to attack our critical infrastructure, prompting the General Accounting Office to include cyber critical infrastructure protection on its high-risk series for the first time in January 2003.

We have three distinguished witnesses with us this morning to help shed some light on this important issue.

On our first panel, the Committee will hear from Ms. Karen Evans, Administrator of the Office of Electronic Government at OMB. She will testify about the Federal government's response to this growing cyber-threat. I understand this is her first congressional appearance; welcome.

On our second panel is Dr. Tom Leighton, Co-Founder and Chief Scientist of Akamai Technologies and Mr. Kenneth Ammon, President and Co-Founder of NetSec. Akamai will give a demonstration of the "Slammer" worm's effect in elapsed time and its estimated impact on individual computers and networks. A presentation from NetSec will show the ease

with which the average computer user can obtain names, Social Security numbers and other sensitive information through popular search engines like Google.

I would like to thank all of our witnesses for appearing before the Committee, and I look forward to their testimony. And I now yield to Mr. Waxman for his opening statement.

Mr. WAXMAN. Thank you, Mr. Chairman. I want to commend you for holding this hearing. This hearing today is another important hearing on computer security.

Earlier this year we held a series of hearings on the risks of peer-to-peer file sharing programs, including how they could be used to find all kinds of personal data about computer users. This then led to the introduction and passage in the House of the Government Network Security Act of 2003, which requires Federal agencies to assess the risk posed by peer-to-peer file sharing programs.

Today we are exploring another aspect of computer security: how worms and viruses spread rapidly across the Internet, finding unprotected computers. We also will learn how millions of people are using wireless networks, many unaware that their computers are vulnerable to attack. Business, governments, and individual home users are at risk for computer invasion. Efforts must be taken by all users to make the Internet more secure.

There is an important role for government in protecting families from the risks of worms, viruses, and other malicious files. American families do not have computer experts on staff, or even easy access to training. If the family is lucky, it has a teenager who understands computers, but even that is not enough. The Government can help by providing the public access to the vast wealth of information on computer security developed by our Government agencies.

Computer software manufacturers can help also. Patch management on home computers is becoming more automated, but it is not clear that the majority of the public understands the importance of installing these patches and what the patches do. It would be better if the software had fewer holes when it was shipped.

The Internet is a communal good. No one person or organization can secure it; it can only be secured by a joint effort. That effort needs active participation from businesses that work on the Internet as well as businesses that produce computer software. And there is a role for Government both in securing its own computers and in educating the public of the risks and how to handle those risks.

Mr. Chairman, the hearings you have held on these important topics have helped inform Congress and the public and provided the foundation for legislation. I want to commend you for your leadership on these issues, and I look forward to the hearing.

[The prepared statement of Hon. Henry A. Waxman follows:]

Statement of Rep. Henry Waxman, Ranking Minority Member
Committee on Government Reform
Hearing on
"You've got mail -- but is it secure? An Examination of Internet Vulnerabilities Affecting Businesses, Governments, and Homes."

October 16, 2003

Today the Committee is holding another important hearing on computer security.

Earlier this year, we held a series of hearings on the risks of peer-to-peer file sharing programs, including how they can be used to find all kinds of personal data about computer users. This then led to the introduction and passage in the House of the Government Network Security Act of 2003, which requires federal agencies to assess the risks posed by peer-to-peer file sharing programs.

Today we are exploring another aspect of computer security: how worms and viruses spread rapidly across the Internet finding unprotected computers. We also will learn how millions of people are using wireless networks; many unaware that their computers are vulnerable to attack.

Businesses, governments, and individual home users are at risk for computer invasion. Efforts must be taken by all users to make the Internet more secure.

There is an important role for government in protecting families from the risks of worms, viruses, and other malicious files. American families do not have computer experts on staff or even easy access to training. If a family is lucky, it has a teenager who understands computers, but even that is not enough. The government can help by providing the public access to the vast wealth of information on computer security developed by our government agencies.

Computer software manufacturers can help also. Patch management on home computers is becoming more automated, but it is not clear that the majority of the public understands the importance of installing these patches or what the patches do. It would be better if the software had fewer holes when it was shipped.

The Internet is a communal good. No one person or organization can secure it. It can only be secured by a joint effort. That effort needs active participation from businesses that work on the Internet as well as businesses that produce computer software. And there is a role for government both in securing its own computers and in educating the public of the risks and how to address those risks.

Mr. Chairman, the hearings you have held on these important topics have helped inform Congress and the public and provided the foundation for legislation. I commend you for your leadership on these issues, and I look forward to the hearing.

Chairman TOM DAVIS. Thank you very much.

Any other Members wish to make statements? Ms. Sanchez.

Ms. SANCHEZ. I would like to commend Chairman Davis and Ranking Member Waxman for calling this important hearing today, because I know, firsthand, how tedious and cumbersome computer infections can be. In the past year I have had several computer viruses, and, as a result, every time my computer screen freezes, I am paranoid that I have another virus.

Through an e-mail list serve that I have called the Washington Update, I update my constituents on a regular basis about what is happening in Washington, DC, and when I wrote to my constituents about today's hearing and requested that they share with me some of their experiences with computer viruses, the results were immediate and resounding. I was inundated with e-mails about the economic, social, and personal toll computer viruses have on the lives of my constituents, and I just want to share a really quick sampling of some of those stories before we begin.

A gentleman by the name of Mark Patton, who owns a business in my community, wrote to me and said, "Our business was victimized by a number of computer viruses on one occasion. We had hired an IT consultant to provide maintenance for our network, but, unfortunately, they were not keeping up with our virus protection. As a result, we had to replace our server, upgrade our system, and subsequently fire our IT consultant. The entire episode cost our small business over $10,000, without even considering the lost time we incurred. Viruses are a threat to all businesses. The lesson is buyer beware when hiring an IT consultant, but, more importantly, as businesses become more and more dependent on the Internet, Internet security becomes a very important issue."

The Mission Hills Mortgage Bankers Gateway Business Bank wrote to me and said, "At the height of the virus infected e-mail epidemic, Mission Hills Mortgage Bankers Gateway Business Bank Web mail site was swamped with thousands of virus-laden e-mails a day in August and September. Fortunately, our firewall and virus software caught and cleaned up our e-mail system, but the unsanitized e-mail was passed through to the individuals to whom it was addressed. Personally, I was deleting 30 to 50 e-mails a day, both annoying and time-consuming. What I didn't know was how vulnerable a home computer with DSL or cable access is without a firewall, even with virus checker software. I wasn't aware that viruses can come through to your computer in ways other than on an e-mail until I got one. That was a month ago. I purchased and installed a firewall right away, but I am still experiencing a problem with my computer. Apparently the damage to files can remain after the virus is cleaned up."

And this problem has not only affected the businesses that wrote to me, but Rio Hondo Community College wrote to me: "We were hit hard by the worm at Rio Hondo College during the first week of our semester this fall. Our mainframe computer and every desktop computer on campus was unusable for a week. We could not register students, certify athletic eligibility of athletes, process financial aid requests, conduct many of our classes, or function in any capacity for a whole week. Eight weeks later we are still trying to get computers and printers and e-mail functioning for everyone."

This particular little anecdote very much moved me. A constituent by the name of Mark Katt wrote: "I like to take pictures of my daughter, who is currently 2 years old. I use my digital camera to take a picture of her from the moment she was born and every single month until she reached her first birthday. I stored all of those pictures in my hard drive, so when I would be ready I would sort them all out and have them developed and make a nice album that I could show my daughter when she grew up, and maybe play a slide show during her 18th birthday party. But my computer was hit by the virus just before I got them developed. My 1 year worth of project, my dream and my gift to my daughter, are all gone, together with the pictures. I would pay, no matter what the price, if I could retrieve all of those pictures. They were priceless, and you cannot bring back the hands of time."

Diane Schumacher from my district wrote: "I had a virus in September of this year. It was the "So Big" virus. I got it when I purchased an item over the Internet that came with an attachment. I have been laid off. The last thing I needed was to be out of contact not only with the EDD, the Employment Development Department, but also with my job search and support groups, not to mention the expense of trying to repair the damage."

The stories that I have just shared with you today underscore the prevalence of computer infections. Furthermore, computer viruses are a very real problem not just for businesses, but home users are also affected by this burdensome and costly problem. An unemployed constituent, a community college, a bank, and a father all have been victimized by computer viruses. They affect everybody. There is much work ahead of us to eradicate the threat of computer infections, so I want to thank each of the witnesses for being here today to discuss this important topic, and I look forward to their testimony.

Again, I would like to thank the chairman and the ranking member for holding this hearing.

[The prepared statement of Hon. Linda T. Sanchez follows:]

Opening Remarks:
"You've Got Mail—But is it Secure? An Examination of Internet Vulnerabilities Affecting Businesses, Governments, and Homes"

Rep. Linda T. Sánchez
July 18, 2003

- I would like to commend Chairman Davis and Ranking Member Waxman for calling this important hearing today.

- I know first hand how tedious and cumbersome computer infections can be. In the past year, I've had several computer viruses. As a result, every time my computer freezes I automatically think I have another virus.

- Through my email list serve, the Washington Update, I update my constituents on a regular-basis about what's happening in DC.

- When I wrote to my constituents about today's hearing and requested that they share with me some of their experiences with computer viruses, the response was immediate and resounding.

- I was inundated with emails about the economic, social, and personal toll computer viruses have on the lives of my constituents.

- Let me share a sample of these stories with you today to highlight the impact viruses can have on our daily lives.

> ***Mark Patton who owns a business in my community-*** Our business was victimized by a number of computer viruses on one occasion. We had hired an IT consultant to provide maintenance of our network, but unfortunately they were not keeping up with our virus protection. As a result we had to replace our server, upgrade our system, and subsequently fire our IT consultant. This episode cost our small business over $10,000 without considering the lost time we incurred. Viruses are a threat to all businesses...The lesson is buyers beware when hiring an IT consultant, but more importantly as businesses become more dependant on the Internet, Internet security becomes a very important issue.
>
> ***Mission Hills Mortgage Bankers/Gateway Business Bank wrote:***
> During the height of the virus-infected e-mail, Mission Hills Mortgage Bankers/Gateway Business Bank webmail site was swamped with thousands of virus-laden e-mail a day in

August and September. Fortunately, our firewall and virus software caught and cleaned up the e-mail, but the sanitized e-mail was passed through to the individuals to whom it was addressed. Personally, I was deleting 30 to 50 e-mails a day, both annoying and time consuming.

What I didn't know was how vulnerable a home computer with DSL or cable access is without a firewall even with virus-checker software. I wasn't aware that viruses can come thru to your computer in ways other than on an e-mail until I got one. That was a month ago. I purchased and installed a firewall right away. But I am still experiencing a problem with my computer. Apparently, the damage to files can remain after the virus is cleaned up.

- This problem has not only affected businesses:
  Rio Hondo College wrote--We were hit hard by the "worm" at Rio Hondo College during the first week of our semester this Fall. Our mainframe computer and every desktop computer on campus were unusable for a week. We could not register students, certify athletic eligibility of athletes, process financial aid requests, conduct many classes, or function in any capacity for a whole week. Eight weeks later we are still trying to get computers and printers and e-mail functioning for every one.

Mark Catt wrote--
I'd like to take pictures of my daughter who currently is 2 years old. I used my digital camera to take a picture of her from the moment she was born and every single month until she reached her first birthday. I stored all those pictures in my hard drive so when I am ready, I'll sort them all out and have them developed and make a nice album that I can show to my daughter when she grow up and maybe play a slide show during her debut (18th Birthday Party). But my computer was hit by the virus just before I got them developed...my one year worth of project, my dream, and my gift to my daughter are all gone together with the pictures. I would pay-no matter what the price – if I could retrieve all those pictures...they were priceless...you cannot bring back the hands of time!!

Diane Schumacher wrote-
I had a virus in September of this year. It was the SO/BIG Virus. I got it when I purchased an item over the Internet that came with an attachment. I have been laid-off. The last thing I needed was to be out of contact with not only EDD, the Employment Development Department, but also with my job search and support groups. Not to mention the expense of repair.

- The stories I've shared with you today underscore the prevalence of computer infections. Furthermore, computer viruses are a "real problem" not just for businesses, but home users are also affected by this burdensome and costly problem.

- An unemployed constituent, a community college, a bank and a father, all have been victimized by computer viruses. Computer viruses affect all of us.

- There is much work ahead of us to eradicate the threat of computer infections, so I would thank each of the witnesses for being here today to discuss this important topic and I look forward to your testimony.

- Again, I would like to thank the Chairman and Ranking Member for having this hearing.

Chairman TOM DAVIS. Thank you very much.

Any other opening statements?

Mr. CUMMINGS. Mr. Chairman, I have a very brief statement.

Chairman TOM DAVIS. Sure. Gentleman from Maryland.

Mr. CUMMINGS. I want to thank you, Mr. Chairman, for holding today's hearing on the vulnerability of the Internet for both businesses and citizens.

Initially, computers alone were subject to programming errors or bugs that were attached to computer programs affecting only individual computers, without the risk that the error would be passed on to another computer. Today, however, with increased knowledge about cyber technology and the advent of the Internet security weaknesses in both computers and on the Internet and because the Internet connects millions upon millions of computers and computer networks belonging to governments, business, schools, and homes, these seemingly small viruses or worms sent out by hackers have the potential to do major harm to computer operating systems.

The Internet is fundamental to present-day living. Business is conducted online, items are purchased and sold online, individuals communicate daily via e-mail or gather news and information from Web pages, and many even manage their accounts and conduct banking online. More importantly, the Federal Government, as well as other national structures, rely on the Internet for managing issues ranking from banking to defense. Because of this, cyber safety and security is pertinent, not only to individuals and private entities, but also to Federal security.

Today's hearing will serve as an avenue to educate the general public about the Internet's vulnerability, and it will also address important issues regarding the different ways researchers, the Government, and the software industry can work together to eliminate these vulnerabilities through the creation of effective patches and systems for dealing with Internet security risks, as well as the expedition and discovery of cyber criminals. We must be proactive in our efforts to deal with cyber security and our review of the many different ways technology has the potential to greatly enhance or reduce the quality of life for Americans and the rest of the world.

Again, I thank you, Mr. Chairman, for holding this hearing. I look forward to hearing from our witnesses today as we discuss different ways to protect the vital infrastructure of the Internet and educate home and small business users about computer infections.

With that, I yield back.

[The prepared statement of Hon. Elijah E. Cummings follows:]

Statement of Congressman Elijah E. Cummings
Government Reform Hearing
On
"An Examination of Internet Vulnerabilities for Businesses and Citizens"
October 16, 2003 at 10:00 a.m.

Thank you, Mr. Chairman for holding today's hearing on the vulnerability of the Internet for both businesses and citizens.

Initially, computers alone were subject to programming errors or "bugs" that were attached to computer programs affecting only individual computers without the risk that the error would be passed on to another computer. Today, however, with increased knowledge about cyber technology and the advent of the Internet, hackers have developed new software that takes advantage of security weaknesses in both computers and on the Internet. Because the Internet connects millions upon millions of computers and computer networks belonging to governments, businesses, schools, and homes, these seemingly small "viruses" or "worms" sent out by hackers have the potential to do major harm to computer operating systems.

The Internet is fundamental to present day living. Business is conducted online, items are purchased and sold online, individuals communicate daily via email or gather news and information from Web pages, and many even

manage their accounts and conduct banking online. More importantly, the federal government as well as other national structures rely on the Internet for managing issues ranging from banking to defense. Because of this, cyber safety and security is pertinent, not only to individuals and private entities, but also to federal security.

Today's, hearing will serve as an avenue to educate the general public about the Internet's vulnerability, and it will also address important issues regarding the different ways researchers, the government, and the software industry can work together to eliminate these vulnerabilities through the creation of effective patches and systems for dealing with Internet security risks, as well as the expedition and discovery of cyber criminals.

We must be proactive in our effort to deal with cyber security and our review of the many different ways technology has the potential to greatly enhance or reduce the quality of life for Americans and the rest of the world.

Again, thank you for holding this hearing. I look forward to hearing from today's witnesses as we discuss the different ways to protect the vital

infrastructure of the Internet and educate home and small business users about computer infections.

Chairman TOM DAVIS. Thank you.

Any other statements?

All right, we will proceed to our first panel. Again, we have the Honorable Karen Evans, the Administrator of the Office of Electronic Government at the Office of Management and Budget.

It is the policy of this committee that we swear you in, so if you would rise with me and raise your right hand.

[Witness sworn.]

Chairman TOM DAVIS. Thanks for being with us. Your whole statement is in the record. You have a light in front of you. When it turns orange, 4 minutes are up. You are given 5 minutes. If you need more, take it, but I think we would like to keep to that so we can get to questions. Keep it moving. Thank you.

STATEMENT OF KAREN EVANS, ADMINISTRATOR, OFFICE OF ELECTRONIC GOVERNMENT, OFFICE OF MANAGEMENT AND BUDGET

Ms. EVANS. Good morning, Mr. Chairman, Ranking Member Waxman, and members of the committee. Thank you for inviting me to discuss the Federal Government's response to this growing cyber threat.

The Federal Computer Incident Response Center, FedCIRC, within the Department of Homeland Security is the Federal Government's civilian focal point for coordinating response to cyber attacks, promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. As part of its responsibilities, FedCIRC informs Federal agencies about current and potential security threats.

Working with FedCIRC, OMB and the CIO Council have developed a process to rapidly counteract identified threats and vulnerabilities. CIOs are advised via conference call, as well as followup e-mail, of specific actions needed to protect agency systems. Agencies must then report to OMB on the implementation of required countermeasures.

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

Securing cyberspace is an ongoing process as new technologies appear and new vulnerabilities are identified. The National Institute of Standards and Technology [NIST], provides timely guidance to Federal agencies on securing networks, systems and applications. NIST recommends that agencies implement patch management programs, harden all hosts appropriately, deploy antivirus software to detect and block malicious code, and configure the network perimeter to deny all traffic that is not necessary. Additional recommendations include user awareness briefings, as well as training for technical staff on security standards and procedures.

