COMPUTER SECURITY: ARE WE PREPARED FOR CYBERWAR?

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MARCH 9, 2000

Serial No. 106–160

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

67–018 CC WASHINGTON : 2000

CONTENTS

COMPUTER SECURITY: ARE WE PREPARED FOR CYBERWAR?

THURSDAY, MARCH 9, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2247, Rayburn House Office Building, Steve Horn (chairman of the subcommittee) presiding.

Present: Representatives Biggert, Walden, and Turner.

Staff present: J. Russell George, staff director and chief clerk; Matt Ryan, senior policy administrator; Bonnie Heald, director of communications; Bryan Sisk, clerk; Ryan McKee, staff assistant; Trey Henderson, minority professional staff member; and Jean Gosa, minority staff assistant.

Mr. HORN. The hearing of the House Subcommittee on Government Management, Information, and Technology will come to order. Earlier this year, the Nation successfully met its first technological challenge of the new millennium, Y2K. Although the time, labor, and $100 billion cost for this effort, private and public, we learned much from this experience. Those lessons will be especially important now as we turn to the second technological challenge of the new year, computer security.

We are here today to learn. In April 1996, this subcommittee held a similar information hearing on the year 2000 computer problem. Our questions will be many of the same questions we asked in that hearing 4 years ago. We want to know the dimension and scope of these cyber attacks. We want to know what efforts are being undertaken toward solving the problem, and we want to know what the Federal Government is doing to address this problem.

Since the early 1990's, the worldwide use of computers and computer networks has skyrocketed. The Internet has revolutionized the way governments, nations, and individuals communicate, and the way to conduct business. The Internet and electronic mail are now available 24 hours a day to anyone with a desktop computer, a modem, and a telephone line. Yet, without rigorous efforts to protect the sensitive information contained in these computer systems, many of the Nation's essential services, telecommunications, power distribution, national defense, and so on down the line are vulnerable to cyber attacks.

Over the last few weeks, several of the Nation's most viable Internet websites have fallen prey to "denial-of-service computer attacks." Although these attacks disrupt essential business services, they only scratch the surface of cyber attacks that may be taking place in other highly integrated computer networks.

Our first panel of witnesses today will discuss the vulnerability of the Nation's vital computer systems and the Government's efforts to protect them. Our second panel, from the private sector, will demonstrate how easy it is to invade or hack a computer system, and what organizations can do to protect these systems. We welcome each of you and we look forward to your testimony.

If you will stand and raise your right hands, we will swear you in.

[Witnesses sworn.]

Mr. HORN. The clerk will note that all four witnesses affirmed the oath. We will start with Mr. Tritak, Director of Critical Infrastructure Assurance Office, Department of Commerce. Mr. Tritak. I might say, the way we work here, once I announce you, your full statement is automatically put in the record.

The staff has read it and when we have had a chance, we read it. We then want you, if you could, to summarize it in 5 minutes. Do not read it, whatever you do, but give us from your heart what this problem is. That is what we are interested. When you are all done, we will then have questions, 5 minutes on each side when those Members come here. We will try to get a rounding out of what the testimony is.

So, Mr. Tritak, you are first.

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

Subcommittee on Government Management, Information, and Technology

Opening Statement
Chairman Stephen Horn (R-CA)
Subcommittee on Government Management, Information, and Technology
March 9, 2000

"A quorum being present, the hearing of the House Subcommittee on Government Management, Information, and Technology will come to order.

"Earlier this year, the nation successfully met its first technological challenge of the new millennium -- Y2K. Although the time, labor and $100 million cost of this effort was enormous, both public and private sectors learned much from the experience.

"Y2K underscored the need for a disciplined management approach to problem solving. Teamwork and determination in both the public- and private-sectors helped meet the Y2K challenge. That type of commitment will be equally important as we turn to the second technological challenge of the New Year -- computer security.

"We are here today to learn. In April 1996, this subcommittee held a similar informational hearing on the Year 2000 computer problem. Our questions will be many of the same questions we asked in that hearing nearly four years ago. We want to know the dimension and scope of these cyber attacks; we want to know what efforts are being undertaken toward solving the problem; and we want to know what the federal government is doing to address this problem.

"Since the early 1990s, the worldwide use of computers and computer networks has skyrocketed. The Internet has revolutionized the way governments, nations, and individuals communicate and conduct business. Financial transactions and electronic mail are now available 24 hours a day to anyone with a desktop computer, a modem and a telephone line. Internet web sites, computer bulletin boards, and e-mail provide a "virtual world" of unlimited information.

"Yet, without rigorous efforts to protect the sensitive information contained in these Web sites and computer systems, many of the nation's essential services, such as telecommunications, power distribution, and national defense, are vulnerable to cyber attacks.

"Over the last few weeks, several of the nation's most visible Internet web sites have fallen prey to "denial of service" computer attacks. Although these attacks disrupt essential business services, they only scratch the surface of the cyber attacks that may be taking place in other, highly integrated computer networks.

"Our first panel of witnesses today will discuss the vulnerability of the nation's vital computer systems, and the Government's efforts to protect them. Our second panel is from the private sector and will demonstrate how easy it is to invade, or "hack," a computer system and what organizations can do to protect these systems.

"We welcome each of you, and look forward to your testimony."

STATEMENT OF JOHN TRITAK, DIRECTOR, CRITICAL INFRASTRUCTURE ASSURANCE OFFICE, DEPARTMENT OF COMMERCE; JOHN GILLIGAN, CHIEF INFORMATION OFFICER, DEPARTMENT OF ENERGY, AND CO-CHAIR, SECURITY, PRIVACY, AND CRITICAL INFRASTRUCTURE COMMITTEE, CIO COUNCIL; KAREN BROWN, DEPUTY DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, DEPARTMENT OF COMMERCE; AND RICH PETHIA, DIRECTOR, COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTERS, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY

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

I am grateful for this opportunity to appear before you today to begin a dialog with you and your committee on the issues relating to critical infrastructure assurance and computer security. In the way of talking about infrastructure, one of them I want to mention is that my slides just showed up. If you do not mind, I would like to just put them up before you.

Mr. HORN. Sure. Keep talking. They can put them up.

Mr. TRITAK. In any event, Mr. Chairman, Americans have long depended on delivery of essential services over the Nation's critical infrastructures. The need to assure the delivery of these services against significant disruptions has been a concern of infrastructures, owners, and operators for as long as there have been electric power plants, telecommunications systems, airlines, railroads, banking, and financial services. In other words, critical infrastructure assurance itself is not new.

What is new is the increasing reliance on information technology and computer networks to operate those infrastructures. This growing reliance introduces new complexities, interdependencies, and potentially vulnerabilities. The threat that individuals, groups, and nation states are seeking to identify and exploit these vulnerabilities is real and growing.

[Chart shown.]

Mr. TRITAK. In recognition of this, President Clinton issued PDD–63 establishing the protection of the Nation's infrastructures as a national security priority. As you can see from the chart, Mr. Chairman, PDD–63 sets forth an ambitious goal. It calls for a national capability by 2003 to protect our critical infrastructure from intentional attacks that could significantly diminish the Federal Government's ability to perform essential national security missions and to ensure general public health and safety, State and local government's ability to maintain order, and to deliver minimal essential services to the public.

Three, the private sector's ability to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. The important conclusion of PDD–63 is that critical infrastructure assurance is a shared responsibility. With 90 percent of the Nation's infrastructures being privately owned and operated, the Federal Government alone cannot guarantee its protection.

In response to the issuance of PDD–63, the Federal Government had to organize itself in order to meet the challenges posed by this unique national security challenge. A national coordinator for secu-

rity, infrastructure protection, and counter-terrorism was created to oversee national policy development and implementation, as well as to advise the President and national security advisor on the same.

My Office of Critical Infrastructure Assurance Office was created to coordinate policy development for the national plan, to assist agencies in analyzing their critical infrastructure dependencies, and to coordinate national education and awareness efforts. The National Infrastructure Protection Center was created at the FBI to serve as a threat assessment center, focusing on threat warnings, vulnerabilities, and law enforcement.

For each infrastructure sector that could be a target for infrastructure cyber or physical attacks, a single government department or agency was established as a lead agency for working directly with representatives from private industry.

[Chart shown.]

Mr. TRITAK. Earlier this year, President Clinton issued the first version of the national plan. Displayed before you is the cover. It says a lot about what the plan is and is not. First, the plan focuses on the cyber dimensions for securing critical infrastructures and underscore the new challenges posed by the information age. That is not to say that physical infrastructure protection is no longer important. It is.

Future versions of the plan will reflect that importance. In fact, the plan is designated 1.0 and subtitled, An Invitation to a Dialogue For a Good Reason. It is very much a work in progress. It concentrates on the Federal Government's efforts in infrastructure protection. The plan acknowledges that this is not enough. We must work closely with industry and include them in the national planning process.

We must also deal with the fact that there is an international dimension to national information assurance, as well as a domestic one. Of course, we must work closely with you in the Congress to ensure that your concerns, ideas, and interests are reflected in subsequent versions of the plan.

[Chart shown.]

Mr. TRITAK. To meet the goal of PDD–63, the national plan establishes 10 programs for achieving three broad objectives. First, steps must be taken to identify the key elements and systems that constitute our critical infrastructures. Their vulnerability to attack must be assessed and plans must be developed to address those vulnerabilities.

In so preparing, we hope to prevent attacks from reaching their target in the first place. Next, should such attacks occur, we must develop a means to identify, assess, and warn about them in a timely manner. The attacks must then be contained. Disrupted services must be restored and affected systems must be reconstituted.

Finally, we must lay a strong foundation upon which to create and support the Nation's commitment to achieving the first two objectives. These include coordinated research and development, training, and employing information security experts, raising awareness, and, where appropriate, identify potential legal or legislative reforms.

[Chart shown.]

Mr. TRITAK. The President requested $2 billion for critical infrastructure protection in his fiscal year 2001 budget request. This represents a 15 percent increase over fiscal year 2000 funding. Of this, 85 percent supports protection of agency infrastructures; 72 percent goes to supporting critical infrastructure efforts within the national security agencies.

Our President proposes a number of key initiatives in his budget request. I will just highlight a few. The Federal Cyber Service Initiative seeks to redress the shortage of information security expertise in the Federal Government. This shortfall reflects the scarcity of college-level programs in information security. It also reflects the inability of the Government to compete for highly skilled workers in this area.

Our goal is to recruit, train, and retain a cadre of IT specialists for Federal service. The Federal Intrusion Detection Network will serve as a centralized burglar alarm system for critical computer systems within civilian government agencies. Intrusion Detection Systems will be installed and operated by the civilian agencies. Alarm data indicating anomalous computer activity will be sent through the agency, by the agency to the GSA for further analysis.

Only if there is evidence of criminal behavior will data be sent to the NIPC and law enforcement. FIDNet will not monitor any private network traffic. It will comply with all existing privacy laws. The Partnership for Critical Infrastructure Security attempts to build on the efforts already underway between government and industry.

It seeks to bring the individual sectors together to encourage a cross-sectoral dialog as a common concern, such as the growing interdependencies among the infrastructure owners and operators. The Partnership also provides a form for infrastructure owners and operators to engage other interested stakeholders, including the audit community, insurance community, Wall Street, and the investment community, and of course mainstream businesses who are the ultimate consumers of infrastructure services.