As part of its statutory responsibilities under the Federal Information Security Management Act, NIST published in September a

draft Computer Security Incident Handling Guide. This publication seeks to help both established and newly formed incident response teams to respond effectively and efficiently to a variety of incidents.

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

Improving the Federal Government's response to Internet-based attacks also requires that we focus on enterprise architecture and standardized deployment of security technologies. As new technologies become available and cost-effective, they must be incorporated into the IT infrastructure where they can monitor common precursors and indications of attacks.

Discerning the source of malicious Internet activity is often difficult. The Federal Government will continue to rely on Federal, State, and local law enforcement to investigate and prosecute developers of worms, viruses, and denial of service attacks. Agencies must continue to report computer incidents and assist law enforcement investigations to the greatest extent possible.

The National Strategy to Secure Cyberspace recommends that the software industry consider promoting a more secure out-of-the-box installation and implementation of their products, including increasing user awareness and user friendliness of their security features. OMB supports the agency use of enterprise licensing agreements which will require vendors to configure software to meet security benchmarks.

Additionally, the Federal Government will soon begin a comprehensive review of the National Information Assurance Partnership [NIAP]. The review will consider to what extent, if any, NIAP can address the continuing problem of security flaws in commercial software products. This review will include lessons learned from the implementation of the Department of Defense July 2002 policy requiring the acquisition of products to be reviewed under the NIAP evaluation process.

Patch management is an essential part of the agency's information security program and requires a substantial investment of time, effort, and resources. At the present time, 47 agencies subscribe to FedCIRC's Patch Authentication and Dissemination Capability. This service validates and quickly distributes corrective patches for known vulnerabilities.

Because of its vast inventory and the vulnerabilities inherent in commercial software, the Federal Government will, for the immediate future, continue to be impacted by threats from the Internet. Through our oversight of agency security polices and practices, OMB will continue to work with agencies to ensure that risks associated with cyber attacks are appropriately mitigated.

In closing, OMB is committed to a Federal Government with resilient information systems. OMB will continue to work with agencies and the Congress to ensure that appropriate countermeasures are in place to reduce the impact of Internet-borne attacks.

[The prepared statement of Ms. Evans follows:]

STATEMENT OF THE HONORABLE KAREN EVANS

ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
October 16, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss Internet vulnerabilities and the dangers they pose to citizens, businesses and governments. My testimony today will focus on the Federal government's response to this growing cyber threat.

Dangers and Vulnerabilities presented by the Internet

The Internet connects over 171,000,000 computers and continues to expand at a rapid pace. At any point in time, there are millions of connected computers that are vulnerable to worms, viruses or denial of service attacks. Malicious actors can take advantage of these vulnerable machines and harness them together to create large scale attacks. Many attacks are fully automated and spread with blinding speed across the entire Internet community.

The private sector has become increasingly dependent on the Internet and now uses it for mission critical applications as well as online business transactions. Even relatively short interruptions in service can cause significant economic loss and can jeopardize critical services.

Similarly, the Federal government's reliance on the Internet will continue to grow in the years ahead. The healthy functioning of cyberspace will be essential to our homeland and national security.

Awareness of Internet Dangers

The Federal Computer Incident Response Center (FedCIRC) within the Department of Homeland Security is the Federal government's focal point for coordinating response to cyber attacks (non-law enforcement), promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. As part of its duties, FedCIRC informs Federal agencies about current and potential security threats from the Internet.

Working with FedCIRC, OMB and the CIO Council have developed a process to rapidly counteract identified threats and vulnerabilities. CIOs are advised via conference call, as well as follow up e-mail, of specific actions needed to protect agency systems. Agencies must then report through FedCIRC to OMB on the implementation of the required countermeasures. In

particular, we track data concerning the percentage of systems patched and the time needed to complete mitigation efforts.

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

Steps the Federal Government is Taking to Protect Itself from this Growing Threat

National Institute of Standards and Technology

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

NIST has produced a number of recent publications that address agency security practices. These publications include: a Guide to IT Security Services, Selecting Information Security Products, Network Security Testing, Building an IT Security Awareness and Training Program, and Security Considerations in the Information Systems Development Life Cycle. Earlier guidance included: Securing the Public Web Server, Electronic Mail Security, IT Contingency Planning, Security Metrics, System Administrator Guidance for Securing Win 2000, Wireless Security, Security Patch Management, Intrusion Detection Systems, Firewall Security, and Risk Management.

As part of its statutory responsibilities under the Federal Information Security Management Act, the National Institute of Standards and Technology published in September a draft Computer Security Incident Handling Guide. This publication seeks to help both established and newly formed incident response teams respond effectively and efficiently to a variety of incidents. More specifically, this document discusses organizing a computer security incident response capability, establishing incident response policies and procedures, structuring an incident response team, and handling incidents from initial preparation through the post-incident lessons learned phase. Finally, it discusses handling a range of incidents, such as denial of service, malicious code, unauthorized access, inappropriate usage, and multiple component incidents.

Federal Information Security Management Act

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

Federal Enterprise Architecture

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

Challenges Facing the Federal Government in Creating a More Secure Cyber-Environment

Attack Attribution

Because of the global nature of cyberspace, vulnerabilities are accessible to anyone anywhere with sufficient capability to exploit them. Discerning the source of malicious activity is often difficult. The federal government will continue to rely on federal, state and local law enforcement to investigate and prosecute developers of worms, viruses and denial of service attacks. Agencies must continue to report computer incidents and assist law enforcement investigations to the greatest extent possible.

Managing Vulnerabilities inherent in Commercial Software

Vulnerabilities result from weaknesses in technology as well as improper implementation and oversight of technological products. The National Strategy to Secure Cyberspace recommends that the software industry consider promoting more secure "out of the box": installation and implementation of their products, including increasing user awareness and user friendliness of their security features.

Use of Security Benchmarks

OMB supports agency use of enterprise licensing agreements which require vendors to configure software to meet security benchmarks. As an example, the Department of Energy recently signed an agreement with Oracle Corporation which calls for the vendor to deliver its database software in a securely configured manner.

Use of Trusted Products

In addition, the federal government will soon begin a comprehensive review of the National Information Assurance Partnership (NIAP). One thing they will consider is to what extent, if any, NIAP can address the continuing problem of security flaws in commercial software products. This review will include lessons-learned from implementation of the Defense

Department's July 2002 policy requiring the acquisition of products reviewed under the NIAP evaluation process.

Patch Management

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

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

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

Conclusion

The Federal government is the world's largest consumer of information technology. Because of its vast inventory and the vulnerabilities inherent in commercial software, the Federal government will, for the immediate future, continue to be impacted by threats from the Internet. Through our oversight of agency security policies and practices, OMB will continue to work with agencies to ensure that the risks associated with cyber attacks are appropriately mitigated.

In closing, OMB is committed to a federal government with resilient information systems. The dangers posed by the Internet must not be allowed to significantly affect agency business processes or disrupt services to the citizen. OMB will continue to work with agencies and the Congress to ensure that appropriate countermeasures are in place to reduce the impact of Internet borne attacks.

Chairman TOM DAVIS. Thank you very much.

Let me start the questioning. Mr. Ammon, in his testimony, states that computer security can't be an add-on but, rather, needs to be integrated into the IT infrastructure management. Can you discuss what efforts the Federal Government is taking in this regard, recognizing you have just been on the job a few weeks? Does OMB adequately address this in the budget review process?

Ms. EVANS. What I believe is occurring and what he means by that is that cyber security cannot be an afterthought; it can't be that the project is thought about or that the business investment is thought about, implemented, and then you add on cyber security. What OMB is doing through the business case and through the budget process is, as agencies develop business cases and propose their IT investments, cyber security is a critical factor in evaluating that investment and how that project is going to move forward. And it is evaluated up front, during the investment, prior to the investment decisions being made, and you have to address how cyber security is going to be implemented as that investment goes forward.

Chairman TOM DAVIS. As we let out these large contracts, is that a part of it, where we are asking the vendors or the potential vendors what the safeguards are they are putting into this? Do you know the answer to that?

Ms. EVANS. I would say right now that I can speak from my experience at Department of Energy of what was required of me through the budget process and through the management process that OMB does have over the agencies. And as we move forward and as agencies move forward in the procurement process, it is incumbent on the CIO, as they make those investment decisions, that those questions are asked during the procurement process of how you evaluate potential vendors and their products going forward so that as those products come into your infrastructure, the risk is identified, the risk then is either mitigated or a risk assessment is done in accordance with FISMA so that you know what the impact of that technology or that investment is going to be on your infrastructure. Then a risk assessment is done and the manager who is responsible accepts whether that risk level is acceptable for implementation within the infrastructure.

Chairman TOM DAVIS. But an IT contract is a very complex piece and procurement officials look at a lot. They look at cost.

Ms. EVANS. Yes.

Chairman TOM DAVIS. They look at experience. They take a look at what innovations can be brought to bear. They may have to look at a set-aside provision, depending on what it looks like and who is getting it. And I guess my question in all this is cyber security is obviously a factor. Ultimately, it could be the most important factor as you look down the road. We found this with Y2K. Even contracts as late as 1999 were being let, and there were no Y2K safeguards being put in. Where does this rank in the pecking order, and is there going to be an effort to try to rev this up as an important component of future IT purposes?

Ms. EVANS. Again, I would like to draw from my past experience and bring it forward into my new job at OMB. As a CIO, as a past CIO and now responsible for the IT assets of the Federal Govern-

ment as a whole, no decision is made without really assessing what the cyber security impact of that will be. If it is not assessed at the time, and continuously assessed through the life cycle of that investment, it will cost more, it could cost more in the long-run; and it is important that it is integrated into everything that we do. So I plan to bring that forward through several initiatives that are already ongoing within OMB to ensure that the cyber security aspect of whatever we do is properly addressed.

Chairman TOM DAVIS. Because it is a tough balancing act when you are looking over cost, experience and innovation, and somebody may have a more secure vehicle that may be far more expensive, and weighing it.

Ms. EVANS. Yes, it is.

Chairman TOM DAVIS. And the purpose of this hearing is, of course, cyber security. I think we are going to see in our next panel just tremendous vulnerabilities that we have that public isn't aware of. I am still very uncomfortable with our level of cyber security in Government and in the Internet at large. I think people don't understand the inherent risks that are out there. So it is a tremendous difficulty, and how we deal with it legislatively is one piece, and then the bulk of the public goes with the administration and what priority you are going to put on it.

I have one other question before we recognize someone else. A number of our vulnerabilities stem from flawed commercial software. Since the Federal Government is the largest consumer, do you feel that the National Information Assurance Partnership is adequately addressing this?

Ms. EVANS. Well, as I stated, we are going to begin a review of that and look to what extent that partnership will be able to address those particular issues. So as we move forward on that, I would be glad to come back to the committee with our evaluations.

Chairman TOM DAVIS. Keep us involved in that.

Ms. Sanchez, any questions?

Any questions?

Mr. CUMMINGS. I was just wondering, does OMB have efforts underway to reduce the amount of paperwork required under the Federal Information Security Management Act?

Ms. EVANS. Well, I would say, and again I have to draw from my agency experience as one who has to submit a lot of that information, who had to submit that, that the current processes and procedures in place allow for flexibility for the CIO and the program offices to be able to determine and assess what the risks are, to be able to submit the information under the Plans of Action and Milestones. So I don't know that I necessarily look at it as a reduction of paperwork, but it is really a process going forward of doing the risk assessment and how you accurately reflect that and be able to submit to OMB through the Plans of Action and Milestones.

Mr. CUMMINGS. So when you have older computers, I guess it makes it a lot more difficult, that is, the security issues.

Ms. EVANS. If you have older computers? I don't understand the question. Are you asking about the security vulnerabilities associated with older computers?

Mr. CUMMINGS. That is correct.

Ms. EVANS. We are getting into a technical discussion here, but it is a debate. Some people view that older computers could be more secure from the aspect that hackers have a tendency to attack and develop malicious code for newer operating systems. So some people may argue with you that an older computer is more secure because the current attacks are actually targeted to more current vulnerabilities. I would say that a CIO, in assessing overall security, would have to look at both of those: what are the risks associated with maintaining an older platform and ability to continue the operations and maintenance of that for the program that it is supporting versus the cyber security. I believe that we talked about the balancing act and the decisions that need to be made so that you can have a full comprehensive program moving forward.

Mr. CUMMINGS. Thank you.

Chairman TOM DAVIS. I just have a couple other questions before I let you go.

Ensuring adequate information security obviously requires a very skilled level of Federal employee. The Federal Government finds itself competing against the private sector for talented employees in these areas, and we have seen that some of our best and brightest are eligible to retire over the next few years in Government. Do you think that agencies have the resources necessary to execute the elaborate security measures that are necessary to maintain their systems and keep Government connected?

Ms. EVANS. I think that there are several initiatives that are underway so that agencies have tools that are available to them to capitalize on succession planning. Through the President's Management Agenda there is a human capital initiative that really outlines how an agency is going to deal with all aspects of human capital and succession planning. Also, through the work of the Federal CIO Council and through the work on the Committee on Human Workforce Development, under the chairmanship of Ira Hobbs, that has really put together a lot of work that has gone forward so that we can maximize the use of that within our existing resources, to be able to really deploy and utilize the talent that we have while we are also planning for the future and being able to move forward; that it is identified skill gaps for us to be able to concentrate on and to be able to move forward.

I think that the budget process, the way that it is set up, as agencies continue to move forward and identify where they want to invest and how they want to do things, that the budget process allows for them to identify how they want to deal with this and how they want to move forward in the future, and it will be evaluated and reflected in the budget and the budget decisions.

Chairman TOM DAVIS. OK. My last question is, the prevalence of Internet vulnerabilities highlights the need to establish a balance between the Government's communication with citizens and businesses and the security of Government networks. In his written testimony, Dr. Leighton recommends removing public-facing Web sites from Government networks. Are you aware of agencies that do this or are considering implementing such measures, and would this adversely affect any of the electronic government initiatives?

Ms. EVANS. Those are considered managed services and each CIO, as he goes forward in his planning and his strategy to man-

age those resources, that is an alternative that is considered. And so if that is the best solution for that agency's cyber security posture, as well as meeting the mission that it needs, that is an alternative that is evaluated for potential service providers. So it is a great idea if it meets your business need and it matches your cyber security posture of what you are doing for your department as a whole.

Chairman TOM DAVIS. OK. Well, thanks, this is the beginning of ongoing discussions and communications with you. I congratulate you on your new position. We are going to get our next panel in, and I wonder if you can stay for their testimony. I guess we wanted you to hear what they both have to say. We have two very able people from the private sector in this, and thank you very much.

We will take a 1-minute recess and try to move our next panel on, and swear them in and hear their testimony. It is going to be, I think, pretty interesting.

[Recess.]

Chairman TOM DAVIS. Our next panel is Tom Leighton, the co-founder and the chief scientist of Akamai Technologies, and Mr. Kenneth Ammon, the president and co-founder of NetSec.

It is our policy that we swear you in before you testify, so if you will just rise with me and raise your right hands.

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you very much. We are the chief investigative committee in Congress, and that is why we swear people in. We are not anticipating any acts of perjury, although I did have Wes Unseld, who was the head coach for the Bullets, up before a committee 1 year, and I asked him, since he was under oath, "Are the Bullets going to have a winning season this year?" And his answer was "I can promise you we will have exciting basketball." Now, at the end of the year we evaluated whether that qualified as crossing the line or not, given the record, but it is just the way we do things. But thank you both for being here. Dr. Leighton, why don't I start with you, and then Dr. Ammon. I think you have a demonstration?

Mr. LEIGHTON. Yes.

Chairman TOM DAVIS. So take whatever time you need on that, the same with you, Dr. Ammon, and then we will move to questions.

STATEMENT OF DR. F. THOMSON LEIGHTON, CHIEF SCIENTIST, AKAMAI TECHNOLOGIES, INC., PROFESSOR OF APPLIED MATHEMATICS, MIT; AND KENNETH AMMON, PRESIDENT AND CO-FOUNDER, GOVERNMENT SOLUTIONS, NETSEC, INC.

Mr. LEIGHTON. Chairman Davis, Ranking Member Waxman, Subcommittee Chairman Putnam, Subcommittee Ranking Member Clay, and members of the committee, I appreciate the opportunity to testify this morning about one of my personal and professional passions, namely, the Internet. The Internet has been a focus of my work at the Massachusetts Institute of Technology, and also constitutes the basis for our creation of Akamai Technologies.

Akamai runs the world's largest distributed computing platform with more than 14,000 computer servers located in over 1,100 dif-

ferent networks in 70 countries. Like the Internet itself, Akamai evolved from what was originally an academic research project sponsored by the Defense Advanced Research Projects Agency [DARPA]. Today, Akamai is a major commercial enterprise that delivers a substantial portion of all Web traffic. Using sophisticated mathematical methods and algorithms to coordinate the operation of thousands of Web servers across the Internet, Akamai distributes content and applications from thousands of Web sites to hundreds of millions of consumers worldwide. We serve each of you every day. Over 70 of the businesses on the Fortune 500 utilize the Akamai platform to distribute their content and applications reliably, securely, and efficiently, as do the Department of Defense, Department of Education, Department of Homeland Security, the FBI, Internal Revenue Service, the Centers for Disease Control and Prevention, the U.S. Geological Survey, the Supreme Court, and many other Federal, State, and local government organizations.

As part of our services, Akamai provides an extensive, real-time, worldwide view of Internet traffic and conditions, a glimpse of which we will see this morning. One of our central missions at Akamai is to enable enterprises and government agencies to understand and manage the many vulnerabilities and problems associated with using the Internet.

At Akamai we understand the power and potential of the Internet. Hundreds of millions of people use the Internet on a daily basis to send e-mail, search for information, pay a bill, buy a book, get the news, make a reservation, download music, run a business, or just to chat with a friend. Trillions of dollars of e-commerce are conducted over the Internet annually. The Internet is also used to manage critical national infrastructure in sectors such as transportation, banking, manufacturing, utilities, and defense. The Internet is truly a communications phenomenon that is transforming the way people work, live, derive entertainment, and communicate all over the world. It embraces fundamental notions of individual choice and freedom that are hallmarks of our American society.

Unfortunately, the power of the Internet can be exploited for evil as well as good, a phenomenon that is not atypical for such a great advance in technology. And for reasons that I will describe shortly, the Internet is particularly vulnerable to the exploits of those with malevolent intentions. As you know, we have already witnessed events wherein a single individual has been able to disrupt Internet communications on a widespread basis, thereby causing billions of dollars in economic damage. Less well understood is the fact that information being transmitted on the Internet can also be rerouted, stolen, and manipulated with relative ease. The consequences of such vulnerabilities are becoming increasingly dangerous as our dependence on the Internet grows. Internet and software security are talked about much but understood little. Today I will spend a few minutes talking about how the Internet works and why it is vulnerable.

Many people think of the Internet as a single network. This is a misconception. In fact, the Internet consists of over 15,000 separate networks spread across most every nation in the world. The wires and fibers in these networks are interconnected in a somewhat haphazard fashion by millions of switches known as routers.

There was no central architect who decided how or where the 15,000 networks should be connected to one another, and there was no central command center to govern the minute-by-minute or even month-by-month operations of the Internet.

The glue that holds the Internet together and that allows it to function are the protocols such as the Border Gateway Protocol [BGP], that are used to route packets of data from one network to another, the services such as the Domain Name System [DNS], that are used to identify the correct destination for traffic on the Internet, and the myriad software packages used to support such diverse tasks as e-mail, Web browsing, file sharing, and instant messaging. All of the software and protocols have flaws that can be exploited by an attacker. Thousands of new flaws were discovered in just the last year.

For the most part, the protocols used in the Internet today are very similar to those that were developed over 20 years ago when the Internet was first invented. Back then, the Internet was known as the DARPANet and it was used by only a small number of researchers in a few locations. The original Internet protocols were based on a foundation of trust. It was assumed that the users of the Internet would use the Internet for the purposes for which it was intended and that they would do nothing to harm either the infrastructure or other users, either intentionally or even by accident. There was a strong sense of community in which the individual user would not take actions to the detriment of the common good, even if such actions would directly benefit the individual. While such noble assumptions were fairly safe in the collegial environment of the DARPANet of 20 years ago, they are clearly not valid in the Internet of today, where there are many individuals and perhaps even terrorists or governments whose intentions are malevolent. And therein lies the problem.

Let me begin the discussion of Internet vulnerabilities by showing you a video of what happened to the Internet when the Slammer Worm hit on January 25th of this year. On the monitor you can see a map of the world. Shading is used to differentiate between daytime and nighttime in the various geographics. The current time on this display is in the evening around 7 p.m. on January 23rd. On the monitor you will notice some red and yellow lines. A yellow line indicates a major Internet link that is experiencing a substantial degradation in performance. A red line indicates a link that is performing so poorly that it may well be unusable. It is normal to see a few such lines at any time on the Internet; the Internet is very large and it always has problems. This is one of the many displays that we use in our Cambridge Network Operations Command Center to diagnose the problems on the Internet.

I will now advance this display over a period of several days. You will see the sun move over the globe and you will see changes in Internet conditions as various problems occur and abate. Everything is normal until just after midnight on January 25th, when the Slammer Worm was released into the Internet. As you will see, the impact of Slammer was dramatic.

Akamai personnel first detected Slammer in Asia. Within minutes, Slammer had spread to hundreds of thousands of computers

worldwide, causing a serious disruption to Internet communications that lasted for days on some networks. Akamai's measurements indicate that in the hours following Slammer's outbreak, as much as 20 percent of all Web traffic was interrupted. It is estimated that Slammer caused well over $1 billion of economic damage.

Critical U.S. Government networks were also affected. In fact, the BGP churn, a measure of network health, on a key Defense network was among the highest of the thousands of networks that we monitor worldwide.

On the monitor you can see a plot of the churn caused by Slammer aggregated over the entire Internet. From left to right you will see time advance and the spike, of course, corresponds to the outbreak of Slammer. The pink or orange color denotes the churn on North American networks in the Internet, including Defense networks; the blue indicates the churn on Asian networks; and green denotes the churn on European networks. Of course, most of the networks are North American, and so you would expect to see a high churn in North America.

The damage caused by Slammer is fairly well known. In fact, Slammer was the subject of some excellent testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census last month. What may be less well known is that Slammer was a relatively benign worm in that it had no "payload." Slammer's only function was to replicate itself, and it was the mechanics of the replication that caused the damage. Had Slammer been specifically designed to cause damage, the outcome could have been far worse.

Slammer exploited a software bug that had been discovered 6 months earlier, one of the many such vulnerabilities that are discovered in Internet-based software each year. Other worms and viruses are more malevolent. In addition to using the infected computer as a host for self-replication, they also cause the computer to perform an Internet-based attack of some kind. For example, the Code Red virus released 2 years ago was specifically designed to attack the White House Web infrastructure. The recent Blaster worm was designed to attack Microsoft's Web infrastructure.

On the monitor I have displayed the initial outbreak and current activity of Code Red and Blaster. On the left-hand column and the top row you will see the outbreak of Code Red roughly 2 years ago. On the bottom left you see the outbreak of Blaster. On the right-hand side you will see the current activity of those viruses and, as you can see, both viruses are still active, although both the White House and Microsoft have taken steps to mitigate any damage they may cause.

In other cases, the virus or worm acts as a Trojan horse, leaving the infected computer in a vulnerable state that can be exploited later in a manner and at a time chosen by the attacker. In this way, an attacker can assemble an army of subverted computers from the comfort of his own home, perhaps in a foreign country. The attacker can then use the computer army to carry out an attack at will. Typically, the subverted computers reside in our homes and offices. It sounds strange, but the reality is that as we buy more powerful computers and provide them with better

connectivity to the Internet, for example broadband, we increase the power of the attacker to inflict damage upon us.

Even the world's largest Web presences cannot, by themselves, withstand a distributed denial of service attack, also known as a DDOS attack, from an army of thousands of subverted computers. As shown on the monitor, a typical Web site such as www.fbi.gov can process millions of bits of data per second. This shows normal use. Now we see what happens when the Web site is attacked by an army of subverted computers. The volume from a DDOS or distributed denial service attack can be 1,000 times as large as normal usage. Recently, Akamai has observed volumes of attack traffic exceeding 6 gigabits a second. That is 6 billion bits of data being dumped on the target every second. Needless to say, the Web site will crash along with the infrastructure around it.

Akamai's distributed network helps to mitigate such attacks by providing a shield for its customer's Web site. Instead of attacking a single location, with a distributed network architecture the army of subverted computers must now mount simultaneous attacks against thousands of servers in hundreds of locations. This is much harder to do. Moreover, the Akamai system has been designed to immediately recover from the loss of even large numbers of its servers, and so even if the attacker is successful in neutralizing some of our servers, Akamai still delivers the content from the Web site as if everything were running normally. This capability was proved during the recent war in Iraq, when the Akamai platform successfully thwarted several large-scale attacks that were mounted against key Government Web sites. It was also proved during the Slammer, Blaster, Code Red, and numerous other attacks, during which Akamai services operated normally.

As I noted earlier, critical Government networks are also vulnerable to Internet-based attacks. In part, this is because Government networks often use the same hardware and software as the rest of the Internet and several are connected to the Internet just like everyone else. Hence, as was seen with Slammer, they are often affected like everyone else.

Defending against Internet-based attacks can be difficult. For example, one defense against proliferation of viruses and worms on Government networks is to shut down all Web-based traffic on the network. Another defense is to disconnect the Government network from the rest of the Internet. Both defenses have the unfortunate side effect of cutting off access to thousands of Government Web sites from their daily users.

Many steps can be taken to help prevent attacks on Government networks and to mitigate their effect. Monitoring of virus activity, maintaining up-to-date software patches, and improving the security and consistency of firewalls would all be helpful. It could also make sense to remove public-facing Web sites from Government networks altogether. As can be seen on the monitor, as long as the public is invited into Government networks in order to access public Web sites it is difficult, if not impossible, to prevent unwanted access by attackers. Attackers come in just as the normal public does. By serving the content externally, however, the public no longer needs direct access to the Government network and it is much easier to filter out attack traffic.

The perpetrators of Slammer, Code Red, the original Blaster, and thousands of other Internet attacks have not been caught. That is because the Internet protocols make it very easy to mask one's identity, often by stealing that of another. For example, before a spammer releases his onslaught of unwanted e-mails into the Internet, the spammer will often hijack someone else's Internet identity and use that identity as the home base from which to send the spam. When investigators try to detect the source of the spam they are led to an innocent bystander.

On the Internet most anyone can impersonate most anyone else. Impersonation was never really contemplated when the Internet was designed and so no defenses were incorporated to prevent it. The implications go well beyond spam. For example, there are many ways for a thief to steal credit card numbers, personal passwords, and many other sensitive data that are commonly transmitted over the Internet. If a thief wants to learn the password to your online bank account, the thief simply directs your computer or your Internet service provider to send him or her all Web traffic destined for your bank. He can do this because it is relatively easy to trick your computer and/or the Internet into sending traffic to an unintended destination.

For example, one way of doing this is shown on the monitor. Displayed here is the normal operation of the Internet with end-users going to a Web server. They are directed to that Web server by the Border Gateway Protocol [BGP]. If we can see the next slide, we see what happens when a hacker or attacker wants to intercept that traffic. The hacker simply sends an electronic message to your ISP saying, "Please send me the traffic destined for the bank." Your ISP doesn't check that the hacker is not the bank, and will immediately comply and send all traffic destined for the bank to the hacker. Once the hacker receives that information, it will return to your browser a copy of the bank's Web site. You then will enter your passwords and your confidential information to get access to your account, but now it has gone to the hacker instead of the bank and nobody knows.

This phenomenon often happens by accident. Every day an ISP will accidentally claim the traffic for a Web site by accident, and part or all the Internet will send the traffic to the wrong location. This is known as black-holing. I know of a recent example where a major e-commerce site was black-holed by accident for 5 hours, costing millions of dollars in damages. Precise figures in the total amount of damage caused by e-crime annually are difficult to obtain, but data from the FBI's Internet Fraud Complaint Center indicates that this is a large and very rapidly growing problem.

It is truly remarkable that the Internet technology developed so many years ago has scaled so well and in so many unforeseen ways. But the time has now come to take a fresh look at the Internet's protocols and operating procedures, and to implement the changes that are necessary to make the Internet more secure.

The vulnerabilities that I have mentioned today represent just the tip of the proverbial iceberg. Many more are listed in my written testimony. The number I have talked about today is just limited by my time for this testimony, which is about to expire.

I would be happy to answer any questions you would have.

[The prepared statement of Mr. Leighton follows:]

Statement of Dr. F. Thomson Leighton

Chief Scientist, Akamai Technologies, Inc. ,
Professor of Applied Mathematics, MIT

Testimony before the
House Committee on Government Reform
U.S. House of Representatives

Hearing on "The State of Cyber Security in the United States Government"

October 16, 2003

Chairman Davis, Ranking Member Waxman, Subcommittee Chairman Putnam, Subcommittee Ranking Member Clay, and Members of the Committee, I appreciate the opportunity to testify this morning about one of my personal and professional passions – the Internet.

The Internet has been a focus of my work at the Massachusetts Institute of Technology, and also constitutes the basis for our creation of Akamai Technologies.

Akamai runs the world's largest distributed computing platform with more than 14,000 computer servers located in over 1,100 different networks and 70 countries. Like the Internet itself, Akamai evolved from what was originally an academic research project sponsored by the Defense Advanced Research Projects Agency (aka DARPA). Today, Akamai is a major commercial enterprise that delivers a substantial portion of all Web traffic. Using sophisticated mathematical methods and algorithms to coordinate the operation of thousands of Web servers across the Internet, Akamai distributes content and applications from thousands of Web sites to hundreds of millions of consumers worldwide. We serve each of you every day. Over 70 of the businesses on the Fortune 500 utilize the Akamai platform to distribute their content and applications reliably, securely, and efficiently, as do the Departments of Defense, Education, and Homeland Security, as well as the FBI, the Internal Revenue Service, the Centers for Disease Control and Prevention, the U.S. Geological Survey, the Supreme Court, and many other Federal, state and local government organizations.

As part of our services, Akamai provides the most extensive, real-time worldwide view of Internet traffic and conditions, a glimpse of which we will see this morning. One of our central missions at Akamai is to enable Enterprises and Government Agencies to understand and manage the many vulnerabilities and problems associated with using the Internet.

At Akamai, we understand the power and potential of the Internet. Hundreds of millions of people use the Internet on a daily basis to send E-mail, search for information, pay a bill, buy a book, get the news, make a reservation, download music, run a business, or just to chat with a friend. Trillions of dollars of E-commerce are conducted over the Internet annually. The Internet is also used to manage critical national infrastructure in sectors such as transportation, banking, manufacturing, utilities, and defense.

The Internet is truly a communications phenomenon that is transforming the way people work, live, derive entertainment and communicate all over the world. It embraces fundamental notions of individual choice and freedom that are hallmarks of our American society.

Unfortunately, the power of the Internet can be exploited for evil as well as good, a phenomenon that is not atypical for such a great advance in technology. And, for reasons that I will describe shortly, the Internet is particularly vulnerable to the exploits of those with malevolent intentions.

As you know, we have already witnessed events wherein a single individual has been able to disrupt Internet communications on a widespread basis, thereby causing billions of dollars in economic damage. Less well understood is the fact that information being transmitted on the Internet can also be rerouted, stolen and manipulated with relative ease. The consequences of such vulnerabilities are becoming increasingly dangerous as our dependence on the Internet grows.

Internet and software security are talked about much, but understood little. Today, I will spend a few minutes talking about how the Internet works and why it is vulnerable.

The Internet Architecture

Many people think of the Internet as a single network. This is a misconception. In fact, the Internet consists of over 15,000 separate networks spread across most every nation in the world. The wires and fibers in these networks are interconnected in a somewhat haphazard fashion by millions of switches known as routers. There was no central architect who decided how or where the 15,000 networks should be connected to one another and there is no central command center to govern the minute-by-minute or even month-by-month operations of the Internet.

The glue that holds the Internet together and that allows it to function are the protocols such as the Border Gateway Protocol (aka BGP) that are used to route packets of data from one network to another, the services such as the Domain Name System (aka DNS) that are used to identify the correct destination for traffic on the Internet, and the myriad software packages used to support such diverse tasks as email, web browsing, file sharing, and instant messaging. All of the software and protocols have flaws that can be exploited by an attacker. Thousands of new flaws were discovered in just the last year.

For the most part, the protocols used in the Internet today are very similar to those that were developed over twenty years ago when the Internet was first invented. Back then, the Internet was known as the DARPANet and it was used by only a small number of researchers in a few locations.

The original Internet protocols were based on a foundation of trust. It was assumed that the users of the Internet would use the Internet for the purposes for which it was intended and that they would do nothing to harm either the infrastructure or other users, either intentionally or even by accident. There was a strong sense of community in which an individual user would not take actions to the detriment of the common good, even if such actions would directly benefit the individual.

While such noble assumptions were fairly safe in the collegial environment of the DARPANet of twenty years ago, they are clearly not valid in the Internet of today, where there are many individuals and perhaps even terrorists or governments whose intentions are malevolent. And therein lies the problem.

Viruses and Worms

Let me begin the discussion of Internet vulnerabilities by showing you a video of what happened to the Internet when the Slammer Worm hit on January 25th of this year.

[REFER TO VISUAL #1]

On the monitor, you can see a map of the world. Shading is used to differentiate between daytime and nighttime in the various geographies. The current time on this display is roughly 7:00 p.m. on January 23rd. As I advance the display over time, you will also notice some red and yellow lines. A yellow line indicates a major Internet link that is experiencing a substantial degradation in performance. A red line indicates a link that is performing so poorly that it may well be unusable. It is normal to see a few such lines at any time on the Internet. This is one of many displays that we use in our Cambridge Network Operations Command Center to diagnose problems with the Internet.

I will now advance the display over a period of several days. You will see the sun move over the globe and you will see changes in Internet conditions as various problems occur and abate. Everything is normal until just after midnight on January 25th, when the Slammer Worm was released into the Internet. As you will see, the impact of Slammer on the Internet was dramatic.

[REFER TO VISUAL #2]

Akamai personnel first detected Slammer in Asia. Within minutes, Slammer had spread to hundreds of thousands of computers worldwide, causing a serious disruption to Internet communications that lasted for days on some networks. Akamai's measurements indicate that in the hours following Slammer's outbreak, as much as 20% of all Web traffic was interrupted. It is estimated (CNET, January 31, 2003) that Slammer caused over one billion dollars of economic damage.

Critical US Government networks were also affected. In fact, the BGP churn (a measure of network health) on a key Defense network was among the highest of the thousands of networks that we monitor worldwide.

[REFER TO VISUAL #3]

On the monitor, you can now see a plot of the churn caused by Slammer aggregated over the entire Internet. The spike, of course, coincides with Slammer's release into the Internet.

The damage caused by Slammer is fairly well known. In fact, Slammer was the subject of some excellent testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census last month. What may be less well known is that Slammer was a relatively benign worm in that it had no "payload." Slammer's only function was to replicate itself and it was the mechanics of the replication that caused the damage. Had Slammer been specifically designed to cause damage, the outcome could have been far worse.

Slammer exploited a software bug that had been discovered 6 months earlier, one of thousands of such vulnerabilities that are discovered in Internet-based software each year.

Other worms and viruses are more malevolent. In addition to using the infected computer as a host for self-replication, they also cause the computer to perform an Internet-based attack of some kind. For example, the Code Red virus released two years ago was designed to attack the White House web infrastructure. The recent Blaster worm was designed to attack Microsoft's web infrastructure.

[REFER TO VISUAL #4]

As you can see on the monitor, both viruses are still spreading, although both the White House and Microsoft have taken steps to mitigate any further damage that they may cause.

In other cases, the virus or worm acts as a Trojan horse, leaving the infected computer in a vulnerable state that can be exploited later in a manner and at a time chosen by the attacker. In this way, an attacker can assemble an army of subverted computers from the comfort of his own home, perhaps in a foreign country. The attacker can then use the computer army to carry out an attack at will. Typically the subverted computers reside in our homes and offices. It sounds strange, but the reality is that, as we buy more powerful computers and provide them with better connectivity to the Internet (e.g., broadband), we increase the power of the attacker to inflict damage.