Now, the partnership is dedicated to the belief that once industry recognizes a business case for action, economic self-interest in the market can go a long way toward addressing the challenges of infrastructure assurance. That is not to say that self-interest in the market alone can solve these problems, because they cannot. Where they cannot, and what national security interests of their country requires, the Federal Government must step in to address any gaps and vulnerabilities that may exist.

Last month, over 200 representatives of more than 120 companies began to organize their participation in this Partnership. I think the Partnership represents a good step in not only addressing issues of common concern, but also for industry to take a lead in addressing the problems that confront us today. When you have good partnership between industry and government, we are better able to identify and define our respective roles so that where there

are gaps, where the market cannot address a problem of concern to the Nation, we can fill that gap.

Given the limited time, Mr. Chairman, I am going to conclude my remarks here and I look forward to your questions.

[The prepared statement of Mr. Tritak follows:]

Hearing before the
House Government Reform Committee

Subcommittee on Government Management, Information and Technology

March 9, 2000

Statement of
John S. Tritak
Director
Critical Infrastructure Assurance Office

Mr. Chairman, it is an honor to appear before you today to talk about the National Plan for Information Systems Protection, Version 1.0, and the role being performed by the Critical Infrastructure Assurance Office (CIAO) of which I am Director. I am grateful for the opportunity to discuss the Administration's efforts to achieve President Clinton's goal of establishing by 2003 a full operational capability to defend the critical infrastructures of the United States against deliberate attacks aimed at significantly disrupting the delivery of services vital to our nation's defense, economic security, and the health and safety of its people. This goal cannot be reached without the strong support and active participation of the Congress.

I. Introduction

The Information Age has fundamentally altered the nature and extent of our dependency on these critical, nation-wide infrastructures. Increasingly, our Government, economy, and society are being connected into an ever expanding and interdependent digital nervous system of computers and information systems. With this interdependence comes new vulnerabilities. One person with a computer, a modem, and a telephone line anywhere in the world can potentially break into sensitive Government files, shut down an airport's air traffic control system, or disrupt 911 services for an entire community.

The threats posed to our critical infrastructures by hackers, terrorists, criminal organizations and foreign Governments are real and growing. The need to assure delivery of critical services over our infrastructures is not only a concern for the national security and federal law enforcement communities; it is also a growing concern for the business community, since the security of information infrastructure is a vital element of E-commerce. Drawing on the full breadth of expertise of the federal government and the private sector is therefore essential to addressing this matter effectively.

The President signed Presidential Decision Directive 63 in May1998, detailing the Administration's policy on critical infrastructure protection. In the 22 months since, we have made significant progress in protecting our critical infrastructures. The National Plan for Information Systems Protection (the Plan) was released last month to serve as a blueprint for establishing a critical infrastructure protection (CIP) capability. The plan represents the first attempt by any national Government to design a way to protect those infrastructures essential to the delivery of electric power, oil and gas, communications, transportation services, banking and financial services, and vital human services. Increasingly, these infrastructures are being operated and controlled through the use of computers and computer networks.

The current version of the Plan focuses mainly on the domestic efforts being undertaken by the Federal Government to protect the Nation's critical cyber-based infrastructures. Later versions will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community. Subsequent versions will also reflect to a greater degree the interests and concerns expressed by Congress and the general public based on their feedback. That is why the Plan is designated *Version 1.0* and subtitled *An Invitation to a Dialogue* -- to indicate that it is still a work in progress and that a broader range of perspectives must be taken into account if the Plan is truly to be "national" in scope and treatment.

The Critical Infrastructure Assurance Office (CIAO) was created by PDD-63 to integrate the various sector plans into the National Plan, coordinate analyses of the U.S. Government's own dependencies on critical infrastructures, assist in the development of national education and awareness programs, and coordinate legislative and public affairs. To the extent Federal efforts to protect its own critical infrastructures require strengthening the security of related computer systems, the CIAO works closely with members of the Chief Information Officers Council and other responsible officials who are responsible for the actual development and implementation of appropriate Federal computer security programs.

President Clinton has increased funding on critical infrastructure substantially during the past three years, including a 15% increase in the FY2001 budget proposal to $2.0 billion. He has also developed and requested funding on new initiatives to defend the nation's computer systems from cyber attack.

II. The Plan: Overview and Highlights

President Clinton directed the development of this Plan to chart the way toward the attainment of a national capability to defend our critical infrastructures by the end of 2003. To meet this ambitious goal, the Plan establishes 10 programs for achieving three broad objectives. They are:

Objective 1: Prepare and Prevent: Undertake those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.

> Program 1 calls for the Government and the private sector to identify significant assets, interdependencies, and vulnerabilities of critical information networks from attack, and to develop and implement realistic programs to remedy the vulnerabilities, while continuously updating assessment and remediation efforts.

Objective 2: Detect and Respond: Develop the means required to identify and assess attacks in a timely way, contain such attacks, recover quickly from them, and reconstitute those systems affected.

> Program 2 will install multi-layered protection on sensitive computer systems, including advanced firewalls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers will receive warnings from these detection devices, as well as Computer Emergency Response Teams (CERTs) and other means, in order to analyze the attacks, and assist sites in defeating attacks.
>
> Program 3 will develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with the law. It will assist, transform, and strengthen U.S. law enforcement and intelligence Agencies to be able to deal with a new kind of threat and a new kind of criminal -- one that acts against computer networks.

Program 4 calls for a more effective nationwide system to share attack warnings and information in a timely manner. This includes improving information sharing within the Federal Government and encouraging private industry, as well as state and local governments, to create Information Sharing and Analysis Centers (ISACs), which would share information among corporations and state and local Governments, and could receive warning information from the Federal Government. Program 4 additionally calls for removal of existing legal barriers to information sharing.

Program 5 will create capabilities for response, reconstitution, and recovery to limit an attack while it is underway and to build into corporate and Agency continuity and recovery plans the ability to deal with information attacks. The goal for Government and the recommendation for industry is that every critical information system have a recovery plan in place that includes provisions for rapidly employing additional defensive measures (e.g., more stringent firewall instructions), cutting off or shutting down parts of the network under certain predetermined circumstances (through enterprise-wide management systems), shifting minimal essential operations to "clean" systems, and to quickly reconstitute affected systems.

Objective 3: Build Strong Foundations: Take all actions necessary to create and support the Nation's commitment to Prepare and Prevent and to Detect and Respond to attacks on our critical information networks.

Program 6 will systematically establish research requirements and priorities needed to implement the Plan, ensure funding, and create a system to ensure that our information security technology stays abreast with changes in the threat environment.

Program 7 will survey the numbers of people and the skills required for information security specialists within the Federal Government and the private sector, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.

Program 8 will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyber-based attacks.

Program 9 will develop the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation within the Federal Government, including Congress, and between the Government and private industry.

Program 10 builds mechanisms to highlight and address privacy issues in the development of each and every program. Infrastructure assurance goals must be accomplished in a manner that maintains, and even strengthens, American's privacy and civil liberties. The Plan outlines nine specific solutions, which include consulting with various communities; focusing on and highlighting the impact of programs on personal information; committing to fair information practices and other solutions developed by various working groups in multiple industries; and working closely with Congress to ensure that each program meets standards established in existing Congressional protections.

III. The Program: Goals and Descriptions

I would like to highlight a few of the programs in the remainder of my testimony. In these programs, the Administration seeks to accomplish two broad aims of the Plan – the establishment of the U.S. Government as a model of infrastructure protection, and the development of a public-private partnership to defend our national infrastructures.

A. The Federal Government as a Model of Information Security

We often say that more than 90% of our critical infrastructures are neither owned nor operated by the Federal Government. Partnerships with the private sector and state and local governments are therefore not just needed, but are the fundamental aspect of critical infrastructure protection. Yet, the President rightly challenged the Federal Government in PDD-63 to serve as a model for critical infrastructure protection – to put our own house in order first. Given the complexity of this issue, we need to take advantage of the breadth of expertise within the Federal Government to ensure that we enlist those Agencies with special capabilities and relationships with private industry to the fullest measure in pursuit of our common goal.

The President has developed and provided full or pilot funding for the following key initiatives designed to protect the Federal Government's computer systems:

Federal Computer Security Requirements and Government Infrastructure Dependencies. One component of this effort supports aggressive, Government-wide implementation of federal computer security requirements and analysis of vulnerabilities. Thus, in support of the release of the National Plan, the President announced his intent to create a permanent Expert Review Team (ERT) at the Department of Commerce's National Institute of Standards and Technology (NIST). The ERT will be responsible for helping Agencies identify vulnerabilities, plan secure systems, and implement Critical Infrastructure Protection Plans. Pursuant to existing Congressional authorities and administrative requirements, the Director of the team would consult with the Office of Management and Budget and the National Security Council on the team's plan to protect and enhance computer security for Federal Agencies. The President's Budget for FY2001 proposes $5 million for the ERT.

Under PDD-63, the President directed the CIAO to coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. Many of the critical infrastructures that support our nation's defense and security are shared by a number of Agencies. Even within Government, critical infrastructure outages may cascade and unduly impair delivery of multiple critical services. The CIAO is coordinating an interagency effort to develop a more sophisticated identification of critical nodes and systems, and to understand their impact on national security, national economic security, and public health and safety Government-wide. These efforts support the work of the ERT in identifying critical nodes of the Government's information infrastructures that require vulnerability analyses, and provide valuable input to Agencies for planning secure computer systems and implementing computer security plans. This research, when complete, will permit the Federal Government to identify and redress its most significant critical infrastructure vulnerabilities

first, and provide the necessary framework for well informed critical infrastructure protection policy making and budget decisions.

Federal Intrusion Detection Network (FIDNet). PDD-63 marshals Federal Government resources to improve interagency cooperation in detecting and responding to significant computer intrusions into civilian Government critical infrastructure nodes. The program – much like a centralized burglar alarm system – would operate within long-standing, well-established legal requirements and Government policies covering privacy and civil liberties. FIDNet is intended to protect information on critical, civilian Government computer systems, including that provided by private citizens. It will not monitor or be wired into private sector computers. All aspects of the FIDNet will be fully consistent with all laws protecting the civil liberties and privacy rights of Americans.

To support this effort, the Administration proposes funding in the President's FY2001 Budget ($10 million) to create a centralized intrusion detection and response capability at the General Services Administration (GSA). This capability will function in consort with GSA's Federal Computer Incident Response Capability, and assist Federal Agencies to:

- detect and analyze computer attacks and unauthorized intrusions;
- share attack warnings and related information across Agencies; and
- respond to attacks in accordance with existing procedures and mechanisms.

FIDNet is intended to promote confidence in users of Federal civilian computer systems. It is important to recognize that FIDNet has a graduated system for response and reporting attack. Intrusion information would be collected and analyzed by home-Agency experts. Only data on system anomalies would be forwarded to GSA for further analysis. Thus, intrusion detection would not become a pass-through for information to the Federal Bureau of Investigation or other law enforcement entities. Law enforcement would receive information about computer attacks and intrusions only under long-standing legal rules – no new authorities are implied or envisioned by the FIDNet program.

One additional benefit of Government-wide intrusion detection is to improve computer intrusion reporting and the sharing of incident information consistent with existing government computer security policy. Various authorities require Agencies to report criminal intrusions to appropriate law enforcement personnel, which include the National Infrastructure Protection Center.

FIDNet will support law enforcement's responsibilities where cyber-attacks are of a criminal nature or threaten national security.