Distributed Attacks vs. Centralized Infrastructure

Even the world's largest web presences cannot, by themselves, withstand a distributed denial of service (aka DDOS) attack from an army of thousands of subverted computers.

[REFER TO VISUAL #5]

As shown on the monitor, a typical web site such as www.fbi.gov can process millions of bits of data per second.

[REFER TO VISUAL #6]

But, the volume of data from a DDOS attack can be 1000 times as large. Recently, Akamai has observed volumes of attack traffic exceeding 6 Gigabits per second. That is 6 billion bits of data being dumped on the target every second.

Akamai's distributed network helps to mitigate such attacks by providing a shield for its customer's web site.

[REFER TO VISUAL #7]

Instead of attacking a single location, with a distributed network architecture the army must now mount simultaneous attacks against thousands of servers in hundreds of locations. This is much harder to do. Moreover, the Akamai system has been designed to immediately recover from the loss of even large numbers of its servers and so even if the attacker is successful in neutralizing some of our servers, Akamai still delivers the content from the web site as if everything were running normally.

[REFER TO VISUAL #8]

This capability was proved during the recent war in Iraq when the Akamai platform successfully thwarted several large-scale attacks that were mounted against key Government web sites. It was also proved during the Slammer, Blaster, Code Red and numerous other attacks, during which Akamai services operated normally.

Impact on Government Networks

As I noted earlier, critical Government networks are also vulnerable to Internet-based attacks. In part, this is because Government networks often use the same hardware and software as the rest of the Internet and several are connected to the Internet just like everyone else. Hence, as was seen with Slammer, they are often affected like everyone else.

Defending against Internet-based attacks can be difficult. For example, one defense against proliferation of viruses and worms on Government networks is to shut down all Web-based traffic on the network. This has the unfortunate side effect of cutting off access to thousands of Government web sites from their users.

Many steps can be taken to help prevent attacks on Government networks and to mitigate their effect. Monitoring of virus activity, maintaining up-to-date software patches, improving security and consistency of firewalls would all be helpful. It could also make sense to remove public-facing web sites from Government networks altogether.

[REFER TO VISUAL #9]

As can be seen on the monitor, as long as the public is invited into Government networks in order to access web sites, it is difficult, if not impossible to prevent unwanted access by attackers.

[REFER TO VISUAL #10]

By serving the content externally, the public no longer needs direct access to the Government network and it is much easier to filter out attack traffic.

Internet Theft

The perpetrators of Slammer, Code Red, the original Blaster, and thousands of other Internet attacks have not been caught. That is because the Internet protocols make it very easy to mask one's identity, often by stealing that of another. For example, before a spammer releases its onslaught of unwanted emails into the Internet, the spammer will often hijack someone else's Internet identity and use that identity as the home base from which to send the spam. When investigators try to detect the source of the spam, they are led to an innocent bystander.

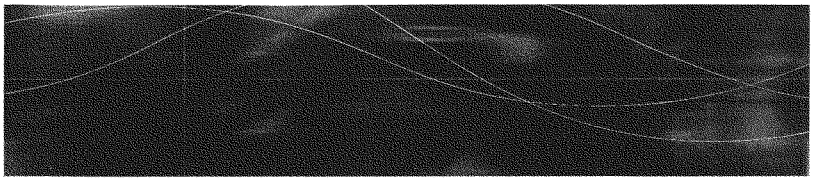
On the Internet, most anyone can impersonate most anyone else. Impersonation was never really contemplated when the Internet was designed, and so no defenses were incorporated to prevent it. The implications go well beyond spam. For example, there are many ways for a thief to steal credit card numbers, personal passwords, and many other sensitive data that are commonly transmitted over the Internet. If a thief wants to learn the password to your on-line bank account, the thief simply directs your computer or your Internet Service Provider (ISP) to send him or her all Web traffic destined for your bank. He can do this because it is relatively easy to trick your computer and/or the Internet into sending traffic to an unintended destination. When your browser contacts the thief instead of your bank, the thief responds by showing you the regular bank web pages that ultimately invite you to sign in with your password. You oblige and the thief can now access your bank account without your knowledge and without fear of detection. Precise figures on the amount of damage caused by E-crime annually are difficult to obtain, but data from the FBI's Internet fraud Complaint Center indicates that it is a large and rapidly growing problem.

Summary

It is truly remarkable that the Internet technology developed so many years ago has scaled so well and in so many unforeseen ways. But the time has now come to take a fresh look at the Internet's protocols and operating procedures, and to implement the changes that are necessary to make the Internet more secure.

The vulnerabilities that I have mentioned today represent just the tip of the proverbial iceberg (see Appendix A). Their number was limited only by the time allotted for this testimony, which I see is about to expire.

I would be happy to answer any questions that you may have.



Internet Vulnerabilities

Appendix A to Testimony Before
The House Committee on Government Reform
U.S. House of Representatives
October 16, 2003

Akamai

Internet Vulnerabilities

The Internet has grown over several decades from what was initially a research project in transporting information into a large-scale distribution mechanism for worldwide commercial enterprise. While the Internet operates smoothly under typical circumstances, it relies upon a number of complex mechanisms to work effectively. These mechanisms, implemented on millions of machines over the thousands of individual networks comprising the Internet, present numerous vulnerabilities that pose a threat to all services and operations performed online. This document intends to outline the most significant vulnerabilities that exist today, and explains how Akamai helps address these issues to enable a reliable, secure Internet – The Business Internet.

> "Even organizations that have deployed a wide range of security technologies can fall victim to significant losses."
> – The 2003 CSI/FBI Computer Crime and Security Survey

> "...a major national attack is not going to go after one company, it's going to go after the thing that all companies use and depend on -- the Internet itself."
> – Richard Clarke[i]

Outside of traditional commercial enterprise, the Internet's advantageous economies offer increased efficiency and ease for a variety of industries and agencies. Every agency uses the Internet in some way, and many rely on it for critical communications. Financial organizations transact electronically, energy corporations manage systems remotely – transportations systems, suppliers, international diplomacy, intelligence communications, and most every other critical component of the global economy benefits from the Internet. Being interdependent, such systems alone possess numerous vulnerabilities, but their use of the Internet requires growing vigilance over Internet threats. To worsen matters, first responders require the Internet and other telecommunications systems to respond effectively to any incident,[ii] making cyberattacks a potentially crippling new weapon against US interests.[iii]

Internet Architecture: History and Evolution of Threats

The Internet's vulnerabilities stem from its origin and evolution. Originally intended as a research project, the Internet arose out of standards developed for network communications. Driven by theoretical research, the underlying mechanisms were designed extremely well for the task at hand – getting data from one place to another over an electronic medium. As with many research projects, though, the protocols and architecture of the Internet did not reflect the eventual implemented scale and situations. The architecture thus reflects a mechanism that was well designed, but designed around intrinsic trust between communicating parties and systems.

The scale and diversity of Internet equipment, systems, implementations, and traffic has escalated immensely, resulting in a conglomeration of systems that has been able to operate extremely effectively based upon the original research efforts. Although the growth of the Internet and testing methods enabled the systems to scale as needed, numerous new methods have been invented and discovered by hackers to exploit almost every system imaginable. With each new threat comes an almost immediate solution, but the cost of change for many attack vectors or basic vulnerabilities remains insurmountable to address.[iv]

New standards pave the way for future security of this critical set of technologies, but this remains a challenge as well. This document intends to portray the most critical areas of vulnerability across the Internet, with an emphasis on different incidents and their impact.

DNS

The Domain Name System provides a mechanism to translate a hostname into an IP address, and is required for users to run most services online. Operating in real-time, the service operates through interactions between a client's operating system component, the resolver, and DNS servers, or nameservers, spread across the Internet.

At the highest level, there are several Internet locations that provide top-level DNS services, and act as the ultimate authority and the initial starting point for other nameservers. These top-level nameservers are subject to attack, and if compromised, would disable the availability of any Web site, mail server, and much more, simply because users could not locate the IP addresses of these services. As DNS is the directory lookup of the Internet, a serious attack could make all services impossible to find.[v]

Other nameserver locations are not necessarily top-level, but provide local services for a wide range of users. For example, many countries and large ISPs utilize a fixed set of servers to handle DNS requests on behalf of any downstream traffic. An attack to such a system would render a large portion of the Internet with the same level of service availability issues as an attack to the top-levels.

DNS's communication mechanisms also suffer from a lack of security. There is no authentication between sources of data, leading to exploits whereby false information is injected into the system. This could be used to hijack traffic intended for a legitimate resource, such as a Web site or email server, or could be used to simply disrupt traffic. In either case, it represents a rather simple way to reroute traffic from where it should be going.

Implementations of both nameservers and resolvers are prone to numerous bugs.[vi] Such bugs can cause an outage to DNS services for a portion of the Internet, or cause a client to be unable to access correct DNS information intermittently. Since DNS is not error-free, many services cannot function with the utmost reliability that is required of them.

Lastly, an organization's DNS information is housed in one, or a set of, authoritative nameservers. As the information present in DNS is a necessary preliminary for any communications with an organization, malicious entities often attack DNS servers at an organization, disrupting availability with even a moderately small or simple attack.[vii] This solidifies the real risks inherent in DNS for the Internet.

While DNS provides critical services that the Internet requires to operate effectively, it is subject to attack on its core components, attacks targeted at an organization's architecture, corruption of data, or unreliability due to implementation differences and bugs.

The Routing Infrastructure

The Internet relies on the capability of directing traffic between different locations across physical connections and between individual network providers. This functionality is implemented by pieces of hardware equipment and a variety of protocols, each with a high level of variation and configurability.

This level of configuration allows for human error to affect connectivity between parts of the Internet. Many issues over several years of the Internet's operation have resulted because of misconfiguration of equipment, typically causing outages for organizations or networks, and

occasionally to the Internet as a whole.[viii] When such configuration issues arise, there is no easy way to prevent a recurrence – as human error will never be fully avoidable.[ix]

BGP, Border Gateway Protocol, enables the core connectivity on the Internet, allowing different networks to identify what other networks to use in order to transport a payload of data to its destination. BGP ignores key elements affecting reliable communications – latency, reliability, congestion, and much more – and only identifies which networks are connected to each other. With limited data, BGP cannot provide optimal delivery across the Internet, and often is the cause of serious performance and connectivity issues.[x]

BGP also suffers from more severe vulnerabilities, such as the lack of any reporting or security. A malicious entity can compromise one of over one hundred thousand devices currently using BGP, and force some or all Internet traffic to be diverted to another location. While this can cause an outage, it can also be used to steal information, including financial, personal, or other extremely sensitive data.[xi] Efforts are under way to secure particular implementations of BGP and networks, but this will take an immense amount of effort and cost, and will never reach full security of the BGP protocol.[xii]

The connectivity between different networks is not only subject to electronic issues, but due to the inherent economics of telecommunications online. For networks to exist on the Internet, they must share traffic, but they do not wish to make other networks perform better than their own. Due to this reason, many incidents have forced connectivity and reliability issues between individual spots on the Internet.[xiii] With this conflict present in all Internet communications, it will remain difficult to fully optimize the Internet.

Lastly, it is easy for an attacker to cripple these critical components of the Internet. With several types of attack methods available, one could disrupt connectivity on a wide scale by attacking core routers.[xiv] It often takes several minutes for routers to return online, and a large number of changes in the routing structure causes enough computational strain on equipment that this alone can cause widespread problems. Certain large-scale network outages and router-impacting worms caused such issues, affecting the Internet as a whole in an extremely negative manner.[xv]

The core aspect of data transport on the Internet, routing, is subject to several significant vulnerabilities and weaknesses, including human error, ignorance of key information, a lack of security around data, computational scalability, single points of failure, and the economic conflicts between carriers.

Client & Server Exploits

The key elements that derive value from the Internet are end users and organizations providing service online. Clients and servers use a variety of tools to connect to the Internet and communicate, but suffer from vulnerabilities on any number of implementations and components required to operate.

A variety of exploit paths exist from which to steal data from, break, or otherwise infect particular systems. Many exploits are centered around specific operating systems, hardware equipment, or vendor implementations. Others leverage specific traits of protocols, development and communication languages, and types of servers. While the volume of potential exploits is even larger than the number of exploitable systems, it remains a fact that most any system is subject to exploit.

Many worm and virus outbreaks targeted clients, infecting end user machines in a rapid manner. Some use email, while other directly attack exposed ports, and many use multiple delivery

mechanisms.[xvi] In all cases the incidents generated an increased fear in the consumer marketplace, and an increase in the perceived risk of using online services.

More severe worm and virus outbreaks affected servers operating services. This caused not only large availability issues,[xvii] but created a much-heightened user fear due to the security implications involved. Most users would accept that their equipment may not be adequately secure, but all expect their service providers to have invested a fair level of effort securing services. Failure of those efforts implies that security online is much worse than most in the community realize.

Even more severe, such exploits often do not result in a worm or virus, but the implanting of an agent. Once a system is compromised, especially if it is very covertly performed, the system can be later used to launch attacks on critical services or portions of the Internet.[xviii] Most distributed denial of service attacks arise from machines thus exploited, and represent a future uncertainty that could effect crippling blows to the Internet as a whole.

Many forms of exploits exist to compromise systems, be they users accessing services or the servers servicing requests. Any such exploits result in reduced online consumer confidence, and work to revert the progress of the Internet towards viability as a true business tool.

Denial of Service

Direct attack, with the sole intent of taking down infrastructure, is extremely effective at interrupting service. Using sophisticated methods, hackers have developed a variety of methods to generate such attacks, and have created a real risk to the security of online services and the Internet in general.

Basic denial of service attacks can be performed by the average teenager by downloading small tools off of the Web. While very simple, these attacks operate by flooding a link connecting infrastructure to the Internet – effectively blocking any outbound data transmission, and denying service to legitimate visitors.

Many such attacks are now performed in a distributed manner, whereby multiple compromised systems are instructed to deliver a massive surge in traffic from all points on the Internet. This can not only deny service for an enterprise-class Web site, but can cause entire datacenter connectivity outages, affecting multiple organizations. Sophisticated attackers could compromise the entire Internet, as well, by targeting such attacked at core services – either routers, DNS servers, or other core components.

DoS attacks are thus a very effective and highly dangerous mechanism of attack and, although not too many organizations have been affected by these types of attacks, they will continue in both frequency and strength.[xix]

Akamai's Ability to Help

Akamai operates a massively distributed infrastructure that provides organizations with the flexibility to extend their architecture, delivery services, and control across the entire breadth of the Internet. This platform provides two key benefits when considered in relation to the vulnerabilities of the Internet: the ability to understand what vulnerabilities exist and are being exploited, and the power to protect a variety of services from being affected.

Akamai provides a distributed, redundant authoritative DNS service, Enhanced DNS, that provides a resilient way for organizations to protect their DNS services from attack. Utilizing IP anycasting, the top-level DNS servers used by Akamai are located in numerous physical and network locations that cannot be easily identified by an attacker. Akamai's distributed presence, currently numbering over 2,400 datacenters on over 1100 networks, allows a very thorough vantage point into any localized attempts to hijack, spoof, or poison a client's DNS information. Lastly, although Akamai cannot protect the current top-level DNS infrastructure, it can report on its availability and performance from across the globe, both under normal operations and when systems are under attack.

Akamai's distributed architecture enables customers to bypass a lot of the problems with BGP and other routing mechanisms. Firstly, by delivering Web sites, applications, and services from the end user's ISP, Akamai effectively bypasses the need to leverage BGP. For any information that must traverse the Internet to centralized facilities, Akamai utilizes an innovative technology called SureRoute to bypass any connectivity disruptions via an objective view of true performance. Additionally, Akamai receives hundreds of BGP feeds from partners around the globe, and can monitor the state of BGP in distant regions of the Internet to determine if any misconfigurations or malicious individuals are causing connectivity disruptions or BGP security exploits. Lastly, Akamai's insight into the topology of the Internet enables it to identify the key routers, NAPs, and gateways that exist as key resources, but also as key vulnerabilities, both physically and topologically, to global Internet functionality.

The Akamai network can act as a shield against various types of worm and viral attacks, cloaking a customer's infrastructure from direct accessibility. For viruses such as Code Red, Nimda, and SQL Slammer, the malicious code attacked random IP addresses – but Akamai blocks transmission of such requests because they are not well-formed HTTP/S requests. This enabled customers delivering their site through Akamai to prevent infection of their systems. Secondarily, Akamai continues to support the largest antivirus and software download corporations in their efforts to distribute patches and virus updates when issues arise. Akamai has also set up a distributed detection mechanism that monitors for different types of exploits, and can help establish an early warning feed to identify new attacks and their vectors of distribution.

Akamai acts as a scalable shield to a Web infrastructure, protecting against denial of service attacks intended to saturate resources. Be they targeted against a Web, DNS, or application infrastructure, Akamai's distributed resilient presence deflects and absorbs such attacks.

Summary

While the Internet remains an uncertain place,[xx] many vulnerabilities can be addressed through innovative uses of a distributed platform. Akamai Technologies provides services to help cope with such challenges, and can be a crucial partner in making the Internet a predictable, and ultimately profitable, business platform – the Business Internet.

More generally, the Internet suffers from evolving standards and threats, coupled with a cost-prohibitive means of securing critical components. These threats are often poorly understood and ignored, and the vast majority of organizations outside of the public sector lag in realizing secure infrastructures. Industries and agencies need to realize the reality and risk of such threats, and take active steps to addressing not only individual security vulnerabilities, but the breadth of risks that can interfere with critical operations. Without such steps, the Internet remains a usable, but vulnerable platform to act as the foundation for the global economy.

[i] "Looking at Vulnerability Issues in Addressing Cyber Security." Remarks by Richard Clarke, Special Advisor to the President for Cyberspace Security, before the Business Session of the President's National Security Telecommunications Advisory Committee (NSTAC), Washington, D.C., March 13, 2002.

[ii] Fire departments, police departments, public health labs, and most cities do not even have sufficient equipment to handle major catastrophes, while they are called on as the first to respond to any incidents and are critical in saving lives. (Clarke, Richard A.; Metzl, Jamie F.; Rudman, Warren B. "Emergency Responders: Drastically Underfunded, Dangerously Unprepared," Report of an Independent Task Force Sponsored by the Council on Foreign Relations, 2003)

[iii] Several examples of serious incidents include the shutdown of a Chinese communications satellite, the shutdown of a nuclear power plant monitoring system by the Slammer worm, and the potential that British hacker attacks performed against Korea through compromised US Defense machines would be seen as an act of war. (1999 Report of the Special Senate Committee on Security and Intelligence chaired by the Honourable William M. Kelly, Canada) (Poulsen, Kevin. "Slammer work crashed Ohio nuke plant network," SecurityFocus, Aug 2003) ("Hacker Pair Illustrates Pentagon's Vulnerability," USA Today, March 23, 1996; "How Datastream Cowboy Took U.S. to the Brink of War," The Toronto Star, April 12, 1998)

[iv] According to Symantec, approximately 250 new software vulnerabilities are discovered each month – and between 400 and 500 new viruses emerge. ("Battling the net security threat," BBC News online, November 7, 2002)

[v] A rudimentary attack against the top-level nameservers in October 2002 highlighted the need for more security around these services. While the attack didn't cause a global outage, 9 of the 13 nameservers were down as a result – if all 13 were down, the Internet would have experienced serious problems. (Lemos, Robert. "Net attack flops, but threat persists," CNET News.com, October 23, 2002)

[vi] Multiple Linux resolver implementations are susceptible to buffer overflow attacks, enabling execution of arbitrary code on the compromised machine. (Caldera International, Inc. Security Advisory CSSA-2002-034)

[vii] Microsoft experienced availability issues when its DNS was attacked in January 2001. (Bekker, Scott. "Microsoft Taps Akamai for DNS Backup System," ENT News, January 29, 2001)

[viii] In 1997, a major provider misconfigured a router and caused global connectivity disruptions for up to two hours. (Vamosi, Robert. "Router security hole threatens Web," CNET News.com, March 3, 2003)

[ix] The researchers of a study estimate that between 200-1200, or 0.2%-1.0% of BGP prefixes, are misconfigured every day. This misconfiguration in many cases showed at least a 10% increase in route update load, but in several cases doubled the load. BGP misconfigurations can cause connectivity disruption, either globally or locally, in 13% of misconfigurations. While half of incidents were corrected in 10 minutes, 80% were corrected in an hour, and 95% within 10 hours. Those causing connectivity disruption, however, are fixed within an hour 95% of the time. The potential to announce IP space not belonging to one's AS is "a major security flaw." (Anderson, Tom; Mahajan, Ratul; and Wetherall, David. "Understanding BGP Misconfiguration," from SIGCOMM '02, Copyright ACM: 2002)

[x] BGP takes, on average, 3 minutes to failover to an alternate path, and such failover paths can cause traffic to be sent around the world or exhibit other strange characteristics. "Mission critical systems can not use Internet as the underlying communications medium." (Cheriton, David; Gritter, Mark; and Zhu, Dapeng. "Feedback Based Routing." Computer Science Department, Stanford University, work in progress as of Aug 03)

[redacted]

[xi] Security consultants are warning that BGP has many security holes, and must be addressed. According to Stephen Dugan, a security expert speaking at the Black Hat Security Briefing, said "We need to develop the technology before someone attacks the system." (Vamosi, Robert. "Router security hole threatens Web," CNET News.com, March 3, 2003)

[xii] BGP has several serious security risks – and many can be patched, but must be done so on vendor implementations, specific networks, and there will continue to be issues with BGP security as a result of ongoing bugs and those who do not pay attention to the risks. (Convery, Sean, and Franz, Matthew. "BGP Vulnerability Testing: Separating Fact from FUD." NANOG 28 – June 2003)

[xiii] Cable & Wireless and PSINet stopped exchanging traffic for a period of time that preventing communications between either network. Although either could still communicate with the rest of the Internet, it was not possible to communicate from PSINet to Cable & Wireless, or vice versa. (Borland, John. "Net blackout marks Web's Achilles heel," CNET News.com, June 6, 2001)

[xiv] The Internet breaks down when BGP stops working – "A single BGP router can shut down the entire Internet." (Cheriton, David; Gritter, Mark; and Zhu, Dapeng. "Feedback Based Routing." Computer Science Department, Stanford University, work in progress as of Aug 03)

[xv] The Slammer worm, which crippled routers because of its transportation mechanism, caused approximately $1B in damages. (Lemos, Robert. "Counting the cost of Slammer," CNET News.com, January 31, 2003)

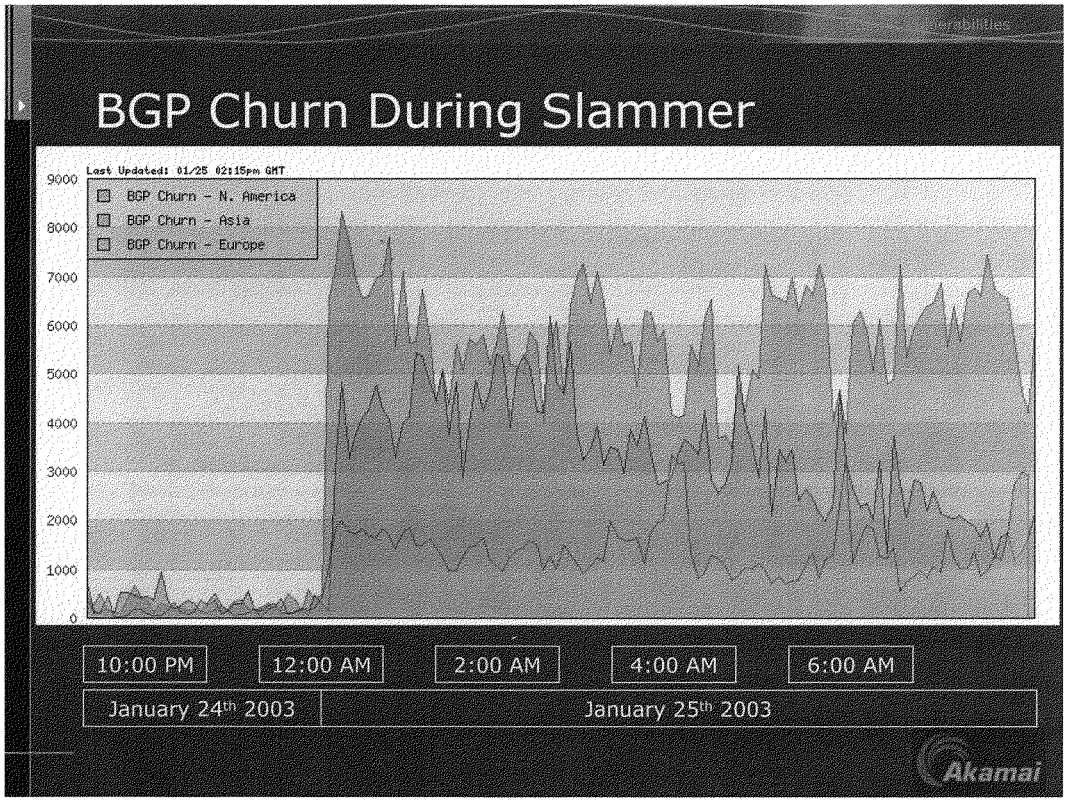
[xvi] Nimda propagated through multiple delivery mechanisms – email, network sharing, exploits of servers, and browsing of exploited Web sites. (CERT Advisory CA-2001-26 – Nimda Worm)

[xvii] The SQL Slammer worm caused global connectivity disruptions, simply because of its method of spreading – not because of the systems it infected. (Boutin, Paul, "Slammed!" Wired Magazine, Issue 11.07, July 2003)

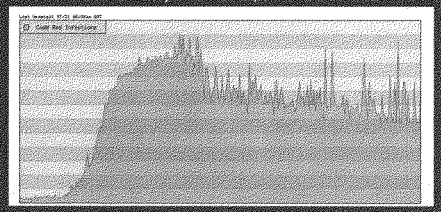
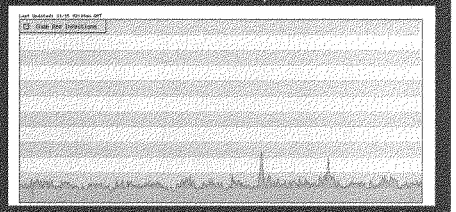
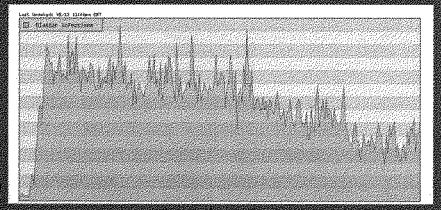
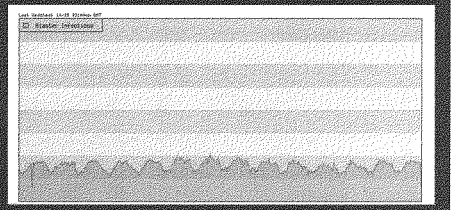
[xviii] NIPC identifies that multiple DDoS attacks are occurring by leveraging fragmented UDP transmissions to bypass traditional filtering mechanisms, and come from a distributed set of agents. They have also made available a tool to scan a system to determine if an agent has been installed on it. (NIPC Advisory 01-012. "Ongoing DDoS Disruption Attempts," 5/5/2001)

[xix] 42% of respondents indicated that they were hit by denial of service attacks in the past 12 months. The average cost of a denial of service attack across many separate incidents was $1.427M, up from $297,000 in 2002 – but ranged from $500 to $60M. Respondents were from High-Tech, Financial, Manufacturing, Medical, Federal Government, Education, State Government, Telecom, Utilities, Retail, Local Government, Legal, and Transportation sectors, in order of relative percentage, and represented 530 computer security practitioners. (Richardson, Robert. "The 2003 CSI/FBI Computer Crime and Security Survey." Computer Security Institute: 2003)

[xx] "So there are vulnerabilities in the very mechanisms of the Internet. The Domain Name Servers, the Border Gateway Protocols [BGPs], the things that make the Internet work are not secure. They could be hit by a denial of service attack, as we talked about last year. They could be hit by a corruption of the look-up tables, the address space, very easy to do." ("Looking at Vulnerability Issues in Addressing Cyber Security." Remarks by Richard Clarke, Special Advisor to the President for Cyberspace Security, before the Business Session of the President's National Security Telecommunications Advisory Committee (NSTAC), Washington, D.C., March 13, 2002)

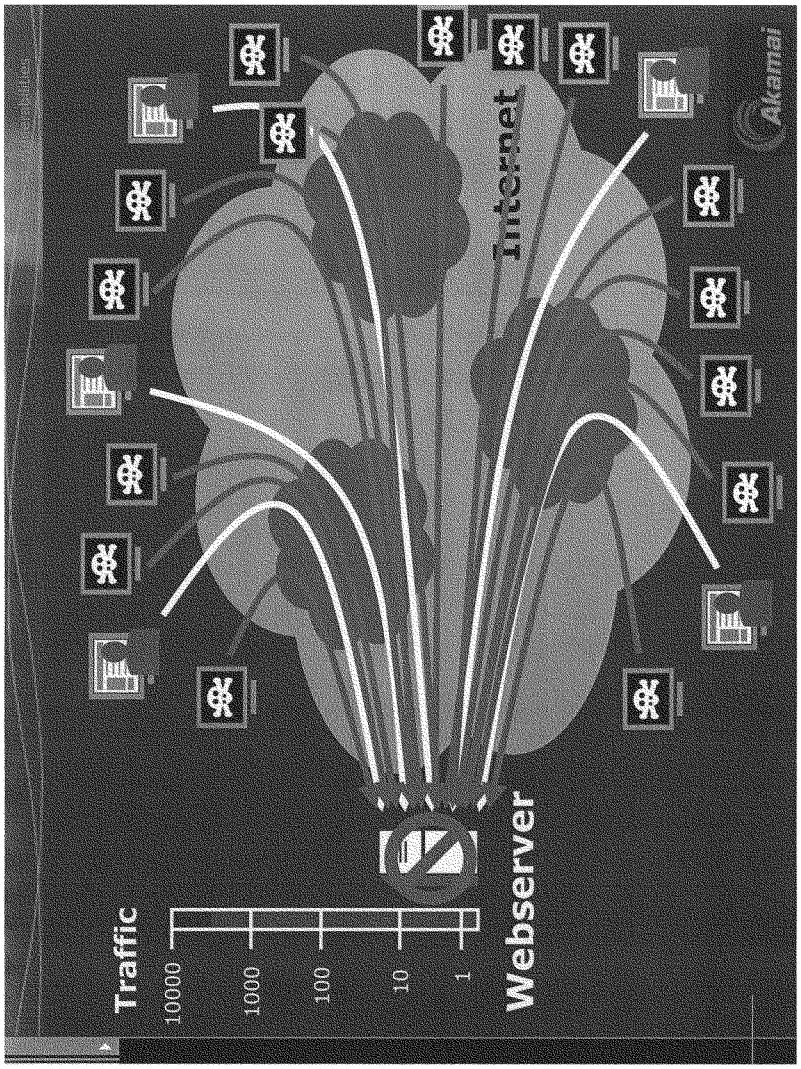

BGP Churn During Slammer
Last Updated: 01/25 02:15pm GMT
BGP Churn - N. America
BGP Churn - Asia
BGP Churn - Europe
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
10:00 PM
12:00 AM
2:00 AM
4:00 AM
6:00 AM
January 24th 2003
January 25th 2003
Akamai

Virus Activity

	Breakout - 2 day period	Current – 2 week period
	July 19th – 21st, 2001	October 1st – 14th, 2003
CodeRed v2		
	August 11th – 13th, 2003	October 1st – 14th, 2003
Blaster		

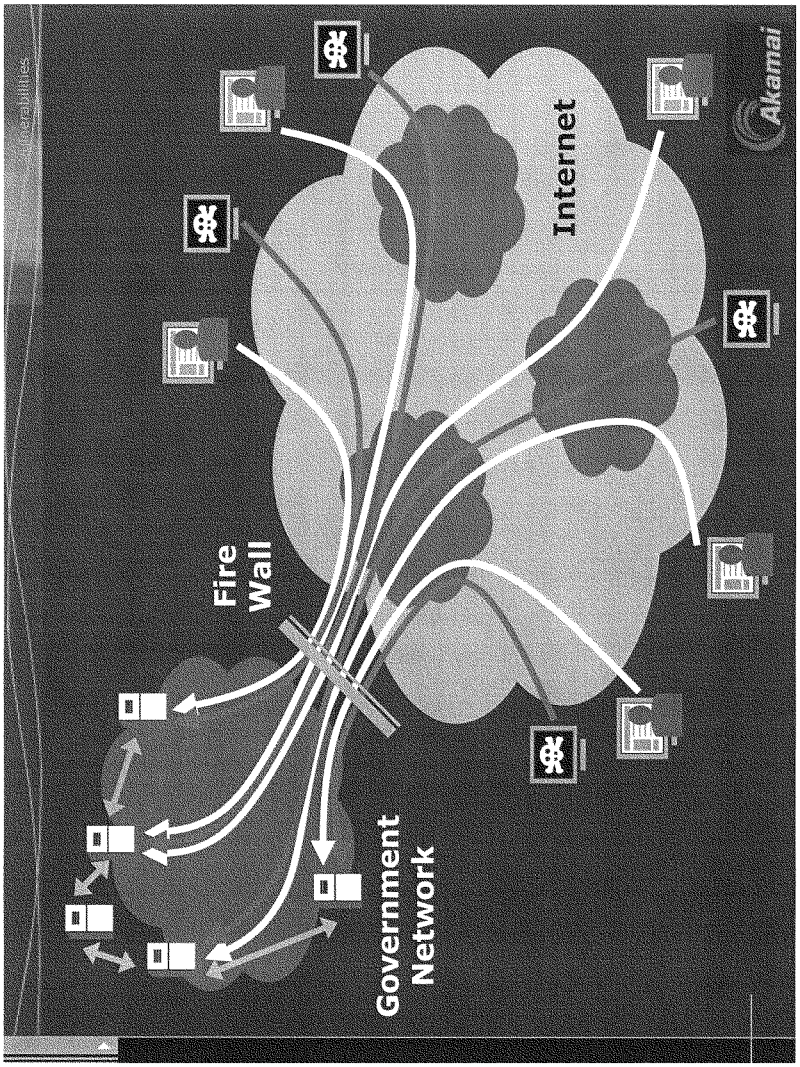
Akamai

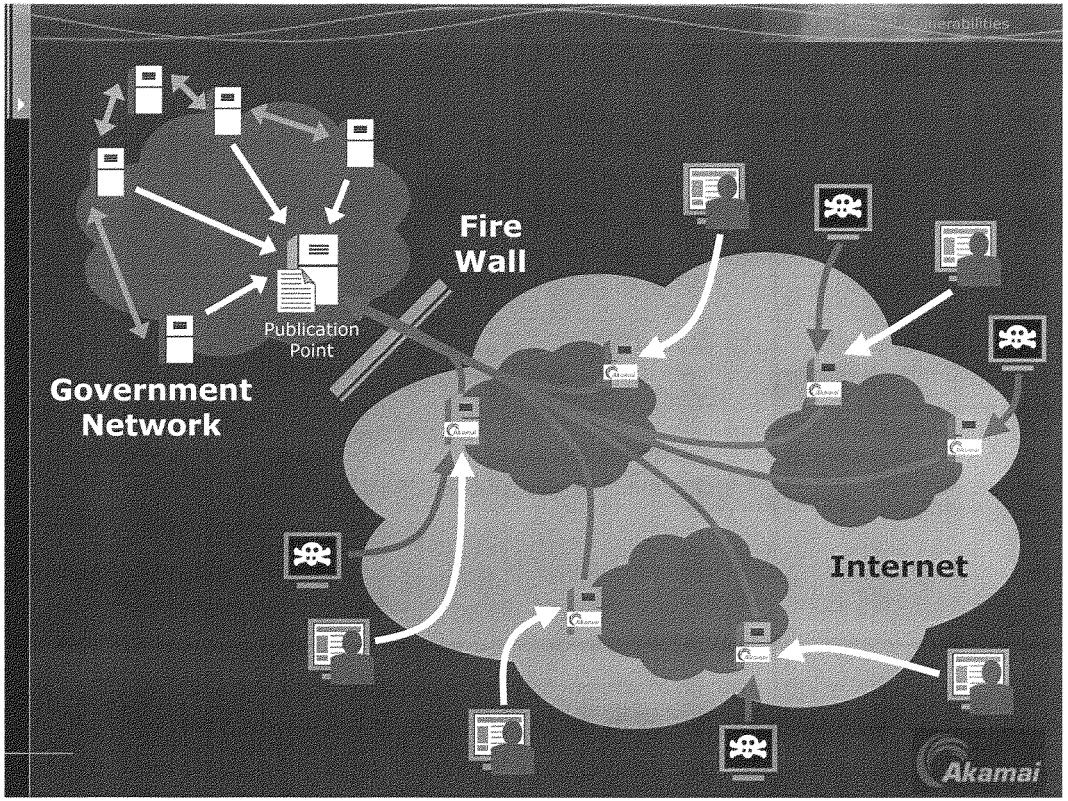
Traffic
10000
1000
100
10
1
Webserver
Internet
Akamai