In short, FIDNet will:

- be run by the GSA, not the FBI;
- monitor only Federal Government networks, not monitor any private network traffic;
- operate within current legal authorities, and confer no new authorities on any Government Agency;
- be fully consistent with privacy law and practice, and

- provide a coordinated analysis process for early identification of malicious intrusion attempts against Federal networks.

Federal Cyber Services (FCS). One of the nation's strategic shortcomings in protecting our critical infrastructures is a shortage of skilled information technology (IT) personnel. Within IT, the shortage of information systems security personnel is acute. The Federal Government's shortfall of skilled information systems security personnel amounts to a crisis. This shortfall reflects a scarcity of university graduate and undergraduate information security programs and the inability of the Government to provide the salary and benefit packages necessary to compete with the private sector for the limited number of these highly skilled workers. In attacking this problem through the Federal Cyber Services initiative described below, we are leveraging the initial efforts made by the Defense Department, the National Security Agency, and some other Federal Agencies. The President's Budget for FY2001 proposes $25 million for this effort.

The Federal Cyber Services training and education initiative, highlighted by the President at the Plan's release, introduces five programs to help solve the Federal IT security personnel problem. The programs include all facets of information assurance education and training in order to address the immediate need for more skilled professionals, create a pipeline for recruitment of new professionals, and promote a national commitment to information assurance.

- a study by the Office of Personnel Management to identify and develop competencies for Federal information technology (IT) security positions, and the associated training and certification requirements.

- the development of Centers of IT Excellence to establish competencies and certify current Federal IT workers, and maintain their information security skill levels throughout their careers.

- The creation of a Scholarship for Service (SFS) program to recruit and educate the next generation of Federal IT managers by awarding scholarships for the study of information security, in return for a commitment to work for a specified time for the Federal Government. This program will also support the development of information security faculty.

- The development of a high school outreach and awareness program that will provide a curriculum for computer security awareness classes and encourage careers in IT fields.

- The development and implementation of a Federal Information Security awareness curriculum aimed at ensuring computer security literacy throughout the entire Federal workforce.

Research and Development. A key component to our ability to protect our critical infrastructures now and in the future is a robust research and development plan. As part of the structure established by PDD-63, the interagency Critical Infrastructure Coordination Group (CICG) created a process to identify technology requirements in support of the Plan. Chaired by the

Office of Science and Technology Policy (OSTP), the Research and Development Sub-Group works with Agencies and the private sector to:

- gain agreement on requirements and priorities for information security research and development;
- coordinate among Federal Departments and Agencies to ensure the requirements are met within departmental research budgets and to prevent waste or duplication among departmental efforts;
- communicate with private sector and academic researchers to prevent Federally funded R&D from duplicating prior, ongoing, or planned programs in the private sector or academia; and
- identify areas where market forces are not creating sufficient or adequate research efforts in information security technology.

That process, begun in 1998, has helped focus efforts on coordinated cross-government critical infrastructure protection research. Among the priorities identified by the process are:

- technology to support large-scale networks of intrusion detection monitors;
- artificial intelligence and other methods to identify malicious code (trap doors) in operating system code;
- methodologies to contain, stop, or eject intruders, and to mitigate damage or restore information-processing services in the event of an attack or disaster;
- technologies to increase network reliability, system survivability, and the robustness of critical infrastructure components and systems, as well as the critical infrastructures themselves; and
- technologies to model infrastructure responses to attacks or failures; identify interdependencies and their implications; and locate key vulnerable nodes, components, or systems.

The President's Budget for FY2001 proposes $606 million across all Agencies for critical infrastructure related R&D investment.

The need exists, however, to coordinate R&D efforts not just across the Federal Government, but between the public and private sectors as well. A fundamentally important initiative that has the ability to pull disparate pieces of the national R&D community into closer relationships is the Institute for Information Infrastructure Protection (I^3P). This organization is created to identify and fund research and technology development to protect America's cyberspace from attack or other failures. I will discuss the I^3P in detail when I address Public-Private Partnership issues.

Public Key Infrastructure. Protecting critical infrastructures in the Federal Government and private sectors requires development of an interoperable public key infrastructure (PKI). A PKI enables data integrity, user identification and authentication, user non-repudiation, and data confidentiality through public key cryptography by distributing digital certificates (essentially electronic credentials) containing public keys, in a secure, scalable, and reliable manner. The potential of PKI has inspired numerous projects and pilots throughout the Federal Government and private sectors. The Federal Government has actively promoted the development of PKI technology and has developed a strategy to integrate these efforts into a fully functional Federal PKI. The President's Budget for FY2001 proposes $7 million to ensure development of an interoperable Federal PKI.

To achieve the goal of an integrated Federal PKI, and protect our critical infrastructures, the Federal Government is working with industry to implement the following program of activities:

- *Connect Agency-wide PKIs into a Federal PKI*: DoD, NASA, and other Government Agencies are actively implementing Agency-wide PKIs to protect their internal critical infrastructures. While a positive step, these isolated PKIs do not protect infrastructures that cross Agency boundaries. Full protection requires an integrated, fully functional PKI.

- *Connect the Federal PKI with Private Sector PKIs*: Private sector groups are actively developing their own PKIs as well. While a positive step, these isolated PKIs do not protect infrastructures that cross Government or industry sector boundaries.

- *Encouraging development of interoperable Commercial Off-the-Shelf (COTS) PKI Products*: Limitation to a single vendor's solution can be a serious impediment, as most organizations have a heterogeneous computing environment. Consumers must be able to choose COTS PKI components that suit their needs.

- *Validating the Security of Critical PKI Components*: Protecting critical infrastructures require sound implementation. The strength of the security services provided to the critical infrastructures depends upon the security of the PKI components. Validation of the security of PKI components is needed to ensure that critical infrastructures are adequately protected. NIST is pursuing a validation program for PKI components.

- *Encouraging Development of PKI-Aware Applications*: To encourage development of PKI-aware applications, the Government is working with vendors in key application areas. One example is the secure electronic mail projects that have been performed jointly with industry.

B. Public-Private Partnership

Inter-dependent computer networks are an integral part of doing business in the Information Age. America is increasingly dependent upon computer networks for essential services, such as banking and finance, emergency services, delivery of water, electricity and gas, transportation, and voice and

data communications. New ways of doing business in the 21st century are rapidly evolving. Business is increasingly relying on E-commerce for its commercial transactions as well as for its critical operations. At the same time, recent hacking attempts at some of the most popular commercial Web sites underscore that America's information infrastructure is an attractive target for deliberate attack or sabotage. These attacks can originate from a host of sources, such as terrorists, criminals, hostile nations, or the equivalent of car thief "joyriders." Regardless of the source, however, the potential for cyber damage to our national security and economy is evident.

The infrastructures at risk are owned and operated by the private sector. The use of information technology is so embedded in the core operations and customer service delivery systems of industry that inevitably, it will be they who must work together to take the steps necessary to protect themselves. The Federal government can help. The first major step is the elevation of awareness across industry of the "business case for action" for leaders within industry. They have a commercial interest in maintaining a secure business environment that assures public confidence in their institutions. We can help identify and publicize problems as well as good practices in management policies and strategies. We can also encourage planning, promote research and development, and convene meetings. In short, we can act as a catalyst for industry to mobilize.

A strategy of cooperation and partnership between the private sector and the U.S. Government to protect the Nation's infrastructure is the linchpin of this effort. The President is committed to building partnerships with the private sector to protect our computer networks through the following initiatives:

Institute for Information Infrastructure Protection (I^3P). The Institute would identify and address serious R&D gaps that neither the private sector nor the Government's R&D community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure. First proposed by the scientists and corporate officials who served on the President's Committee of Advisors on Science and Technology, the Institute is supported by leading corporate Chief Technology Officers. The President's FY2001 Budget proposes $50 million for the Institute. Funding would be provided through the Commerce Department's National Institute of Standards and Technology (NIST) to this organization.

The Institute will work directly with private sector information technology suppliers and consumers to define research priorities and engage the country's finest technical experts to address the priorities identified. Research work will be performed at existing institutions including private corporations, universities, and non-profit research institutes. The Institute will also make provisions to accept private sector support for some research activities.

Partnership for Critical Infrastructure Security. Last month, Commerce Secretary Daley met with senior representatives from over 120 major corporations, many Fortune 500, representing owners and operators of critical infrastructures, their suppliers, and their customers, to organize a Partnership for Critical Infrastructure Security. Industry has taken the lead on this effort, and is actively pursuing ways to assure their ability to deliver critical services.

The Partnership will explore ways in which industry and Government can work together to address the risks to the nation's critical infrastructures. Federal Lead Agencies are currently building partnerships with individual infrastructure sectors in private industry, including communications, banking and finance, transportation, and energy. The Partnership will serve as a forum in which to draw these individual efforts together to facilitate a dialogue on cross-sector interdependencies, explore common approaches and experiences, and engage other key professional and business communities that have an interest in infrastructure assurance. By doing so, the Partnership hopes to raise awareness and understanding of, and to serve, when appropriate, as a catalyst for action among, the owners and operators of critical infrastructures, the risk management and investment communities, other members of the business community, and state and local Governments.

National Infrastructure Assurance Council (NIAC). President Clinton established the NIAC by Executive Order 13130 on July 14, 1999. When fully constituted, it will consist of up to 30 leaders in industry, academia, the privacy community, and state and local Government. The NIAC will provide advice and counsel to the President on a range of policy matters relating to critical infrastructure assurance, including the enhancement of public-private partnerships, generally.

IV. Conclusion

In conclusion, the National Plan is an important step forward. My staff and I are committed to building on this promising beginning, coordinating the Government's efforts into an integrated program for critical infrastructure protection in support of the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, and the Federal Government, generally. We are actively working with members of the CIO Council, as well as members of the defense, intelligence, and law enforcement agencies to develop this program. However, we have much work left to do, and I hope to work with the members of this committee, indeed with the Congress as a whole, as we wrestle with this developing field.

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

Mr. HORN. Thank you very much. I would appreciate it at this point in the record if you would submit the national plan for the record. So, without objection, it will be put right after this point.

We now go the next gentleman who is very familiar to this committee. You are doing a fine job. Mr. John Gilligan, Chief Information Officer, Department of Energy, and Co-Chair, Security, Privacy, and Critical Infrastructure Committee of the Chief Information Officer Council. Mr. Gilligan.

Mr. GILLIGAN. Thank you, Chairman Horn.

As you noted, I come before the committee speaking in both my role as Chief Information Officer of the Department of Energy and as well the Co-Chair of the Federal CIO Council Security, Privacy, and Critical Infrastructure Committee. As I prepared for this testimony, I gave a lot of thought to what I viewed were the two critical issues that I face as a Federal CIO. I would like to spend a moment addressing these issues for you.

Up-front, let me tell you that my biggest issues are not technology challenges. The primary challenge is educating and convincing line management that computers and networks, as well as the information they possess and process, should be treated and managed as mission-essential and strategic organization resources. Let me illustrate my point with an example.

Last summer, at one of the Department of Energy laboratories we conducted a security audit. The laboratory was evidenced as having the best firewall within the Department, very good security policies, and adequate protection of our classified systems. However, that same organization had a number of instances of what I refer to as no-brainer security weaknesses. For example, there were a number of computer systems that had software configurations that were years out of date.

In this case, they were not taking advantage of dozens of patches that had fielded to upgrade the security of those systems over the years. In addition, there were a number of systems where their passwords, including system administrator passwords were easily guessed, or in some cases even used the term "password." These and other weaknesses provided relative ease of a potential hacker to break into the laboratory's unclassified computer system.