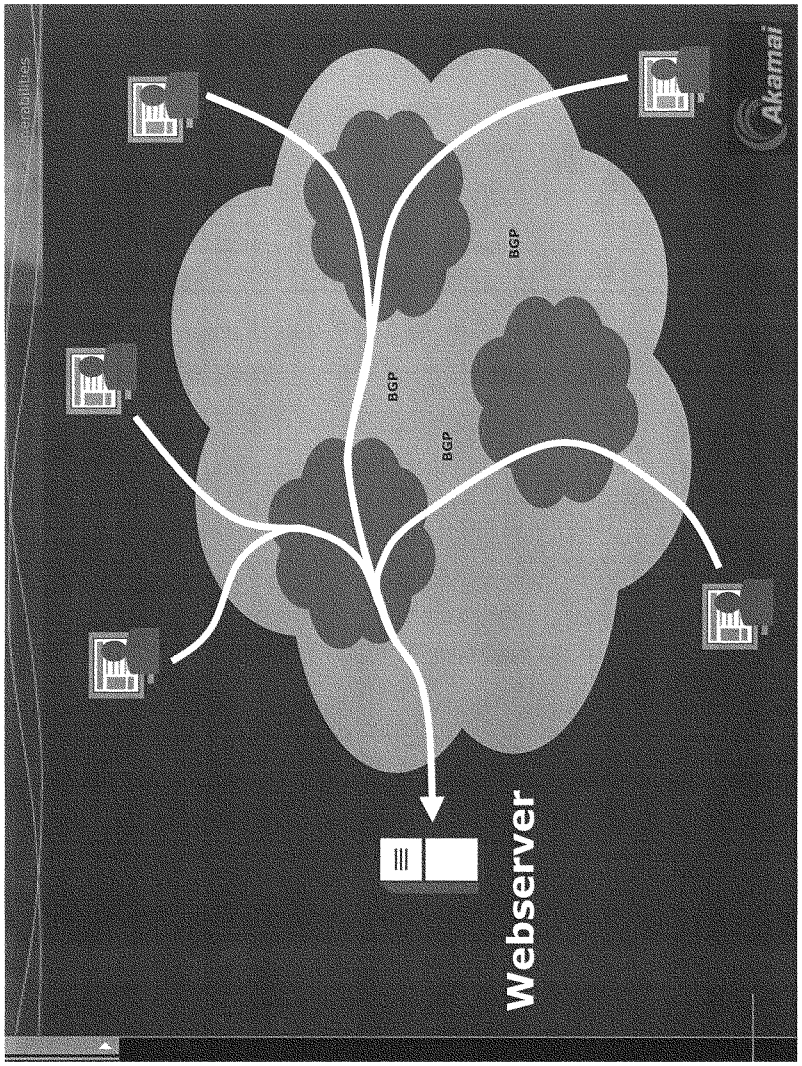

Traffic
10000
1000
100
10
1
Webserver
Internet
Akamai

Traffic
10000
1000
100
10
1
Webserver
Internet
Akamai

Traffic
10000
1000
100
10
1
Webserver
Internet
Akamai


Fire
Wall
Government
Network
Internet
Akamai


Fire
Wall
Publication
Point
Government
Network
Internet
Akamai


Webserver
BGP
BGP
BGP
Akamai

Hacker
BGP
BGP
BGP
Webserver
Akamai

Chairman TOM DAVIS. Thank you very much.

Mr. Ammon, thanks for being with us.

Mr. AMMON. My name is Ken Ammon, and I am co-founder and president of NetSec, an information security services firm headquartered in Herndon, VA. From our 24/7 security operations center, NetSec provides managed and professional security services to 5 of the Global 10 largest corporations, and 9 of the 15 cabinet-level departments of the U.S. Government. We monitor and manage systems in 22 countries around the globe. I would like to thank Chairman Davis, Ranking Member Waxman, and the committee for the opportunity to share with you the perspectives on enterprise security I have gained in my 5 years running NetSec, as well as my tenure in the U.S. Government, where I served as an Air Force officer and later as a security expert for the National Security Agency.

I know the time of the committee is limited, so I will focus my remarks on two important and related subjects affecting the security of the information in the U.S. Government. The first examines some very real, rapidly emerging threats; the second looks at law this committee developed, the Federal Information Security Management Act, and how it can be the guidepost for effectively managing sensitive information across Government.

Every member of this committee is familiar with the high profile worms and viruses that have disrupted operations and caused billions of dollars in economic damage across private and public sectors. We just observed how devastating these can be and how rapidly they can move. Clearly, such threats are serious and need to be addressed as part of any comprehensive information security strategy. But I am going to shift things and talk about the threats you don't hear about and can't readily detect. I submit that the threats I will demonstrate this morning may be less pervasive in their global reach, but may be far more devastating in their ability to breach the most sensitive boundaries of our national security and citizen privacy.

In my mind, there are two important platforms involved in securing information. The first platform is the infrastructure, and that is personal computers, servers, and networks. This infrastructure platform has been the dominant focus of information security strategies to date. The second platform revolves around the applications and information within the network. It simply does not follow that a secure infrastructure ensures secure information.

NetSec maintains what we call an Attack Lab, a facility where highly skilled ethical hackers are paid by our clients to break into their security systems in order to attempt to identify and resolve security vulnerabilities. In the course of recent application security research, NetSec's Attack Lab uncovered a method using the popular Google search engine and some advanced search key words to access sensitive data regarding U.S. military personnel actions, suspected terrorists, and very personal information about U.S. citizens.

The slide up now demonstrates that information—some of which has been redacted—such as Social Security numbers, the name of the individuals, locations; and for those of you that can't read it, I know that the committee has a copy of this. Information about terrorist connections, passport numbers, countries of birth and

such, this was all retained off a simple Google search, and this is just an example of thousands of records that we were able to access. Virtually anyone present in this hearing could access this information within a couple of minutes from virtually any PC connected to the Internet.

It is highly probable that systems that house the data in exhibit 1 here were each certified and accredited to process sensitive information. Simple configuration changes to the applications could have prevented this information leak. However, only through end-to-end application-level testing can the full scope of such vulnerabilities be identified. While this type of testing is becoming more common among commercial clients, there seems to be little awareness of or interest in this kind of testing in the Federal Government. And this testing, just for simplicity purposes, is testing Web-facing applications and how they react to and accept information, as well as deliver information, both Government-to-Government and Government-to-citizens. This information needs to be carefully examined as a critical component of information security in the Federal Government as well, we believe.

The second emerging threat involves the growing reliance on wireless networks that are being installed in Government facilities for obvious convenience, efficiency, and cost-avoidance reasons. Wireless networks pose a great potential danger, because if the wireless network is not properly secured it can open gaping holes in previously secure wired networks. We refer to this problem as the "steel door-grass hut" approach to security.

In the past, our Attack Lab has conducted several "war drives," which are basically taking a car and driving around a particular region and, using a device similar to this, a Pringles can—you can get the instructions for this right off the Internet. And what this does is, it connects to your laptop and allows you to access wireless networks from a much greater distance than would be advertised by the providers. What we found is that they were able to connect to numerous, hundreds of wireless networks in the Federal core of Washington, DC. The image on the screen here, you can't see the color coding key, which is a little lower on the screen, but red, yellow, and green are represented here, red being high density, yellow being low density, and green is roughly 14 separate points is the low point for abilities to connect to these systems.

Once again, the tools that the hackers use to connect to these networks are readily available on the Internet, and for our purposes we just detected the networks; it actually takes some additional effort to try to actually connect to the information available on the network. But literally you have the ability to be sitting in the desk next to somebody's computer once you connect to these wireless networks, and more than likely he will never know that it happens.

So we believe the Federal Government must create an environment that continuously rises to the challenge of threats such as these. Congress has made an important contribution to securing our Federal information assets with the enactment of FISMA. The visibility and importance bestowed upon the issue of information security by the passage of this law are invaluable. However, Congress needs to pay close attention and continuous attention to how

this law is interpreted and enforced in order for it to be effective in driving practical, pragmatic, and optimal use of resources available to achieve the best possible information security posture. To that end, I offer the following observations.

FISMA does run the risk of becoming a paperwork exercise. I believe we need more focus on "rubber meets the road" risk measures that reflect our actual progress in reducing vulnerability, not just a report card on how much of the required paperwork has been filed on time. If you look at the reporting that is being done under the auspices of FISMA, there are virtually no objective measures of agencies' real-world security posture, and this is what is and is not acceptable risk.

A good illustration is the emphasis on system certification and accreditation [C&A]. In the Federal IT community today, FISMA law and OMB guidance are widely interpreted as equating system security with the completion of system C&A. Much FISMA reporting focuses largely on the progress agencies are making in completing the C&A process for all of their major systems. C&A is the process whereby tradeoffs between security and efficiency are identified, optimized, documented, and approved in the course of fielding a new information system. It is an excellent way to reduce risk and to make sure the appropriate level of security is being designed into the system from the outset. Unfortunately, C&A provides little value when applied to existing or legacy systems. But due to the fact that FISMA compliance and progress has been equated with how many systems have gone through C&A, agencies are lavishly spending scarce resources to produce C&A reports that merely state the obvious: the legacy system is not secure and can't be effectively secured, in page after gory page of detail. And I actually have an example of one of these documents with us, and it is 5 inches of documentation. So it is a lot of paperwork that you go through for just one system, and thousands of these are being produced. Just reviewing the resulting stacks of hundreds of these pages of documentation per system presents a daunting task. You can imagine that much of the documentation gets filed, never to be looked at again.

In cases such as this, and in this I mean the legacy systems that are already in place, we need to stop wasting money on C&A reports, shortcut the paperwork process, and spend more of our money effectively for pragmatic risk reduction until the system can be modernized. If we fail to set up a system of reporting and oversight that promotes practical actions in the face of known vulnerabilities, we risk putting our best people in lose-lose situations such as that faced by a recently audited Federal agency. In this case, the agency was cited in the GAO report for failing to do C&A on an aging security system that was slated for imminent replacement by the agency. And I understand the price tag for one of these C&As is anywhere from $100,000 to $200,000 to certify and accredit a single system. The managers responsible decided, correctly in my opinion, that spending the money to do a C&A report on these systems would be a waste of taxpayer funds, but in doing the right thing agency technology and management executives left themselves open to criticism from the auditors and, subsequently, sensationalization of that criticism in the press. The irony

is that the system cited had actually been rock solid—tested for security vulnerability and found not to contain any—and was actually put in place to mitigate significant risk that was in place in the system. It continued to perform flawlessly until its recent replacement with newer technology.

My second observation is that security can't be bolted on to the IT infrastructure, and failures in IT management equal failures in security; you cannot separate the two, I believe. We must continue to get our IT management house in order to achieve a secure environment. No amount of focus on security can overcome fundamental weaknesses in how our information systems are managed.

As Government and industry have learned from the recent worm outbreaks, you can't protect what you don't know about, and what you don't know about your infrastructure will hurt you. Automated malicious code and hackers are very efficient in finding the machines in your infrastructure that are not properly patched. Even though the information goes to the departments and agencies, there are vulnerabilities. In many cases they do not have the asset management and configuration controls in place to adequately ensure all these systems have been patched, and we believe this to be a foundation of security.

Not to be ignored, a key issue for proper infrastructure management is organizational structure. Agencies should steer clear of having the fox watch the security hen house. There should be a healthy system of checks and balances and a positive relationship in place between those responsible for IT infrastructure and those responsible for information security management.

My final observation this morning is that we mustn't waste scarce resources reinventing the wheel. There are too many redundant, ineffective efforts going on in parallel, all designed to provide 24/7 security vigilance for Federal networks. In many cases there are multiple, redundant efforts taking place, separate bureaus within the same department each building their own security operations infrastructure. This is a serious waste of precious security expertise and budget.

NetSec clients, some of the world's largest corporations and government agencies, have recognized that enterprise security requires a level of focus and expertise hard to find in any organization, and we don't believe that these resources are going to be produced at a rate to meet this demand any time soon. That is why they have elected to entrust the monitoring and management of network security pieces to us, leaving scarce internal resources to focus on more core security-related issues.

Where feasible, the Government should take advantage of the proven capability of commercial companies already providing top-notch 24/7 security services on an outsourced basis. Commercially managed security providers offer an unparalleled combination of research and operational 24/7 security expertise. Government should avoid investing in internal development of services already available in the commercial marketplace.

In conclusion, not one of us in the room had an idea 10 years ago, when the Internet was first made available to the public, that our addiction to this medium would become so substantial in such a short period of time. None of us knew the incredible potential of

this medium to positively improve the lives of every citizen, increase the efficiency of Government and frankly, enhance the principles of freedom and communication that are hallmarks of our American society. So few of us had any idea the extent to which critical and sensitive information would become vulnerable to multiple kinds of mischief and misuse. There is no right or wrong answer. This may be the most important on-the-job training and learning program ever devised.

Security must be addressed. I believe it has been relegated to a second-tier status when it comes to discussions of and investments in security and other national priorities. This committee led the effort that produced FISMA, and I believe the committee has an opportunity to lead and educate Government, especially at the senior executive levels, of just how important ongoing and coordinated information security management is to our national security.

It has been a pleasure for NetSec as a company and me personally to appear here today. Your efforts are in fact very, very important. I wish you every success and stand ready to assist in an appropriate way. While the task of securing Government information systems is a daunting one, I am encouraged by the level of awareness and activity that has been fostered by the enactment of FISMA. We really do see this as landmark legislation and the focus on security is unprecedented. This committee has the opportunity, through its approach to FISMA oversight, to ensure that the attention paid yields true results and lowers the Federal Government's exposure to the security risks that go hand-in-hand with the benefits of the Internet.

Thank you.

[The prepared statement of Mr. Ammon follows:]

Testimony of Mr. Kenneth Ammon

President of NetSec Corporation
Before the Committee on Government Reform
Honorable Tom Davis, Chairman
October 16, 2003

INTRODUCTION

My name is Ken Ammon, and I am co-founder and President of NetSec, an information security services firm headquartered in Herndon, Virginia. From our 24x7 network security operations center, NetSec provides managed and professional security services to five of the Global Ten largest corporations, and 9 of the 15 cabinet-level departments of the US government. We monitor and manage systems in 22 Countries around the globe. I would like to thank *Chairman Davis, Ranking Minority Member Waxman,* and the committee for the opportunity to share with you the perspectives on enterprise security I have gained, both in my 5 years running NetSec as well as in my tenure in the US government, where I served as an Air Force officer and later as a security expert for the National Security Agency.

AGENDA

I know the time of the committee is limited, so I will focus my remarks on two important and related subjects affecting the security of information in the United States government. The first examines some very real, rapidly emerging threats. The second looks at a law this committee developed – the Federal Information Security Management Act (FISMA) - and how it can be the guidepost for effectively managing sensitive information across government.

Every member of this committee is familiar with the high profile worms and viruses that have disrupted operations and caused billion of dollars in economic damage across the private and public sectors. We just observed how devastating these can be and how rapidly they can move. Clearly, such threats are serious and need to be addressed as part of any comprehensive information security strategy. But I am going to shift things and talk about the threats you don't hear about, and can't readily detect. I submit that the threats I will demonstrate this morning may be less pervasive in their global reach, but may be far more devastating in their ability to breach the most sensitive boundaries of our national security and citizen privacy.

APPLICATION THREATS

In my mind, there are two important platforms involved in securing information. The first platform is the infrastructure – personal computers, servers and networks. This infrastructure platform has been the dominant focus of information security strategies to date. The second platform revolves around the applications and information within the network. It simply does not follow that a secure infrastructure ensures secure information.

NetSec maintains what we call our Attack Lab, a facility where highly skilled ethical hackers are paid by our clients to break into their secure systems in order to identify and resolve security vulnerabilities. In the course of recent application security research, NetSec's Attack Lab uncovered a method, using the popular Google search engine and advanced search key words to access sensitive data regarding US military personnel actions, suspected terrorists, and very personal information about private US citizens. Virtually anyone present at this hearing could access this same information within a couple of minutes from virtually any PC connected to the Internet.

It is highly probable that the various components and systems that house the data in exhibit 1 were each deemed to be secure, and certified and accredited to process sensitive or private data. Simple configuration changes to the application could have prevented these information leaks. However, only through thorough end-to-end application level testing can the full scope of such vulnerabilities be identified. While this type of testing is becoming more common among our commercial clients, there seems to be little awareness of or interest in this kind of testing in the federal government. This issue needs to be carefully examined as a critical component of information security in the Federal government as well.

WIRELESS NETWORKS, A SECURITY CHALLENGE

The second emerging threat involves the growing reliance on wireless networks that are being installed in government facilities for obvious convenience, efficiency and cost avoidance. Wireless networks pose a great potential danger because if the wireless network is not properly secured, it can open gaping holes into previously secured wired networks. In the past year, our Attack Lab has conducted several "war drives" around the federal core of Washington DC. Using a knapsack equipped with readily available, off the shelf devices, and downloadable software tools, our engineers surveyed the National Capitol Region area to ascertain the presence of wireless networks and their level of security.

As illustrated in exhibit 2 a war driver can detect hundreds of wireless networks in the federal core, and readily ascertain their vulnerability to break-ins. There are additional tools that hackers can then use to gain connection to those networks, even breaking the encryption algorithm if need be. If successful, the hacker has gained a place on the wired network from which to scan and launch attacks, and pull data off of agency machines

onto the hard drive of his or her laptop computer on the street below. And you may never know it happened.

OBSERVATIONS ON FISMA

The federal government must create an environment that continuously rises to the challenge of threats like those we just discussed, as well as the better-known issues already on the agencies' radar screens. Congress has made an important contribution to the securing of our federal information assets with the enactment of FISMA. The visibility and importance bestowed upon the issue of information security by the passage of this law are invaluable. However, Congress needs to pay close and continuous attention to how this law is interpreted and enforced in order for it to be effective in driving practical, pragmatic and optimal use of the resources available to achieve the best possible information security posture. To that end, I offer the following observations:

- **FISMA runs the risk of becoming a paperwork exercise**. We need more focus on "rubber meets the road" risk measurements that reflect our actual progress in reducing vulnerability, not just report cards on how much of the required paperwork has been filed on time. If you look at the reporting that is being done under the auspices of FISMA, there are virtually no objective measures of the agencies' real-world security posture.

  A good illustration is the emphasis on system certification and accreditation (C&A). In the federal IT community today, FISMA law and OMB guidance are widely interpreted as equating system security with the completion of system C&A. Much FISMA reporting focuses largely on the progress agencies are making in completing the C&A process for all of their major systems. C&A is the process whereby the trade-offs between security and efficiency are identified, optimized, documented and approved in the course of fielding a new information system. It is an excellent way to reduce risk and to make sure the appropriate level of security is being designed into systems from the outset. Unfortunately, C&A provides little value when applied to existing or legacy systems. But due to the fact that FISMA compliance and progress have been equated with how many systems have gone through C&A, agencies are slavishly spending scarce resources to produce C&A reports that merely state the obvious: the legacy system is not secure and can't be effectively secured – in page after page of gory detail.

  Just reviewing the resulting stacks of hundreds of pages of documentation per system presents a daunting task. You can imagine that much of this documentation gets filed, never to be looked at again.

  In cases such as this, we need to stop wasting money on C&A reports, short-cut the paperwork process and spend our money effectively, for pragmatic risk reduction, until the system can be modernized

  If we fail to set up a system of reporting and oversight that promotes practical actions in the face of known vulnerabilities, we risk putting our best people into lose-lose situations such as that faced by a recently audited Federal agency. This example

agency was cited in a GAO audit for failing to do C&A on an aging security system that was slated for imminent replacement by the agency. The managers responsible decided, correctly in my opinion, that spending money to do a C&A report on these systems would be a waste of taxpayer funds. But in doing the right thing, agency technology and management executives left themselves open to criticism from the auditors, and the subsequent sensationalization of that criticism in the press. The irony is that the system cited had actually been rock solid, fielded on a very cost effective basis, and yielded ahead-of-its-time levels of security when it was first deployed. It continued to perform flawlessly until its recent replacement with newer technology.

- **My second observation is that security can't be "bolted on" to the IT infrastructure. Failures in adequate IT management = Failures in security.** We must continue to get our IT management house in order if we are to achieve a secure environment. No amount of focus on security can overcome fundamental weaknesses in how our information and systems are managed.
    - As government and industry learned from the recent worm outbreaks - You can't protect what you don't know about and what you don't know about will hurt you. When Microsoft announces the latest vulnerability in its server software, you need to know where that software resides in your infrastructure, and who is responsible for patching it, before the worm that exploits that vulnerability is set loose in the wild. Automated malicious code and hackers are very efficient at finding the one machine in your infrastructure that wasn't properly patched. Asset management and configuration control are the foundation for a successful security program,
    - Not to be ignored, a key issue for proper infrastructure management is organizational structure. Agencies should steer clear of having the fox watch the security hen house. There should be a healthy system of checks and balances and a positive relationship in place between those responsible for IT infrastructure management, and those responsible for information security.

- **My final observation this morning is that we mustn't waste scarce resources re-inventing the wheel.** There are too many, redundant, ineffective efforts going on in parallel to provide 24x7 security vigilance for federal networks. In many cases there are multiple, redundant efforts taking place - separate bureaus within the **same department** each building their own security operations infrastructure. This is a serious waste of precious security expertise and budgets.

  NetSec's clients, some of the largest corporations and government agencies in the world, have recognized that enterprise security requires a level of focus and expertise hard to find in any organization. That's why they have elected to entrust the monitoring and management of their network security to us – leaving scarce internal resources to focus on more core security issues.

  Where feasible, the government should take advantage of the proven capabilities of commercial companies already providing top-notch 24 x 7 security services on an outsourced basis. Commercial managed security providers offer an unparalleled combination of research and operational 24x7 security operational expertise.

Government should avoid investing in internal development of services already available in the commercial market place.

CONCLUSION

Not one of us in this room had any idea ten years ago, when the Internet was first made available to the public, that our addiction to this medium would become so substantial in so short a period of time. None of us knew the incredible potential of this medium to positively improve the lives of every citizen, increase the efficiency of government, and frankly, enhance the principles of freedom and communication that are hallmarks of American society.

So, too, few of us had any idea the extent to which our critical and sensitive information would become vulnerable to multiple kinds of mischief and misuse. There is no right or wrong answer. This may be the most important on-the-job training and learning program ever devised.

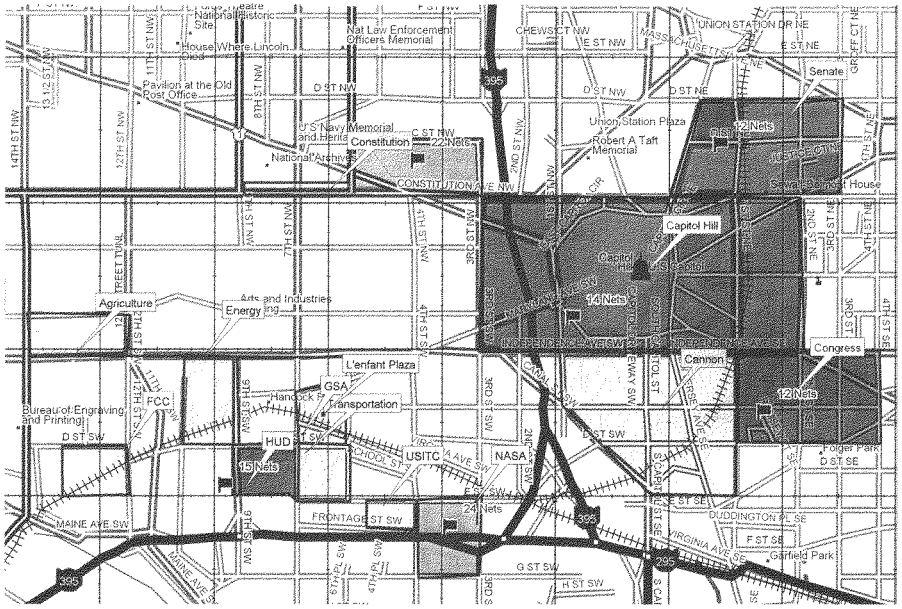
Security must be addressed. I believe it has been relegated to second-tier status when it comes to discussions of and investments in homeland security and other national priorities. This committee led the effort that produced FISMA. I believe this committee has the opportunity to lead and educate the government, especially at the senior executive levels, of just how important ongoing and coordinated information security management is to our Nation's security.

It has been a pleasure for NetSec as a company, and me personally, to appear here today. Your efforts are so important. I wish you every success and stand ready to assist in any appropriate way. While the task of securing our government's information systems is a daunting one, I am encouraged by the level of awareness and activity that has been fostered by the enactment of FISMA. This committee has the opportunity through its approach to FISMA oversight to ensure that the attention paid yields true results – and lowers the federal government's exposure to the security risks that go hand in hand with the benefits of the Internet.

EXHIBIT 2

Confidential. © 2003 NetSec. All Rights Reserved.

Capitol Hill IEEE 802.11b Wireless Network Density Map



Region Shading	Density Classification	Description
	High Density	21+ Wireless Networks
Green Area	Medium Density	11-20 Wireless Networks
Yellow Area	Low Density	1-10 Wireless Networks

Confidential. © 2003 NetSec. All Rights Reserved.

NetSec

Chairman TOM DAVIS. Well, thank you both. I don't know if I feel better after your testimony, but I think it is very revealing, and it is information the committee has to have. I just have two or three questions I want to go through.

First of all, Dr. Leighton, let me start with you. Basically, if you are concerned about security on the Internet, whether you are government, business, or an individual, you can't just buy a piece of software and be secure. I think that is the message here.

Mr. LEIGHTON. That is correct.

Chairman TOM DAVIS. You basically need some kind of filter, some kind of system, your own pipes, to be able to protect, is that fair?

Mr. LEIGHTON. You need all that and you need the Internet to be fixed in the sense of securing the basic underlying protocols. Even if you bought the fanciest filters, firewalls, all the software patches, and did everything else right, as soon as your traffic goes out onto the Internet, the Internet is not secure, and someone could alter BGP because BGP is not secured, someone could alter DNS because that is not secured, and you could be compromised.

Chairman TOM DAVIS. That is a huge job, to try to alter.

Mr. LEIGHTON. That is correct.

Chairman TOM DAVIS. That is beyond the scope of this hearing and I think that will take some time to fix, but I think a lot of people don't understand that.

Mr. LEIGHTON. That is correct.

Chairman TOM DAVIS. They plug it in and they don't understand how this evolved and how it came about.

In your testimony you discussed some of the vulnerabilities affecting the Internet and indicated that these are only a fraction of the ones that we face. I wonder if you could just go into some of the others briefly.

Mr. LEIGHTON. Yes. I didn't speak at length about the Domain Names System. This is like the 411 of the Internet. When you go to call somebody on the phone, you punch in a phone number instead of their name, and you get the phone number by looking it up in a phone directory or calling 411. The Internet works the same way. You type www.fbi.gov into your browser, but your browser actually consults an Internet-like phone book to find the IP address, and that Internet phone book is distributed through something called the Domain Name System. That system is not authenticated, it is easy for a hacker or an attacker to change entries in the domain name servers, and that means that you think you are going to fbi.gov, but if someone changed the IP address or changed the equivalent of a phone number, you are going to go somewhere else. This is one way to get your bank information. You think you are going to your bank, but in fact you get routed somewhere else.

DNS should be authenticated. You shouldn't be able to change an entry. It would be like changing the white pages in every city in the country, or your favorite city, without anybody knowing, only it is a lot easier to do on the Internet.

BGP should be authenticated. Today, anybody can send traffic wherever they want, and they can do it selectively. It happens by accident all the time, and it is largely, today, untraceable. Akamai

actually runs a service where we keep track of that and try to notify people when it is happening.

And, of course, there are all the software vulnerabilities on the end computers. People, as we speak, are assembling armies of zombies to send spam. As we speak, there is a new bug in Internet Explorer that will send traffic to the wrong place namely, the hacker will direct where he wants your traffic to go. So it is yet another way that you can type your bank's name into your browser, but you are not going to your bank because someone has installed a Trojan horse on your computer without your knowledge. And it is easy to forge return addresses. One of the aspects that made spam so effective was the mail appeared to come from your friend and if you looked at it, everything looked like it was coming from somebody you recognized, so you opened it and looked at it and, wham, you got infected. Both at the packet level and at the application or e-mail level it is easy to forge the return address to make the traffic look like it came from somewhere else. And there are ways that one could hope going about stopping that and making it so you can't fake it on the Internet.

So given these kinds of vulnerabilities, it is very easy to construct all different kinds of attacks to do bad things on the Internet.

Chairman TOM DAVIS. I think some of those you are describing as cyber attacks could be nothing more than mere probing, searching for weaknesses, but the worst could be yet to come. I mean, could we potentially be facing a digital Pearl Harbor?

Mr. LEIGHTON. Yes, the attacks we have seen so far, for example, Slammer, which was considered so devastating, may well have just been a probe; it had no payload. It wasn't meant to do any damage, per se, it just grew so fast, that is what brought down so much of the Internet. One could imagine if you actually put a payload in a Slammer and made it more sophisticated, you know, it was only a very narrow attack, the possibilities are large. As we become more dependent on the Internet with critical national infrastructure, it becomes frightening what might be doable.

Chairman TOM DAVIS. Thank you.

Mr. Ammon, thanks for being here as well, and both of you for your presentations.

Can you give me two or three specific actions you could identify to ensure that the Federal Government gets on track to secure the application and information environments that now reside on literally thousands of old and emerging computer systems?

Mr. AMMON. I think there are two issues that are fairly critical. One is that the efforts that take place in assessing vulnerabilities on legacy systems should be pragmatic and those dollars should be split between finding out where the most significant vulnerabilities are and then applying dollars to mitigating that risk until the system could be modernized. Once again, the certification and accreditation process is fairly lengthy, and it is designed to provide the decisionmaker with a quantification of risk. In, I would say, 10 out of 10 cases there is really nothing substantial you can do to go back and change that risk in a legacy system, you pretty much have to take a look at how to do it right the next time around. I think what we are trying to do here is close 15 years of lack of security focus

in a year or 2-year period, and I think we need a process to ramp up those older systems and then follow C&A for new systems that are coming out.

The second issue as far as application level security goes, I know that there is a push to Web-enable much of Government, and I think that follows in step with commercial business and what everybody is trying to do, be more friendly with who you have to do business with and citizens, and make it easier for folks to exchange information. I think that there needs to be some type of information or legislation put into the existing FISMA Act that calls out specifically transaction-level assessments. Much of the focus is on infrastructure and, like I said, you can get that right and everything can check out, and we have seen examples where by just changing some information in your Web browser, right at the very top where you actually request to get to the Web site, you are now staring at somebody else's information. And this has been prevalent in financial and other communities, and they have been very concerned with this, and so they have made significant efforts to modify their methodology to ensure they assess this risk and correctly field these types of applications. But literally we have seen zero interest in the Government for actually taking a look at these types of risk and figuring out what to do about them.

Chairman TOM DAVIS. Well, thank you very much.

Mr. Tierney.

Mr. TIERNEY. Thank you.

This is intriguing and fascinating, and made all the more mysterious by my lack of knowledge in the technical area, so bear with me, if you would. Thank you for your testimonies.

When you talk about new protocols, can we do that? I mean, is there likelihood that we are going to be able to accomplish a set of new protocols to get over the hurdles that we talked about? And if that is the case, what is being done now and who is doing it, is it Government or private industry moving in that direction? And what would Government's role be if there is a role for it in moving along that path?

Mr. LEIGHTON. Yes, Government has an important role to play. Just the way that Government provided the funding that created the Internet over 20 years ago, Government can provide the funding and direct funding toward research initiatives to help secure the Internet today. Some progress has already been made. There is technology available that can help secure BGP and DNS and the core infrastructure protocols. It is not being applied today, and part of that may be the expense associated with applying it.

So there can be a combination of getting protocols that are even more affordable to be deployed on the Internet and also using the purchasing power of the Government to buy products and buy from companies that are supplying companies that are more secure, that have invested in the security. Typically, a company that is invested in security, the services cost more, the products cost more, and Government can play a role by deciding that they want the secure offering versus maybe an offer that is less secure, and using the purchasing power to do that. So it is a combination approach.

Mr. TIERNEY. And is that happening now? Is something being done as we speak about securing some of these protocols, changing them?

Mr. LEIGHTON. There is some of that happening now. It would help to have it be happening a lot more and a lot faster.

Mr. TIERNEY. You talked in your testimony a little bit about removing the public-facing Web sites from Government networks altogether.

Mr. LEIGHTON. Yes.

Mr. TIERNEY. Is that a recommendation, that you would no longer have that public access to Government information in order to secure it? Or is there some way of doing that where you just separate the two and work from there?

Mr. LEIGHTON. The recommendation would be to actually improve the public access, which you would do by taking the public-facing Web sites off of the sensitive Government networks. Today you have a situation where there is a very large Government network, many Government networks, where they have thousands of public-facing Web sites sitting side-by-side with sensitive Government servers, and that is a recipe for problems. As the public comes in, the attackers come in, they infect the machines, and then the sensitive servers sitting right next door, they get infected, and now you have a serious problem. If you were to take the public-facing material and export that off of the Government network, take it outside of the sensitive network, now you don't invite the bad guys in with the public so, in effect, by doing that the access to the public content will be improved; it will be faster, it will be cheaper, and it will be more reliable, so the public gets better access to the Government and the Government stays more secure.

Mr. TIERNEY. Mr. Ammon, I represent a lot of people who are really concerned about identity theft, and it hits all age groups, and I have heard some pretty horrendous stories right across the board, with seniors in particular, those that are able to rate the technology barrier and actually get access to computers and the Internet, if they are disabled or aged, things of that nature. What is the message to them here from what you talked about today, should they not trust doing business over the Internet? Should they be concerned that there is nothing in place to protect them absolutely right now, or should they be encouraged to do that, and what protections could they take to be reasonably certain that they won't be the victims?

Mr. AMMON. Just from my observations on the use of the Internet, I think a lot of folks understand there is this level of risk, but the value of the Internet and the access to this information they feel really is something that drives them to still use the capability, even being aware this is possible. I believe, though, that there is an expectation that things are being done to make it better, and I think we are going to let a lot of folks down if we don't actually step up and do something to make it better, because these are widely publicized, these events, and the information definitely is used for ill intent, and we have seen more activity with organized crime wanting to get to this information so that you create a more effective way of exploiting that theft of identity. So I think that

there is some patience still available, but things have to be moved quickly.

Mr. TIERNEY. And who would we place that responsibility with, would it be industry, particularly the commercial side of these things, that they should protect themselves, or must the Government step in and do it because they might not do it?