As I evaluated this apparent paradox, the same organization having both the best and the worst security practices, the root issue became clear to me. The organization was not focusing on information technology as an overall laboratory resource, rather only sub-sets of the systems and networks were being pro-actively managed. Most of the unclassified computers were procured and operated as work center or personal resources.

I have found similar dichotomy at a number of other daily sites. The problem at this lab was not the absence of sound security policies or lack of security technology knowledge, but the fact that management of computers had become highly decentralized and, in many cases, was a personal task. I found that the number of system administrators approached the number of laboratory employees.

The security audit findings highlighted to the laboratory director and senior management that they had fundamental problems with information technology management. The solution required a fun-

damental change in how computers, networks were purchased, installed, and operated. I firmly believe that this is the most significant and pervasive problem facing Federal agency CIOs.

A second challenge I face is working with Federal managers in the Department of Energy in determining how much security is enough. That is, how much is adequate? In the past, primary security focus was on the protection of national security information, classified systems, and more easily controlled mainframe computers. Adequate security was defined by security gurus, in most cases, with much input from line management, and defined, in most cases, in absolute terms.

Today, we use computers for a wide variety of missions where it is not cost effective or appropriate to apply the same protection mechanism or security policies in all cases. We have information relating to national security. Personnel data and business operations must be protected to ensure confidentiality. On the other hand, we have public websites where we want to protect the integrity of the information. In addition, there are mission impact and perception factors which influence what is adequate, as well as rapidly changing threats, missions, and technologies.

Federal security policies require an assessment of risk to guide management decisions on what is adequate. Sounds easy. I would submit that it is not. The Federal Government is also held to a very high standard and one that continues to change and become more stringent over time. In my testimony, I have included some status updates within the Department of Energy on our recent security activities. I will not detail them here.

I would like to, however, turn for a few minutes to the work of the CIO Security, Privacy, and Critical Infrastructure Protection Committee, which I co-chair with Roger Baker, CIO of the Department of Commerce, and Fernando Robano, CIO of the Department of State. Our committee is developing a set of products that we believe will augment and accelerate improvements in implementing adequate levels of protection in assuring appropriate privacy of Federal information and systems.

I would like to submit for the record a brief summary of our committee activities.

[The information referred to follows:]

Initiatives and Activities of the Federal CIO Council's Security, Privacy, and Critical Infrastructure Committee.

Identify, evaluate, and disseminate best practices, including products that have been certified or accredited under recognized federal authorities (e.g. Common Criteria, National Infrastructure Assurance Plan (NIAP), etc.)

- Best Security Practices (BSPs) are essential components of sound security programs. Because no coordinated Government initiative has existed to put BSPs in the hands of Federal Organizations, the Security Practices Subcommittee was formed to collect, document and develop a web-based repository for Best Security Practices (BSPs)[1].

Promote the maintenance of up-to-date system patches, the closing of vulnerabilities, and the establishment of other warning and noticing processes to improve the security of systems by federal agencies

- The "Sample Policy Working Group" of the CIO Council has prepared a draft of a "Computer Incident Response and Handling " policy. Based on the Department of Energy's policy implemented by the Computer Incident Advisory Center, this sample policy is intended to serve as a guideline for other agencies to follow.

Identify security and privacy solutions that enable delivery of services while ensuring adequate security and privacy in a risk balanced implementation

- As the Federal government continues to create E-Government services—thus changing the way citizens and companies interact with government—a major issue is information security, including the validity, reliability and privacy of both stored and transmitted information. In light of this issue, the CIO Council is partnering with the Chief Financial Officers Council and the Information Technology Association of America to develop and identify security solutions that enable delivery of services while ensuring adequate security in a risk balanced implementation.

Work with OMB and NIST to identify draft or sample policies (e.g. model procurement guidelines for the acquisition of information assurance products, systems, and services, and model privacy impact assessments) for use by federal agencies in the areas of security and privacy

- The CIO Council has outlined a measurement framework to determine the maturity of an agency's Information Technology (IT) security program. The Information Technology (IT) Security Maturity Framework comprises six levels to guide and prioritize agency efforts as well as provide a basis to measure progress.

Lead and partner with other organizations to sponsor conferences, newsletters, and workshops to promote activities and issues in regard to PDD-63 and privacy issues (e.g. IRMCO, FOSE, E-Gov, IAC)

- The CIO Council is sponsoring Critical Infrastructure Protection Day (March 2), Security Awareness Day (TBD) and is considering several options to participate as a co-sponsor in other conferences (Defending Cyberspace '99 and National Information Systems Security Conference).

---

[1] *A best security practice is a method, proven by effective experience, that people use to perform a security-related task.*

Initiatives and Activities of the Federal CIO Council's Security, Privacy, and Critical Infrastructure Committee.

Identify funding for technological solutions that advance secure information access and exchange with privacy

- The CIO Council has identified the opportunity for organizations to submit proposals through the National Science Foundation for agencies to partner with R&D universities to address IT Security and Privacy Challenges. This funding totals a potential of $146 million.

Partner with the GITS Board to promote coordinated agency efforts to use public key technology for authentication

Mr. GILLIGAN. I would also like to highlight a few of the committee's efforts. Our project to develop and Information Technology Security Maturity Framework is intended to help guide agencies and senior government officials in establishing and maturing an effective cyber security program. Following the example of the successful Software Capability Maturity Framework developed by Carnegie Mellon University, the Information Technology Security Maturity Framework recommends the building block approach to security.

Emphasis is placed at lower levels on critical foundation activities, such as documented policy, and clearly defined assigned responsibilities, as well as robust training and security assessment of progress. I have brought a display that summarizes the six levels of security maturity described in the draft framework. The Security Committee believes that all agencies should be working toward achievement of level 2 in the near term.

This level describes what is called a documented security program. It is based on policy and guidance from the General Accounting Office, the Office of Management and Budget, and the National Institute for Standards and Technology. The committee is working to develop specific evaluation criteria, a checklist guide that could be used for level 2, as well as further definition of level 3.

We have invited the Software Engineering Institute and the General Accounting Office to participate in the refinement of the framework. The committee also has initiatives in the development of a tool that will allow us to identify and make available the Federal agency's best security practices. We are developing sample agency policies and guidelines dealing with security and privacy.

We are working to accelerate the use of so-called public key encryption. We are working with the Information Technology Association of America in the development of security solution benchmarks, linked to common electronic services such as financial track statues with the public, benefit inquiries over the web, and electronic submission of contractor pricing proposals.

I would like to conclude my remarks with some recommendations from my perspective as co-chair of the Security, Privacy, Critical Infrastructure Committee. The first two recommendations deal with funding for security. First, I recommend that organizations specifically identify and analyze their expenditures in cyber security. In this regard, I suggest that we work with the government and industry to establish and refine benchmarks against which line managers can assess whether their investment is comparable to similar organizations.

Work by the Gardner Group suggests that a reasonable range for cyber security spending is somewhere between 1 and 5 percent of an organization's spending for information technology. Second, I would recommend consideration of increased funding for a set of governmentwide security initiatives that are focused not on multiyear research or product development, but on short-term immediate operational benefits for Federal agencies.

I note that most of our CIO Council cyber security efforts are focused toward ongoing operational support. Furthermore, I recommend that we continue to tightly tie our cyber security efforts

with other initiatives to improve overall management of information technology resources from an enterprise perspective.

Finally, I suggest that we continue to focus our education efforts toward government managers. I believe managers need to know how to make risk tradeoffs. What they need is greater awareness of their responsibility in managing information technology as a strategic resource, as well as simple benchmarks and metrics, such as funding levels and a maturity framework, against which they can evaluate organization-specific risks, as well as the progress of their cyber security programs.

This concludes my testimony. I look forward to your questions.

[The prepared statement of Mr. Gilligan follows:]

STATEMENT OF

JOHN M. GILLIGAN

CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE GOVERNMENT REFORM

SUBCOMMITTE ON GOVERNMENT MANAGEMENT,

INFORMATION, AND TECHNOLOGY

MARCH 9, 2000

Chairman Horn, I want to thank you for this opportunity to appear before the Subcommittee to share my views relating to the increasingly important subject of security of Federal computer systems. I am addressing the Committee both as the Chief Information Officer for the Department of Energy, as well as Federal Co-Chair of the CIO Council's Security, Privacy and Critical Infrastructure Committee.

I will focus initially on the significant challenges that I face as CIO of a large, diverse and decentralized organization to improve computer security. Up front, let me tell you that my biggest challenges are not technology challenges. The primary challenge is educating and convincing line management that the computers and networks, as well as the information that they process, should be treated and managed as mission essential and strategic organization resources. Let me illustrate my point with an example. Last summer, we conducted an audit of security at one of DOE's laboratories. The laboratory was evaluated as having good local security policies, the best firewall in DOE, and outstanding protection of classified systems. This same organization, however, exhibited a large number of instances of what I call "no brainer" security weakness. For example, there were a number of computers with software configurations that were several years out of date -- that is, not taking advantage of dozens of security patches and upgrades -- and a significant number of systems, including system administrator's stations, had easily guessed passwords like the term "password" or in some cases no password protection. These and other weaknesses provided a relatively easy ability to break into the laboratory's unclassified systems.

As I evaluated this apparent paradox, the same organization having the best and the worst security practices, the root issue became clear. The organization was not focusing on information technology as an overall laboratory resource. Rather, only subsets of the systems and networks were being proactively managed. Most of the unclassified computers were procured and operated as "work center" or "personal" resource. I have found a similar dichotomy at other DOE sites. The problem at this lab was not the absence of sound security policies or lack of technical security knowledge, but the fact that the management of computers had become highly decentralized and in many cases was a "personal" task. I found that the numbers of systems approached the number of laboratory employees.

The security audit findings highlighted to the Laboratory Director and senior management that they had fundamental problems with information technology management. The solution required a fundamental change to how computers and networks were purchased, installed, and operated. Significant cost benefits would accrue as well. In short, this organization, and I would submit many Federal organizations, needs to move from treating computers and networks as personal or work-center tools to enterprise-wide resources requiring rigorous and consistent management. I firmly believe this is the most significant and pervasive problem facing Federal agency CIO's.

To manage information technology as an enterprise activity requires a major culture shift for many organizations. Without making this shift, as I saw at the DOE

Laboratory, world-class security protection capabilities in other parts of the organization were of little value.

A second challenge I face working with managers in DOE is determining how much security is enough: how much is adequate. In the past, primary computer security focus was on the protection of national security information and more easily controlled mainframe systems. Adequate security was defined by security "gurus," in most cases without much input from line management and in absolute terms. Today, we use computers for a wide variety of missions where it is not cost-effective or appropriate to apply the same protection mechanism or security policies in all cases. We have information relating to national security, personnel, and business operations that must be protected to ensure confidentiality. On the other hand, we have public web sites for which we want to protect the integrity of the information presented therein, and in many cases reliability of service is important. In addition, there are mission impact and perception factors that influence what is "adequate," as well as rapidly changing threats, missions, and technologies.

Federal policies require an assessment of risk to guide management decisions on what is "adequate". Sounds easy? I would submit that it is not! The Federal government is held to a very high standard, one that continues to change and become more stringent over time.

Let me turn now to a brief summary of what the Department of Energy has done over the past year to improve our computer security efforts. To start, we revised our cyber security policies to better define expectations and to require each DOE site to

document threat-based security plans based on a risk management assessment. We also clearly placed risk management and security implementation accountability in the line management chain. As I noted earlier, this is a major culture change and will take some months to be fully effective.

We have just completed an expedited program to train 1000 system administrators across the DOE complex, and we have had security awareness "stand downs" at all DOE sites to heighten management and employee awareness of all facets of security. I have doubled the size of our Department-wide team of cyber security experts -- our Computer Incident Advisory Capabilities or CIAC -- who monitor key Department cyber resources, analyze cyber incidents, and provide early warning of attacks or vulnerabilities. We are in the process of developing a DOE Cyber Security Architecture that will serve as a guide for each site in establishing site specific security implementation consistent across the DOE enterprise. In addition, we have taken a number of measures to significantly reduce the risk of inadvertent or intentional compromise of our classified data at our weapons laboratories. In summary, we have made a lot of progress since last spring when security problems at DOE made national headlines. We still have areas where additional progress is needed, but we have established what I believe is a proper, solid foundation and we are seeing rapid progress.

I would like to also comment about the work of the CIO Council Security, Privacy and Critical Infrastructure Protection Committee that I co-chair with Roger Baker, CIO of the Department of Commerce, and Fernando Burbano, CIO of the

Department of State. Our Committee is developing a set of products. We believe that these products will augment and accelerate improvements in implementing "adequate" levels of protection and ensuring appropriate privacy of Federal information and systems. I would like to submit for the record a brief summary of our specific initiatives.

I would also like to highlight a few of the Committee's efforts. Our project to develop an Information Technology Security Maturity Framework is intended to help guide agencies and senior government officials in establishing and maturing an effective cyber security program. Following the example of the successful Software Capability Maturity Framework developed by Carnegie Mellon University, the Information Technology Security Maturity Framework recommends a building block approach to security. Emphasis is placed at the lower levels on critical foundation activities such as documented policy and clearly defined assigned responsibilities, as well as robust training and security assessment progress.

I have brought a display that summarizes the six levels of security maturity described in the Framework. The Committee believes that all agencies should be working for achievement of Level 2 in the near term. This level describes a Documented Security Program and is based on policy and guidance from the GAO, OMB and NIST. The Committee is working to develop specific evaluation criteria, a checklist guide, that could be used for Level 2 as well as further definition of Level 3. We have also invited the Software Engineering Institute and GAO to participate in the refinement of the Framework. We would welcome the opportunity to work with this Committee to make

this a meaningful and effective tool for both the Executive as well as the Legislative branches.

The Committee also has developed a web-based repository for Best Security Practices (BSP), leveraging initial work done by the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). This tool supports rapid search and retrieval of exemplary security practices (tools, policies, processes) as well as on-line submission of candidate best practices. The BSP system tool is available in prototype now and will be operational in May. We are also promoting sample agency policies or guidelines dealing with privacy risk analysis and incident response and security patch distribution. Separately, the Committee is working with several government organizations to accelerate use of Public Key encryption, to improve security within the Federal government and in our interactions with the private sector.

An additional effort that we are just initiating with the support of the Chief Financial Officer's Council and the Information Technology Association of America (ITAA) is the development of security solution benchmarks linked to common electronic services such as conducting financial transactions electronically with the public, benefits inquiries over the web and electronic submission of contract or pricing proposals. This effort is specifically focused to provide managers with guidance on what government and industry believes to be an adequate level of security. Our goal is to provide a sufficiently robust set of examples, or a framework, that managers could use to assist them in addressing the question of what is adequate security in a particular application. In

addition, we are aggressively working with the Critical Infrastructure Assurance Office to promote greater awareness of Critical Infrastructure Protection requirements and methods in order to energize Federal Agency efforts in this area.

I would like to conclude my remarks with some recommendations from my perspective as co chair of the Security, Privacy, and Critical Infrastructure Protection Committee. My recommendations are provided with intent of helping to accelerate the pace of achieving a level of adequate security for Federal systems. The first two recommendations deal with funding for security. In an effort to improve visibility of cyber security, I recommend that organizations specifically identify and analyze their expenditures in cyber security. In this regard, I suggest that we work within the government and with industry to establish and refine benchmarks against which line managers can assess whether their investment level is comparable to similar organizations. The Department of Energy recently started doing this, and while this is not a perfect metric, it does allow me to engage in discussion with line managers on the question of what is adequate -- in this case how much should they be spending on security. Work by the Gartner Group suggests that a reasonable range for cyber security spending is somewhere between 1% and 5% of an organization's spending for information technology. Clearly, we will need to improve and refine these measures, but I believe there would be great benefit with focused attention on this area.

Second, I would recommend consideration of increased funding for a set of government-wide security initiatives that are focused, not on multi-year research or product development, but on short-term, immediate operational benefit for Federal agencies. I note that most of our CIO Council Cyber Security efforts are focused toward

ongoing operational support. Similar efforts by GSA and NIST focus on immediate operational support. Furthermore, I recommend that we continue to tightly tie our cyber security efforts with efforts to improve overall management of information technology resources from an enterprise-wide perspective. The personal computer and ubiquitous networks have resulted in a culture of local "ownership" and fragmented management that make it very difficult to achieve the level of security that we need and deserve. Moreover, many of our security policies focus on individual systems and fail to emphasize the necessity of enterprise-wide focus. Finally, I suggest that we continue to focus our education efforts toward government managers. I believe managers know how to make risk tradeoffs. What they need is greater awareness of their responsibilities in managing information technology as a strategic resource, as well as simple benchmarks and metrics (such as funding levels or maturity framework) against which they can evaluate organization specific risks as well as the progress of their cyber security programs.

This concludes my testimony. I look forward to your questions.

Mr. HORN. Thank you very much, Mr. Gilligan.

Our next witness is Ms. Karen Brown, the Deputy Director, National Institute of Standards and Technology, otherwise known as NIST. With the Weather Bureau there, I wonder why we cannot be MIST? Anyhow, the Department of Commerce. Thank you for coming.

Ms. BROWN. Thank you.

Thank you Mr. Chairman and members of this subcommittee for the invitation to speak to you today about computer security issues. Computer security continues to be an ongoing and challenging problem that demands the attention of the Congress, the executive branch, industry, academia, and the public. Computer security is not a narrow technical concern.

The explosive growth in electronic commerce highlights the Nation's ever-increasing dependence upon the secure and reliable operation of our computer systems. Computer security has a vital influence on our economic health and our Nation's security, and we commend the committee for your focus on this security. Today, I would like to address NIST computer security activities that contribute to improving computer security for the Federal Government and the private sector.

I would also like to briefly describe for you our proposed new program activities for next year. Under NIST statutory responsibilities, we develop standards and guidelines for agencies to help protect their sensitive, unclassified information systems. In meeting the needs of our customers in both the public and private sector, we work closely with industry, Federal agencies, testing organizations, standards groups, academia, and private sector users.

As awareness of the need for security grows, more secure products will be demanded in the marketplace. Addressing security will also help ensure that electronic commerce growth is not limited because of security concern. What does NIST do specifically? To meet these responsibilities in customer needs, we first work to improve the awareness of the need for computer security, which is an ongoing effort.

Additionally, we research new technologies and their security implications. We work to develop security standards and specifications to help users specify security needs, and establish minimum security requirements for Federal systems. We develop and manage security testing programs in cooperation with the private sector to enable users to have confidence that a product meets a security specification.

We also produce security guidance to promote security planning and secured system operations in administration. I will briefly discuss the need and benefits of each. First, there is a need for timely, relevant, and easily assessable information to raise awareness about risk, vulnerabilities, and requirements for protection of information systems. This is particularly true for new and rapidly emerging technologies which are being delivered with such speed in the Internet age.

We host and sponsor information sharing among security educators, the Federal Security Program Managers' Forum, and industry. We seek advice from our external advisory board of computer experts. We meet regularly with members of the Federal computer

security community, including the Chief Information Officer of the Security Committee, and the Critical Information Assurance Office.

We actively support information sharing through our conferences, workshops, webpages, publications, and bulletins. A second need is for research on information technology vulnerabilities and cost effective security. When we identify new technologies that could potentially influence our customer security practices, we research these technologies and their potential vulnerabilities.

We also work to find ways to apply new technologies in a secure manner. The solutions we develop are made available to both public and private users. Research helps us to find more cost effective ways to implement and address security requirements. The third is the need for standards and for ways to test that standards are properly implemented on products. For example, cryptographic algorithms and techniques are essential for protecting sensitive data and electronic transition.

NIST has long been active in developing Federal Cryptographic Standards and working in cooperation with private sector voluntary standards organizations in this area. We are currently leading a public program to develop the Advanced Encryption Standard [AES], which will serve 21st Century Security needs. Another aspect of our standards activity concerns public key and key management infrastructures.

We have been actively involved in working with industry and the Federal Government to promote the security and inter-operability of such infrastructures. Standards help users to know what security specifications may be appropriate for their needs. Testing complements this by helping users have confidence that security standards and specifications are correctly implemented in the products they buy.

Testing also helps reduce the potential vulnerabilities that products contain that could be used to attack systems. For over 5 years, we have led the Cryptographic Module Validation Program, which has now validated about 90 modules, with another 50 expected this year. This successful program utilizes private sector accredited laboratories to conduct security conformance testing of cryptographic modules against the Federal standard we developed and maintain. Many of these activities are being done in cooperation with the Defense Department's National Security Agency in our National Information Assurance Partnership.

The goal is to enable product developers to get their products tested easily and voluntarily, and for users to have access to information about test products. Under this program, we have also led the development of an international mutual recognition arrangement, whereby the results of testing in the United States are recognized by our international partners, thus reducing costs to the industry.

Advice and technical assistance for both government organizations and private sector is the fourth need. While I have given you a few examples of NIST work, I obviously have not covered everything. I want to emphasize there is still much more to be done.

Please keep in mind that approximately $6 million of direct congressional funding supports both our Federal and industry computer security responsibilities. This is plainly not enough.

Thank you.

[The prepared statement of Ms. Brown follows:]

Karen H. Brown
Deputy Director

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

before the

Committee on Government Reform
Subcommittee on Government Management,
Information, and Technology

March 9, 2000

Mr. Chairman and members of the subcommittee thank you for the invitation to speak to you today about computer security issues. I am Karen Brown, Deputy Director of the National Institute of Standards and Technology of the Department of Commerce's Technology Administration.

Computer security continues to be an ongoing and challenging problem that demands the attention of the Congress, the Executive Branch, industry, academia, and the public. Computer security is not a narrow, technical concern. The explosive growth in Electronic Commerce highlights the nation's ever increasing dependence upon the secure and reliable operation of our computer systems. Computer security, therefore, has a vital influence on our economic health and our nation's security and we commend the Committee for your focus on security.

Today I would like to address NIST's computer security activities that contribute to improving computer security for the Federal Government and the private sector. I also would like to briefly describe for you our proposed new program activities for next year as requested in the President's budget.

Under NIST's statutory federal responsibilities, we develop standards and guidelines for agencies to help protect their sensitive unclassified information systems. Additionally, we work with the information technology (IT) industry and IT users in the private sector on computer security in support of our broad mission to strengthen the U.S. economy, and especially to improve the competitiveness of the U.S. information technology industry. As awareness of the need for security grows, more secure products will be more competitive in the marketplace. Addressing security will also help ensure that Electronic Commerce growth is not limited because of security concerns.