Mr. AMMON. I think that one of the challenges that you face is that it is impossible at this point to point to a model that someone has put in place and say, "They have it right so let us just do what they have." I think what we have seen is, commercially more is being done at the actual "rubber meets the road" level for protecting their infrastructure, but Government has taken, I think, some fantastic leadership in putting together the visibility and oversight necessary in acts such as FISMA. I think that what we are doing is we are kind of closing the gap here, and Government has a great opportunity to take a leadership role and set a model for how this can be done, and I think corporate America would willingly adopt this if there was a Government model for actually executing on these problems. So I would recommend Government take a leadership position.

Mr. TIERNEY. Thank you.

Chairman TOM DAVIS. Thank you very much.

Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

I am really interested in the discussion concerning the wireless network access. In my own community, a couple years ago, a company that was interested in promoting their efforts to provide security services for companies that are using the Internet went around the city and identified networks that were open where there was a spillover, where the company was not even necessarily aware that they were broadcasting access to their network. We know that there are some places where people are advertising as an opportunity, bookstores and the like, to come in and utilize the wireless network, but many companies that implement the wireless network to one, get rid of a lot of the costs of wiring or two, provide themselves greater assistance in areas, for example, a building like this, where it may be very difficult to modify a building for wiring—might choose a wireless alternative, not really knowing that they are broadcasting access to their network.

You began to discuss that even though people might have access to the network itself, they might not be able to gain access to secure information. But I think it is still a shock to many companies that might be using wireless that anyone could have any access to the network at all through that. So could you talk a little about the spillover and if there is any ability to limit the spillover if you choose to have a wireless network? And also how you might be able to secure access; if you aren't able to limit spillover, how can you make it so that someone cannot access it? I know that certainly any company, if they saw someone walk into their business and begin to plug into their network, would immediately consider that as doing something criminal but think nothing of the fact that outside of their walls people might be able to access their network. Could you elaborate on that, please?

Mr. AMMON. Sure. I think wireless does have a lot of very beneficial features and it can be useful. I think that creating a policy and then having a way of enforcing that policy, the latter half of that statement is the real challenge. We see many organizations with a policy either prohibiting wireless security or stating how it can be done effectively and securely, but they really don't know when it is showed up in a way other than in that manner. Case in point, we had one agency where they had fielded a brand new security system, and all of the cameras that covered the perimeter actually were using wireless networking protocol to communicate. So the IT organization was not even aware that capability existed, that with a laptop you could sit a mile away, point these cameras at trees, at any point that you wanted to, because it had not been protected. And it really has to do with a lack of knowledge that these systems exist. So there are some emerging technologies that allow you to detect and actually enforce your policy, and we think there needs to be perhaps more education and focus that these technologies exist, and that can be an instrumental part for fielding a successful wireless program.

Mr. TURNER. Dr. Leighton, do you have anything else to add?

Mr. LEIGHTON. No. He covered it very well.

Mr. TURNER. Thank you.

Chairman TOM DAVIS. Mr. Ruppersberger, any questions?

I have a couple more questions.

Dr. Leighton, you mentioned that Internet protocols make it very easy to mask one's identity, often by latching on and stealing somebody else's. This impersonation can be taken a step further, where an attacker can redirect Internet traffic to an unintended destination, pretending to be that of the original site, thereby getting access to highly sensitive information. What practical steps can we take to protect innocent bystanders from both forms of theft, outside of redoing the whole Internet?

Mr. LEIGHTON. I don't know that you would need to redo the entire Internet. It would help to authenticate Border Gateway Protocol so that if I went to an ISP and said, "Send me the traffic for this IP address," it would check first and make sure that I own that IP address. There is mathematical technology called authentication encryption and authentication digital signature technology which could be applied in this context. A similar process could be applied to the Domain Name System. Secure protocols can be used to communicate if you are sure that both ends are actually using the protocol. One of the misconceptions today is when you go to your bank you are using SSL or HTTP secure, you think you are secure, but if I can intercept your traffic ahead of time, I won't start the session using the right key or I won't start the secure session at all, and so you are misled into thinking you are secure when you are not.

So there are a variety of steps, and I guess the first is education, making people aware that the problem exists today and there is something to be dealt with. And then the next step is developing the right procedures to put into place in the existing Internet. I don't think you need to replace the Internet to make it more secure, it is improving the protocols to make them work better.

Chairman TOM DAVIS. Do you think that is best directed from the Federal Government as a practical matter?

Mr. LEIGHTON. I think the Federal Government can certainly play an important role in highlighting the problem.

Chairman TOM DAVIS. Absent us doing that, is it likely to occur, do you think, anytime soon?

Mr. LEIGHTON. No.

Chairman TOM DAVIS. I guess that is what I am after.

Mr. LEIGHTON. No, we have known about this for a long time. We are seeing the effects of it now in a very public way, in the news stories, and it is something that affects all of us today. The effects will get worse if we don't correct the problem. Part of it is that you have 15,000 different competing economic units that make up the Internet, and they have to cooperate somehow, and leadership from the Government could be helpful.

Chairman TOM DAVIS. Mr. Ammon, let me ask you. You talked about how FISMA could be nothing more than a big paperwork display, and that is our fear too. I think you said that the certification and accreditation process in FISMA should not be considered a panacea because it can't guarantee the security of legacy systems in the Federal Government. What are commercial best practices for ensuring older systems?

Mr. AMMON. They are searching for leadership here also. I know that IT governance has now been augmented to include IT security governance, designed to drive visibility and such in commercial organizations. And I think that is a positive move forward, but they have spent, I think, more time at the execution level trying to ensure that these older systems are either phased out, and I think they have done that fairly rapidly, or they have put measures in place to, at a minimum, minimize the risk that is apparent. And they spend the money doing that as opposed to generating a very large document that just captures what they already know.

And, look, we do certification and accreditation as a company, so I could sit back and say, great, we will keep doing it and make lots of money at doing this, but we think that it just leaves too much risk on the table. So having a parallel process that allows the Government and the security decisionmakers to short-circuit that process for legacy systems, but not basically meet the criticism of an audit, would be very helpful in allowing them to mitigate risk and build the systems more securely as they roll out the new systems. And I think that is something that could perhaps be put into FISMA, or at least guidance should be produced in that direction.

Chairman TOM DAVIS. When I go home tonight, what is the first thing I can do to minimize the security threat to my own computer?

Mr. LEIGHTON. Get all the patches installed on your software, get a firewall installed, and be familiar with how to use it and make sure it is functioning properly.

Chairman TOM DAVIS. OK. Do you agree with that?

Mr. AMMON. We used to have a joke about this at the National Security Agency: "Turn it off and put it in a box." But I think the real answer there is that bad things happen to computers. Sometimes the disk blows up, sometimes it is a virus that comes in. You know, back up your data, do some common sense, straightforward things, and make sure you have available security software such as

virus protection software. There are personal firewalls that I think still have some growing to do, they seem to be overly complex for the average user, but even that can be helpful in mitigating some of the risk.

Chairman TOM DAVIS. All that mitigates it, but clearly you are still very vulnerable.

Mr. AMMON. You are still going to have issues, so just be smart about what you put on there, back it up. You know, these pervasive connections such as cable modems and such, they definitely increase the level of risk that you have. So if you are not going to be home, shut it down, don't leave it up and running, because people are constantly knocking on that door, and if they find something wrong, they will take advantage of it.

Chairman TOM DAVIS. And the vulnerabilities are tremendous. If you get some malevolent group that understands this stuff and comes in, they can do severe damage. I mean, we talked before about a digital Pearl Harbor, that is the potential here.

Mr. AMMON. Absolutely. Yes.

Mr. LEIGHTON. In addition to the harm that can be caused to you, if you are keeping track of your machine and the latest virus scanning and so forth, you want to be sure that your machine isn't contributing to the attack on somebody else's infrastructure, to make sure that your computer hasn't been subverted.

Chairman TOM DAVIS. I know Mrs. Blackburn is on her way back from the floor. She just e-mailed and had some questions she wants to ask.

Let me ask if any other Members have any other questions they want to ask at this point.

And is there anything else that you would like to add that maybe you didn't get a chance to say that you want to emphasize in lieu of some of the questions that have come forth?

Mr. LEIGHTON. Well, I think we have covered the basic points: that there are serious problems, we need to be educated about them, and there are steps we can start taking to make things better, and I think Congress has a very important role there.

Chairman TOM DAVIS. Viruses or worms can leave an infected computer in a very vulnerable state, as you noted before, that can be exploited later by an attacker. So it comes in and it is literally like a virus, it weakens the system so an attacker can come in. Now, how can homes and businesses protect themselves to ensure that their systems are not used as a Trojan horse? Is there any detection device on that you are aware of? If a home user's computer has such a Trojan horse and they want to file their taxes electronically or check their bank account online, then are those institutions at risk?

Mr. LEIGHTON. Yes. Getting the latest virus scan software. Typically, once a virus is out there, software has been developed to detect it, you know, in fairly short order, and so if you get that software, you can help detect that your computer has been compromised. In the most obvious cases your computer has all sorts of problems and you know something is wrong; in the less obvious cases it is being used as a Trojan horse and you don't detect the problem, and that is why you want to be proactive about seeing if you have a problem even though you are not witnessing symptoms

currently. There are stories today of computer armies numbering many thousands, maybe hundreds of thousands of computers connected to the Internet that can be used later for an attack, and you want to be sure that your computer is not one of them.

Chairman TOM DAVIS. You are both out there in the private sector, marketing products, meeting with people. Why is there still a lack of attention paid in some cases to information security as a fundamental element of routine business operations in many businesses?

Mr. LEIGHTON. There is a lack of understanding of the nature of the problem and there is severe economic pressure that limits proactive investment in security-related offerings. That makes it hard to invest in a problem that hasn't happened to you yet. We see that all the time in speaking with customers; they haven't been hit yet by something, and so they are not as inclined to put the investment in to prevent that something from happening.

Chairman TOM DAVIS. It is like homeowners insurance almost, right?

Mr. LEIGHTON. Exactly. Once the disaster happens, they are very happy customers, because then they know there is a cost involved and that they can prevent it from happening again at a very low price. So it is exactly that situation.

Mr. AMMON. I think organizational structure is problematic at this point also. When you put the security responsibility directly under the CIO you can have, especially in commercial organizations where CIOs are very driven to reduce costs, you have a security officer basically looking to introduce cost into the business. That can affect incentives, goals, compensation of the person who is trying to reduce the overall expense in IT. So I think in some cases where we have seen commercial organizations place that role in a different organization, I think that you get greater high visibility for what may be wrong and potentially more support for the dollars to fix it, because you are not at odds with your goals that you are trying to achieve in your position.

Chairman TOM DAVIS. Mr. Putnam wanted to ask this question. He says, given that there are oftentimes patches available for identified vulnerabilities, why is it that so many government, corporate, and home users remain so incredibly vulnerable? And I guess from your statement, you can have all the patches you want, but there are always more vulnerabilities out there and people willing to exploit them. But I will let you answer it.

Mr. LEIGHTON. Yes, that is true. That said, the best thing, the first thing to do is get the patches installed. And part of the issue there is there are just so many bugs and exploits that patches just keep on coming, and you have to make sure you stay current, and that takes real effort.

Chairman TOM DAVIS. Are most of these viruses and worms that you are seeing in your businesses coming from outside the United States or from inside the United States?

Mr. LEIGHTON. That is actually hard to say with certainty, because most of them you can't track their origin. We first observed Slammer in Asia, but it spread very quickly. We can't say for sure that it started there. So it is really hard to know for sure where they come from.

Mr. AMMON. And I think that you can get descriptions of how these viruses or worms actually work, and they make your head spin, lots of ones and zeros and Xs and Os and such, but there are tools available on the Internet that basically give you a workbench with a mouse and point and click that allows you to build these. So what has happened is you have enabled the novice now to go out and build these type of destructive capabilities, launch them into the wild, and they do their damage. So it used to be you had to be very smart to put one of these things together, and so you were limited by the number of smart, malicious folks you have. Well, now they have sort of multiplied their ability to do damage by creating toolkits for the novice to do this. And I think it is something worth taking a look into and discussing whether those tools should be out there and available.

Chairman TOM DAVIS. Do you think most of these attacks are malevolent or just people playing games?

Mr. AMMON. Well, I think you get to see the ones that sort of have a life of their own. What you don't see is what I think you should be very concerned about, because the motivated attacker, the enemy to the country or corporation is not going to make a lot of noise, doesn't want to be seen, and they are going to get in and they are going to get out, and they are going to get to the valuable information; and we have seen this in economic espionage as well as just Government situations when I was at NSA.

Chairman TOM DAVIS. Government architecture and computers have locally-loaded application software. Would it be a good idea for Government to use a thin client which would make software applicable to a central control server that would minimize that threat? Any thoughts on that?

Mr. LEIGHTON. I think a lot of the same issues would exist. You know, if it brought greater control and visibility as to what is going on, what software is on your network, that is helpful, but a lot of the same issues will still exist.

Mr. AMMON. A browser is a fairly simple piece of software. What we found is that there is complex infrastructure on the other side of that browser that you connect to to do business; there are data bases, the actual technology that allows you to see a Web page when you go to a site, and that is a fairly complex infrastructure, it involves many components. And I think that end-to-end security of the platform that houses the information and serves the request is where the focus needs to be. If you get that right, then the client shouldn't be able to do damage to you.

Chairman TOM DAVIS. Thank you very much. This has been, I think, very helpful to the committee. I don't see Mrs. Blackburn here. I will give her a minute with you afterwards if she walks in in the next couple of minutes. This has been excellent in terms of collecting information. You know, what we do with it, what the administration does with it, I think is really going to be up to us to sit down and talk about. But I hope to use you both as resources as we move forward. We appreciate what you are doing and the innovations you are bringing to bear and your experience out there in the real world. Again, having been in the private sector and the incentives that are offered for what you get, this is money that you spend defensively that you have nothing to show for on the bottom

line. You are looking at your risk, I guess, but everybody thinks it can't happen to them.

Let me ask one other question. How commonplace is it, Dr. Leighton, with your clients, that there are penetrations that you are able to stop? You can detect that to some extent, can't you?

Mr. LEIGHTON. Yes. Certain kinds of penetrations have substantial success: Web-based attacks and keeping the Web infrastructure running even when it is under attack. We have several high profile Government sites, including the FBI, which we aren't allowed to talk about, which we are having trouble keeping up because of all the attacks, and since they have used Akamai services they haven't witnessed an attack on their site even though it happens every day, and that is because we provide a defensive shield.

Chairman TOM DAVIS. And you can see that from where you are, that the shield is working, basically?

Mr. LEIGHTON. Oh, absolutely. And we give them monitoring tools so they can actually see the attack and say, "Oh my goodness, there is a major attack against the site," but the site is functioning normally because we are fielding that attack and monitoring it. We have seen some extraordinarily large attacks against Government Web sites during the last year.

Chairman TOM DAVIS. And so far you have been impenetrable?

Mr. LEIGHTON. So far.

Chairman TOM DAVIS. That is all I can ask.

Mr. LEIGHTON. We put a lot of investment in trying to make sure it stays up and running and stays secure.

Chairman TOM DAVIS. OK. Well, again, thank you both very much. We appreciate your being here.

And the record will remain open if Members want to add comments until the end of the day. If you have any additional thoughts in the next week or so, we will keep the record open and you can supplement it. The hearing is adjourned. Thank you.

[Whereupon, at 11:45 a.m., the committee was adjourned, to reconvene at the call of the Chair.]

[Additional information submitted for the hearing record follows:]

Congressman Marsha Blackburn: Mr. Ammon, concerning FISMA, why could we not "pitch" the entire system and start over?

Mr. Ammon: I believe that scrapping FISMA would be a big mistake. NetSec believes that the passage of FISMA was a very positive move toward securing our federal information systems. We sincerely believe that FISMA provides a level of visibility, a sense of urgency, and an overall framework that will serve the government well in tackling enterprise security. Enterprise security is complex problem involving both management and technology dimensions. While private industry tends to be in front of government in implementing security technology, most of industry actually lags government in the management dimension of security. This is thanks in large part to the implementation of FISMA and GISRA before it. Government has the opportunity for leadership in enterprise security management.

My comments about performance measures, and about the applicability of the current C&A process to legacy systems are offered in the interest of ensuring that FISMA is as successful as possible in improving the overall security posture of the federal government. I believe if both the executive and legislative branches pay close attention to real-world measurements, and to the incentives our measurement and oversight processes create, FISMA can continue to be an enormously successful law.

Congressman Marsha Blackburn: **How would you organize federal networks?**

Mr. Ammon: I would recommend that departments centralize the management and security of their networks at the department level whenever possible. Centralization of this function enables better security at lower cost.

Congressman Marsha Blackburn: **How much savings would be found if commercial companies were outsourced to providing security services?**

Mr. Ammon: The savings would vary greatly from one agency to another depending on how large their network is and how much traffic passes through it. But let me cite an example of one of our smaller clients, a sub-agency within the Labor Department. They have contracted with NetSec to provide them with expert 24x7x365 monitoring and management of their network intrusion detection sensors and firewall for approximately $150,000 per year. For this price, NetSec provides our expertise, trained personnel, a secure, highly resilient monitoring facility, and the specialized systems it takes to monitor and manage IDS and firewalls. Were they to perform this task in house, they would need a minimum of six engineers and a supervisor, just to provide one-deep coverage of every shift. The personnel cost alone amounts to on the order of $550,000 per year. This does not include the cost of a facility with redundant power and redundant network connections. It does not include the special management systems that would need to be installed in that center and maintained by the agency's IT staff. It does not include the cost of developing and documenting processes and procedures. It does not include training, etc. Now imagine that other sub-agencies within the department are doing the same thing. You can multiply this cost differential many times over.

Moreover, the benefits of outsourcing this function are not limited to cost avoidance. There is severe shortage of personnel with the requisite skills in information security. Agencies need to utilize their skilled personnel dealing with core security functions within the agencies instead of chaining them to consoles 24x7. A managed security provider can watch the consoles for them, and alert agency personnel when an event requires their attention. Managed security services

providers like NetSec have the opportunity to simultaneously monitor a multitude of government and private sector networks worldwide, providing us with superior visibility to what is happening on the Internet, and what threats may loom in the immediate future. So outsourcing this function not only provides a lower cost alternative, it provides superior results.

○