In meeting the needs of our customers in both the public and private sector, we work closely with industry, Federal agencies, testing organizations, standards groups, academia, and private sector users. Cooperation and collaboration are essential to tackle many common problems facing users throughout the country.

What does NIST do specifically? To meet these responsibilities and customer needs, we first work to improve the awareness of the need for computer security. This helps increase demand for secure and reliable products. Additionally, we research new technologies and their security implications and vulnerabilities and develop guidance to advise users accordingly. We work to develop security standards and specifications to help users specify security needs in their procurements and establish minimum security requirements for Federal systems. We develop and manage security testing programs, in cooperation with private sector testing laboratories, to enable users to have confidence that a product meets a security specification. We also produce security guidance to promote security planning, and secure system operations and administration. I will briefly discuss the need and benefits of each.

First, there is a need for timely, relevant, and easily accessible information to raise awareness about the risks, vulnerabilities and requirements for protection of information systems. This is particularly true for new and rapidly emerging technologies, which are being delivered with such alacrity by our industry. We host and sponsor information sharing among security educators, the Federal Computer Security Program Managers' Forum, and industry. We seek advice from our advisory board of computer experts (Computer System Security and Privacy Advisory Board). We meet regularly with members of the Federal computer security community, including the Chief Information Officers' Security Committee, and the Critical Infrastructure Assurance Office. We actively support information sharing through our conferences, workshops, web pages, publications, and bulletins. Raising awareness helps ensure appropriate attention is accorded security and helps increase the demand for secure products and security services.

A second need is for research on information technology vulnerabilities and the development of techniques for the cost-effective security. When we identify new technologies that could potentially influence our customers' security practices, we research the technologies and their potential vulnerabilities. We also work to find ways to apply new technologies in a secure manner. The solutions that we develop are made available to both public and private users. Some examples are methods for authorization management and policy management, ways to detect intrusions to systems, and demonstrations of mobile agents. Research helps us find more cost-effective ways to implement and address security requirements.

Third is the need for standards, and for ways to test that standards are properly implemented in products. For example, cryptographic algorithms and techniques are essential for protecting sensitive data and electronic transactions. NIST has long been active in developing Federal cryptographic standards and working in cooperation with private sector voluntary standards organizations in this area. Moreover, in the standards area we have been working with the private sector in preparing for the future. We are leading a public process to develop the Advanced Encryption Standard (AES), which will serve 21st century security needs. Another aspect of our standards activities concerns Public Key and Key Management Infrastructures. The use of cryptographic services across networks requires the use of "certificates" that bind cryptographic keys and other security information to specific users or entities in the network. We have been actively involved in working with industry and the Federal government to promote the security and interoperability of such infrastructures.

Standards help users to know what security specifications may be appropriate for their needs. Testing complements this by helping users have confidence that security standards and specifications are correctly implemented in the products they buy. Testing also helps reduce the potential that products contain vulnerabilities that could be used to attack systems.

For over five years, we have led the Cryptographic Module Validation Program, which has now validated about 90 modules with another 50 expected this year. This successful

program utilizes private sector accredited laboratories to conduct security conformance testing of cryptographic modules against a Federal standard we develop and maintain. More recently, we have been working with the international security community to define security criteria in an international standard that can be used to develop security specifications for products, such as firewalls or operating systems. We are actively working with industry partners in the smart card, health care, and telecommunications fields to accomplish such development of specifications.

Many of these activities are being done in cooperation with the Defense Department's National Security Agency in our National Information Assurance Partnership. Private sector laboratories are being accredited under our National Voluntary Laboratory Accreditation program to conduct such testing. The effort involves developing testing competencies and a process for accrediting testing organizations. The goal is to enable product developers to get their products tested easily and voluntarily, and for users to have access to information about tested products. Under this program we have also led the development of an international mutual recognition arrangement whereby the results of testing in the U.S. are recognized by our international partners, thus reducing the costs to industry.

Advice and technical assistance for both government organizations and private sector users is the fourth need. For example, we have issued guidance including telecommuting and security, security concerns inherent in PBX technology, security requirements in Public Key Infrastructure (PKI) implementation, use of firewalls, and intrusion detection in networks. We also provide program guidance to agencies and are working to complete a document on security program metrics and self-assessment. The information and guidelines that we have developed are available to all users free-of-charge via our web site. We also support agencies on specific security projects on a cost-reimbursable basis when NIST expertise is required.

While I have given you a few examples of NIST's work, I obviously have not covered everything. I want to emphasize that there is still much more to be done to address the continuing challenges of computer security. To put our program in perspective, please keep in mind that approximately $6 million of direct Congressional funding supports both our Federal and industry computer security responsibilities. (In addition, we receive approximately $2 million in outside agency funding to provide technical assistance on particular projects.) This is plainly not enough.

As reflected in the requests made in the President's FY 2001 budget, NIST needs additional resources to help improve the security posture of the Federal government. Looking at the critical information infrastructures of the nation, we also need substantial investments in security research to find ways to protect our infrastructures.

To address the need for additional research to protect our critical infrastructures, the White House has proposed establishing a $50 million Institute for Information Infrastructure Protection (IIIP), which was initially recommended by the President's Committee of Advisors on Science & Technology (PCAST). The IIIP will identify and

fill the gaps not being met by private sector market demands or Government agency mission objectives in critical infrastructure protection and provide a strong and secure foundation to protect the various critical infrastructures upon which the Nation's security and economy rely. IIIP's R&D, which will aim to help prevent security problems will include work that can be applied to protect multiple sectors' infrastructures, and thus will complement sector-specific R&D underway elsewhere in the government and private sector. This initiative will help strengthen the focused existing and planned security architectures within the critical infrastructure sectors and help prepare the owners/operators of those infrastructures to survive potential hostile activities. The IIIP will not have any direct role in support of law enforcement or deterring attacks, but will fund R&D to develop new generations of IT security solutions that would be made available for DoJ/FBI, other agencies, and the private sector can use to prevent and respond to future cyber-threats. The IIIP will be a partnership among industry, academia and the government (including both state and local governments). At the core of the partnership is IIIP's selection of information infrastructure protection R&D focus areas, which will rely heavily on advice and guidance obtained from outside experts.

The security of Federal systems must also be improved. These systems contain sensitive information about our citizens and provide services upon which our citizens' safety and well-being depend. The government should exert leadership and set an example for the nation in protecting against risks and vulnerabilities. Two of the budget proposals focus primarily upon the security of Federal systems. Specifically, we propose to establish an Expert Review Team (comprised of eight FTE's) to advise agencies of their vulnerabilities, help prioritize and develop strategies for security fixes, assist agencies in preparing for future security threats, and help agencies plan for security in new system developments. This preventative approach will complement the reporting activities of programs such as FedCIRC. Secondly, we seek a five million dollar increase to enable additional critical activities in the area of cryptography, security management and best practices guidance, and the protection of supervisory control systems.

So let me close by again emphasizing that our national commitment to improve security must be increased. NIST stands ready to play a key role through supporting the proposed Institute, leading the Expert Review Team, and conducting additional work to developing needed security guideline and standards, research in security technology, leading testing programs, and raising awareness and demand for security products and services. This will augment the already important activities we have underway. We look forward to continuing this work, and believe that your support of the critical new activities would help us to do so.

I will be pleased to answer any questions.

Mr. HORN. Thank you very much. That was very helpful testimony. We now go to our last witness on this panel. I must say, Mr. Pethia, everywhere I talked and saw people in the last 3 weeks putting this panel together, the first magic word was Carnegie Mellon. So, we are glad to have you come here. We hope to visit your campus sometime. You can show us around.

Mr. Rich Pethia is the director, Computer Emergency Response Team Coordination Centers, Software Engineering Institute at Carnegie Mellon University in Pittsburgh.

Mr. PETHIA. Mr. Chairman and members of the subcommittee, I would like to thank you for the opportunity to come and talk to you today about computer security. Today, I would like to describe a number of the trends that impact security on the Internet. I will illustrate the results of those trends and then outline some steps that I think will help us all effectively manage the increasing risk of damage from cyber attacks.

My perspective comes from the work that we do with the CERT Coordination Center. The Center is charted to respond to security emergencies on the Internet, and to work with both technology producers and technology users to facilitate response to major security problems. Since 1988, we have handled over 24,000 separate security incidents, and analyzed more than 1,500 separate computer vulnerabilities.

The current state of Internet security is cause for concern. The vulnerabilities associated with technology used on the Internet put government, business, and individuals at risk. Security is influenced by many factors. An organization that wishes to improve its security has to deal with a lot of issues. First of all, the Internet itself is growing at an amazing rate.

As the technology is being distributed, so is the management of that technology. System administration and management often fall upon people who do not have the training, skills, resources, or interest needed to operate their system securely. This problem is about to get worse. Now that we have direct Internet connection to homes, schools, libraries, and other venues that do not have training and security staff.

These always-on rarely protected systems will allow attackers to continue to add new systems to their arsenal of captured weapons. Intruder tools are becoming increasingly sophisticated and also becoming increasingly user-friendly and widely available. This technology is evolving like any other.

Sophisticated developers of intruder programs package their tools in user-friendly forms and make them widely available. As a result, even unsophisticated intruders can use them.

On the technology side, when vendors release patches or upgrades to solve security problems, organizations' systems often are not upgraded. The job may be too time consuming, too complex, or just too low a priority for the system administration or staff to handle. There is little evidence of improvement in the security features of most products. Today, we continue to receive new vulnerability reports in second generation and third generation products.

Developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities and doing the engineering work necessary to remove them. Finally, engineering for ease

of use is not being matched by engineering for ease of secure administration. Today, we would all find it ludicrous to safely operate and drive an automobile, a person would have to be a master mechanic.

Yet, today we expect our computer users and novice system administrators to have detailed technical knowledge of all the intricacies and nuances of the technology. We are simply developing technology that is not fit for use in today's environment. Because of these and other factors, organizations and individuals who are using the Internet become vulnerable to various kinds of cyber attack, including the denial-of-service attacks that were widely publicized in February.

The key point about this attack, this attack type, is that although an organization may be able to harden its own systems to help prevent having its systems used as a part of a distributed attack vehicle, there is essentially nothing a site can do with currently available technology to prevent becoming a victim of these coordinated denial-of-service attacks.

The best an organization can do today is get ready to respond and have its response capabilities in place, should it ever become the victim of one of these attacks. These attacks work by having intruders compromise vulnerable systems. They collect these vulnerable systems into aggregated attack networks. These networks act in unison to attack a single victim.

The network can be activated remotely at a later site by a master computer. Communication between the master and the networks is encrypted, often making it difficult to locate the master. Once activated, these tools proceed on their own. They are rapidly evolving. Individual nodes in the attack network can be automatically reprogrammed to change the type of attack so that it becomes increasingly difficult to build defenses against this technology.

Clearly, we have entered a new era in the Internet, where the power of the Internet itself is now being used to attack people who are connected to it. At the CERT, we constantly monitor trends and watch for new attacks and tools. We became aware of this new form of denial-of-service attack in late August, early September 1999. Denial-of-service attacks are not new.

These kinds of attacks have been around since 1994, with significant increases in 1996 and 1998. By the end of September, it was evident that this was a new form of attack. It was something we had never seen before. We called together a workshop of 30 international experts who came together for 2 days in Pittsburgh and produced a paper that explains the threat posed by these intruder tools, as well as guidance to organizations about how to protect themselves and be prepared, and how to be ready to respond.

This paper, along with other advisories, were issued to the community in December. We have had a series of communications out to the Internet community. The problem is serious. It is complex. A combination of approaches must be used to reduce the risks associated with this ever-increasing dependence on the Internet. First of all, we need better ability to collect, analyze, and disseminate information on assurance issues.

A lot of what we do today is reactive. We see a problem. We analyze it. We understand what just happened. That is no longer ade-

quate. New forms of attack are now happening at Internet speed, both automated attacks, like these distributed denial-of-service attacks, as well as new forms of viruses, such as Melissa that showed up in March of this year.

Today, we need to find analysis methods that build a predictive early warning capability. We need to be able to understand what is going to happen before it happens, which means we need new ways of analysis. In addition, better attention paid to collecting information. There has been a lot of discussion and debate about instrumenting networks to collect data to watch the traffic on the network to anticipate what the problems might be.

Certainly, there is a need to be concerned about privacy, but we have to find some way to balance our need to collect information about the operation of networks with our need to keep individual transactions and user's activities private. Until we get a better view into what is happening on our networks, we are going to have a very difficult time defending against new forms of attack.

Third, we need to invest in better education and training to raise the level of security and security awareness. In particular, we need to focus on bringing the understanding of security issues to senior and middle management in government, as well as in industry. Until there is management commitment, and management commitment of resource to solve this problem, little is going to happen. Part of that includes encouraging the development of comprehensive security programs with well-defined responsibilities for managers, users, and system administrators.

Finally, all of this is only going to help us mitigate the problem, stem the flow of quality that we are having. It will not solve the problem. In order to get ahead of this problem, we need to support research and development activities that will lead to a new generation of technology on the Internet and other broad-scale networks. Systems that are easier to secure, systems that do not require so much constant attention, systems that do not repeat the vulnerabilities of the past, the long-term solution is better technology.

That is going to take years. Until we get there, we need better management approaches. Thank you.

[The prepared statement of Mr. Pethia follows:]

Computer Security

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

Before the
Committee on Government Reform
Subcommittee on Government Management,
Information, and Technology

March 9, 2000

Introduction

Mr. Chairman and Members of the Subcommittee on Government Management, Information, and Technology:

My name is Rich Pethia. I am the director of the CERT® Centers, which include the CERT® Coordination Center (CERT/CC) and the CERT® Analysis Center (CERT/AC). The centers are part of the Software Engineering Institute (SEI) at Carnegie Mellon University. Thank you for the opportunity to testify on the issue of computer security. Today I will describe a number of trends that have an impact on the security of the Internet, illustrate the results of those trends by describing the recent distributed denial-of-service attacks (DDoS), and outline steps I believe are needed to effectively manage the increasing risk of damage from cyber attacks.

My perspective comes from the work we do at the CERT Centers. The CERT Coordination Center was established at the SEI in 1988, after an Internet "worm" stopped 10% of the computers connected to the Internet. This program—the first Internet security incident to make headline news—was the wake-up call for network security. The CERT/CC went into operation in just two weeks with a charter to respond to security emergencies on the Internet and to work with both technology producers and technology users to facilitate response to emerging security problems. In the first full year of operation, 1989, The CERT/CC responded to 132 computer security incidents. In 1999, the staff responded to more than 8,000 incidents. In total, the CERT/CC staff has handled well over 24,000 incidents and analyzed more than 1,500 computer vulnerabilities. More details about our work are attached to the end of this testimony (see *Meet the CERT Coordination Center*).

The recently established CERT Analysis Center addresses the threat posed by rapidly evolving, technologically advanced forms of cyber attacks. Working with sponsors and associates, the CERT/AC collects and analyzes information assurance data to develop detection and mitigation strategies that provide high-leverage solutions to information assurance problems, including countermeasures for new vulnerabilities and emerging threats. The CERT Analysis Center builds upon the work of the CERT Coordination Center. The CERT Analysis Center extends current incident response capabilities by developing and transitioning protective measures and mitigation strategies to defend against advanced forms of attack before they are launched. Additionally, it provides the public and private sectors with opportunities for much-needed collaboration and information sharing to improve cyber attack defenses.

Vulnerability of the Internet and World Wide Web

Vulnerabilities associated with the Internet put government, business, and individual users at risk. Security measures that were appropriate for mainframe computers and small, well-defined networks inside an organization, are not effective for the Internet, a complex, dynamic world of interconnected networks with no clear boundaries and no central control. Because the Internet was not originally designed with security in mind, it is difficult to ensure the integrity, availability, and privacy of information. The Internet was designed to be "open," with distributed control and mutual trust among users. As a result, control is in the hands of users, not in the hands of the provider; and use cannot be administered by a central authority. Furthermore, security issues are not well understood and are rarely given high priority by software developers, vendors, network managers, or consumers.

In addition, because the Internet is digital, not physical, it has no geographic location and no well-defined boundaries. Traditional physical "rules" are difficult or impossible to apply. Instead, new

knowledge and a new point of view are required to understand the workings and the vulnerabilities of the Internet.

Another factor is the approach typically taken by intruders. There is (loosely) organized development in the intruder community, with only a few months elapsing between "beta" software and active use in attacks. Moreover, intruders take an open-source approach to development. One can draw parallels with open system development: there are many developers and a large, reusable code base.

Intruder tools are becoming increasingly sophisticated and also becoming increasingly user friendly and widely available. For the first time, intruders are developing techniques to harness the power of hundreds of thousands of vulnerable systems on the Internet. Using what are called distributed-system attack tools, intruders can involve a large number of sites simultaneously, focusing all of them to attack one or more victim hosts or networks. The sophisticated developers of intruder programs package their tools into user-friendly forms and make them widely available. As a result, even unsophisticated intruders can use them.

The current state of Internet security is the result of many additional factors, such as the ones listed below. A change in any one of these can change the level of Internet security and survivability.

- Because of the dramatically lower cost of communication on the Internet, use of the Internet is replacing other forms of electronic communication. The Internet itself is growing at an amazing rate. An additional 16 million computers connected to the Internet between July 1999 and January 2000, bringing the estimated total to 72.4 million.

- There is a continuing movement to distributed, client-server, and heterogeneous configurations. As the technology is being distributed, so is the management of that technology. In these cases, system administration and management often fall upon people who do not have the training, skill, resources, or interest needed to operate their systems securely. The number of directly connected homes, schools, libraries and other venues without trained system administration and security staff is rapidly increasing. These "always-on, rarely-protected" systems allow attackers to continue to add new systems to their arsenal of captured weapons.

- Internet sites have become so interconnected and intruder tools so effective that the security of any site depends, in part, on the security of all other sites on the Internet.

- The difficulty of criminal investigation of cyber crime coupled with the complexity of international law mean that successful apprehension and prosecution of computer criminals is unlikely, and thus little deterrent value is realized.

- The Internet is becoming increasingly complex and dynamic, but among those connected to the Internet there is a lack of adequate knowledge about the network and about security. The rush to the Internet, coupled with a lack of understanding, is leading to the exposure of sensitive data and risk to safety-critical systems. Misconfigured or outdated operating systems, mail programs, and Web sites result in vulnerabilities that intruders can exploit. Just one naive user with an easy-to-guess password increases an organization's risk.

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

- As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. Among security-conscious organizations, there is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations that have applied a "silver bullet" are lulled into a false sense of security and become less vigilant, but single solutions applied once are neither foolproof nor adequate. Solutions must be combined, and the security situation must be constantly monitored as the technology changes and new exploitation techniques are discovered.

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

- Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.

Distributed Denial-of-Service Tools

Because of the factors described above, organizations and individuals using the Internet are vulnerable to many kinds of cyber attacks, including the denial of service attacks that were widely publicized in February. Distributed attack tools based on the client/server model have become increasingly common. In recent months, there has been an increase in the development and use of distributed network sniffers, scanners, and denial-of-service tools. Attacks using these tools can involve a large number of sites simultaneously and be focused to attack one or more victim hosts or networks.

Damaged systems include those used in the attack as well as the targeted victim. For the victim, the impact can be extensive. For example, in a denial-of-service attack using distributed technology, the attacked system observes simultaneous attacks from all the nodes at once—flooding the network normally used to communicate and trace the attacks and preventing any legitimate traffic from traversing the network.

There are indications that the processes for discovering vulnerable sites, compromising them, installing daemons (programs used in the attack), and concealing the intrusion are largely

automated, with each step being performed in "batch" mode against many machines in one "session." Attack daemons have been discovered on a variety of operating systems with varying levels of security and system management.

It is critical to plan and coordinate before an attack to ensure an adequate response when an attack actually happens. Since the attack methodology is complex and there is no single-point solution or "silver bullet," resolution and restoration of systems may be time-consuming. The bottom line is that an organization's systems may be subject at any time to distributed attacks that are extremely difficult to trace or defend against. Only partial solutions are available.

Although an organization may be able to "harden" its own systems to help prevent having its systems used as part of a distributed attack, there is essentially nothing a site can do with currently available technology to prevent becoming a victim of, for example, a coordinated network flood. The impact upon the site and its operations is dictated by the (in)security of other sites and the ability of a remote attacker to implant the tools and, subsequently, to control and direct multiple systems worldwide to launch an attack. The result may be reduced or unavailable network connectivity for extended periods of time, possibly days or even weeks depending upon the number of sites attacking and the number of possible attack networks that could be activated in parallel or sequentially.

Coordinated attacks across national boundaries have occurred. The tools and attacks demonstrate that a network that optimizes its technology for speed and reliability at the expense of security may experience neither speed nor reliability, as intruders abuse the network or deny its services. The intruder technology is evolving, and future tools may be more difficult to defeat.

Here are key points to note about distributed denial-of-service tools:

- Intruders compromise systems through other means and install DDoS tools.
- The DDoS tools often are equipped with a variety of different attack types.
- Computers that are compromised with DDoS tools are aggregated into networks.
- These networks act in unison to attack a single victim. Any computer on the Internet can be a victim.
- The networks can be activated remotely at a later date by a "master" computer.
- Communication between the master computer and the networks can be encrypted and obfuscated to make it very difficult to locate the master.
- Once activated, the tools typically proceed on their own. No further communication is necessary on the part of the intruder—it is not possible to discover the master by tracing an ongoing attack. However, there may be evidence on one or more of the machines in the DDoS network regarding the true location of the master.
- Attacks from the network to the victim typically employ techniques designed to obfuscate the true location of the machines in the DDoS network. This makes it difficult to recognize the traffic (and thus block it), to trace the traffic back from the victim to the nodes in the network, and to analyze an attack while it is in progress.
- There are no proactive technical steps an organization can take to prevent becoming a victim. Everyone's security is intertwined. However, by preparing a response in advance, sites can significantly diminish the impact. For information on preparing to respond to these attacks, see the report on the results of a workshop that the CERT/CC organized in November 1999 to

address the imminent threat posed by the tools:

http://www.cert.org/reports/dsit_workshop.html

- The tools are rapidly evolving but have not reached their full potential by any means.
- The magnitude of the attacks can overwhelm even the largest networks.
- Intruders are building networks of machines used in these attacks ranging in size from tens to hundreds of machines. It is likely that some networks are much larger.
- The individual nodes in the network can be automatically updated by the master machines, enabling rapid evolution of tools on an existing base of compromised machines.
- A variety of tools are available to detect DDoS tools. Each of these tools has weaknesses, and none is a general-purpose solution. Some of these tools can be found at

  http://www.fbi.gov/nipc/trinoo.htm
  http://staff.washington.edu/dittrich/misc/stacheldraht.analysis
  http://www.iss.net/cgi-bin/dbt-display.exe/db_data/press_rel/release/122899199.plt
  http://www.sans.org/y2k/stacheldraht.htm

- Currently, there is a nearly inexhaustible supply of computers with well-known vulnerabilities that intruders can compromise and install DDoS tools on. Additionally, many networks are configured in a way that facilitates the obfuscation techniques used by intruders to conceal their identity. Information about how to configure networks properly is available at

  http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2267.txt

- An archive of DDoS tools can be found at

  http://packetstorm.securify.com/distributed/

- The CERT/CC published advisories and other documents about this topic; for example,

  http://www.cert.org/advisories/CA-2000-01.html
  http://www.cert.org/advisories/CA-99-17-denial-of-service-tools.html
  http://www.cert.org/tech_tips/denial_of_service.html

Role of the CERT/CC in Distributed Denial-of-Service Attacks

The CERT Coordination Center constantly monitors trends and watches for new attack techniques and tools. As the attached timeline shows, we began seeing distributed denial-of-service tools in early 1998. Denial-of-service attacks are not new. (See, for example, the attached CERT advisories CA-96.21 on TCP "syn" flooding and CA-98.01 on "smurf" attacks, as well a "tech tip" on denial-of-service attacks, which the CERT/CC wrote for system administrators in 1997.)

By fall 1999, it was evident that steps needed to be taken to deal with increasingly sophisticated intruder tools before they—and attacks using them—became widespread. On November 2-4, 1999, the CERT/CC invited 30 experts from around the world to address the problem of network attack tools that use distributed systems in increasingly sophisticated ways. During the Distributed-Systems Intruder Tools (DSIT) Workshop, participants discussed a large number of approaches to preventing, detecting, and responding to distributed attacks. The CERT/CC invited people who could contribute technically to the solutions regardless of their position in their home organization or their "political" stature in the community. Thus, the workshop effectively provided a venue for experts around the world to share experiences, gain a common understanding, and creatively brainstorm possible responses and solutions to this category of attack before the dissemination of the attack tools—and the attacks themselves—became widespread. A paper, *Results of the Distributed-Systems Intruder Tools Workshop* (attached), is available on the CERT web site (www.cert.org). This paper explains the threat posed by these intruder tools and provides suggestions for safeguarding systems from this type of malicious activity.

The CERT/CC continues to collaborate with the participants who attended the workshop and with an additional group of security experts to address the ongoing problem.

Earlier this month, Rich Pethia of the CERT/CC, Alan Paller of the SANS Institute, and Gene Spafford of Purdue University, prepared a *Consensus Roadmap for Defeating Distributed Denial of Service Attacks* (attached) for the Partnership for Critical Infrastructure Security. The most current version can be found on the SANS Institute Web site (www.sans.org).

Recommended Solutions

The problem is serious and complex, and a combination of approaches must be used to reduce the risks associated with the ever-increasing dependence on the Internet and the possibility of a sustained attack on it. Effective solutions require multi-disciplinary and cross-domain cooperation that includes information sharing and joint development of comprehensive solutions, as well as support for a long-term research agenda.

Support an established center for collecting, analyzing, and disseminating information assurance information.

The nature of threats to the Internet is changing rapidly and will continue to do so for the foreseeable future. The combination of rapidly changing technology, rapidly expanding use, and the continuously new and often unimagined uses of the Internet creates a volatile situation in which the nature of threats and vulnerabilities is difficult to assess and even more difficult to predict.

To help ensure the survivability of the Internet, and the information infrastructure as a whole, it is essential to continuously monitor and analyze cybersecurity threats and vulnerabilities and to identify trends in intrusion activity. The organization doing this should collect, analyze, and report on quantity, trends, and character of cybersecurity incidents. To obtain the required information, the organization must be well trusted throughout the community. Given the universal concerns about privacy and confidentiality and the inherently voluntary nature of reporting, the collection organization should be neither government nor commercial. Nor can it be responsible for public policy, investigation, enforcement, or other activities perceived as conflicting. Organizations that have suffered attacks are often unwilling to discuss their problems for fear of loss of confidence by their customers.

The CERT/CC is establishing an analysis center to expand its work of collecting and analyzing information assurance data. The goals are to identify trends and to develop detection and mitigation strategies that provide high-leverage solutions to information assurance problems, including countermeasures for new vulnerabilities and emerging threats. It takes advantage of the information dissemination channels already in place at the CERT/CC.

The CERT Analysis Center extends current incident response capabilities by developing and transitioning protective measures and mitigation strategies to defend against advanced forms of attack before they are launched. Additionally, it provides the public and private sectors with opportunities for much-needed collaboration and information sharing to improve cyber attack defenses.

The strength of the CERT/AC will come from contributions across the information technology community. SEI affiliate and visiting scientist programs provide an established model to integrate the contribution of diverse participants. These programs bring together members of academic, industry, and government organizations to address problems and meet common needs. The center provides the means for private sector firms to collaborate with technical staff from the CERT/AC on leading-edge information assurance research.

Research includes intruder tool analysis; that is, in-depth analysis of new and emerging cyber-attack methods in order to develop defenses and countermeasures that can be deployed before these new attack methods are widely used. Equally important is in-depth analysis of information technology vulnerabilities and malicious code in order to develop techniques that are effective at eliminating entire classes of vulnerabilities and entire families of malicious code.

Support the growth and use of global detection mechanisms.
Among the ways to gain a global view of threats are to use the experience and expertise of incident response teams to identify new threats and vulnerabilities. The incident response team at the CERT/CC and other response teams have demonstrated their effectiveness at discovering and dealing with vulnerabilities and incidents. Ongoing operation and expansion of open, wide area networks will benefit from stronger response teams and response infrastructures.

Similarly, it is important to encourage Internet service providers to develop security incident response teams and other security improvement services for their customers. Many network service providers are well positioned to offer security services to their clients. These services should include helping clients install and operate secure network connections as well as mechanisms to rapidly disseminate vulnerability information and corrections.

Support education and training to raise the level of security.
As noted earlier, the security of each system on the Internet depends on the security of all other systems on the network. The interconnectedness and interdependency of systems pose a serious threat to commerce.

The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life. As a result, many users of the Internet who have no more understanding of the technology than they do of the engineering behind other infrastructures. Similarly, many system administrators lack adequate knowledge about the network and about security, even while the Internet is becoming increasingly complex and dynamic. To encourage "safe computing," there are steps we believe the government could take:

- **Support the development of educational material and programs about cyberspace for all users, both adults and children.** There is a critical need for education and increased awareness of the characteristics, threats, opportunities, and appropriate behavior in cyberspace. This need goes far beyond protecting children from pornography. It relates to how quickly cyberspace will be developed, to how rapidly and effectively cyberspace will be exploited for social and economic benefit, and to what influences will drive the economic, social, and political directions in cyberspace.

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

- **Invest in awareness campaigns that stress the need for security training for system administrators, network managers, and chief information officers.** Building, operating, and maintaining secure networks are difficult tasks; and there are few educational and training programs that prepare people to perform them. Training will also enhance the ability of administrators and managers to use available technology for configuration management, network management, auditing, intrusion detection, firewalls, guards, wrappers, and cryptography.

  Furthermore, the increasing need for such roles in organizations of many sizes and descriptions has led to assigning information security responsibilities to inexperienced personnel with little or no training. In the short term, the greatest need is for short "how to" and "what to be aware of" courses. In the long term, there should be undergraduate-level or master's-level specialties in network and information security.

Support research and development in the areas of security and survivability of unbounded systems' architectures with distributed control.
It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches. The research agenda should seek new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Among the activities should be these:

- Develop science-based engineering methods for information assurance specification and design through innovative adaptation of existing formal specification theory originally developed for other purposes.

- Develop prototype tools to assess information assurance properties of specifications and designs by adapting core algorithms of existing theory-based analytical tools that were originally developed for other purposes.

---

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

- Leverage past investment that has produced an extensive, but little used, body of knowledge in rigorous methods for system analysis and design in general, and for security and survivability in particular. Work needs to be done to extend and unify previous research to deal with new problems of information assurance in a coherent and integrated manner, and to make innovative use of existing research, technology, and tools.

Conclusion

The Internet has proven to be an engine that is driving a revolution in the way government, companies, and individuals conduct their business. Capitalizing Internet opportunities, however, brings a new set of risks—risks that must be effectively managed. Because of the interconnectedness and interdependence among computer systems on the Internet, the security of each system depends on the security of all other systems on the network. For the United States to thrive on the Internet, cyber security efforts need to focus on reporting and monitoring threats and vulnerabilities, education and training, and research and development.

Synopsis of Richard D. Pethia's Testimony to the Subcommittee on Government Management, Information, and Technology March 9, 2000

Rich Pethia is the director of the CERT® Centers, which are part of the Software Engineering Institute at Carnegie Mellon University, Pittsburgh, Pennsylvania.

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

- The CERT/CC was established in 1988, after an Internet "worm" became the first Internet security incident to make headline news, serving as a wake-up call for Internet security. The CERT/CC was operational less than two weeks later.
- Since 1988, the CERT/CC has responded to 24,000 computer security incidents and analyzed 1,500 vulnerabilities. In 1999 alone, it handled 8,000 incidents.
- The CERT/CC constantly monitors trends and watches for new attack techniques and tools.
- The CERT/CC coordinated the private-public sector effort to address distributed denial-of-service (DDoS) intruder tools prior to the recent attacks.

Factors Affecting Security

- The security of each system on the Internet depends on the security of all other systems on the network. The interconnectedness and interdependency of systems pose a serious threat.
- The Internet was not originally designed with security in mind, so it is difficult to ensure the integrity, availability, and privacy of information.
- The Internet was designed to be "open," with distributed control and mutual trust among users – no central authority or control.
- Security issues are not well understood and are rarely given high priority by software developers, vendors, network managers, or consumers.
- The sophisticated developers of intruder programs package their tools into user-friendly forms and make them widely available. As a result, even unsophisticated intruders can use them.
- Bottom line: Cyber attacks will continue with more frequency and more severity.

Recommended Actions to Address Threats to Network Security

- Cyber security efforts needed for US government and business to operate on the Internet should include increased and sustained resources to
    - support public-private collaborations, such as those by the CERT/CC
    - monitor and report threats, vulnerabilities, and trends
    - transfer security knowledge through education and training
    - research solutions to the complex problems of security and survivability
    - provide trusted, immediate, and expert response to security problems

The CERT Coordination Center stands ready to work with Congress, federal agencies and departments, industry, academia, and the world-wide network of other incident response teams to address this serious problem.

Attachments to the Testimony

of Richard D. Pethia

CERT® Centers

March 9, 2000

Meet the CERT® Coordination Center

A Chronology of CERT Coordination Center Involvement with Distributed Denial of Service

CERT Incident Note IN-2000-01	Windows Based DDoS Agents
CERT Advisory CA-2000-01	Denial-of-Service Developments
CERT Advisory CA-99-17	Denial-of-Service Tools
CERT Incident Note IN-99-07	Distributed Denial of Service Tools
CERT Incident Note IN-99-06	Distributed Network Sniffer
CERT Advisory CA-98.01	"smurf" IP Denial-of-Service Attacks
CERT Advisory CA-96.21	TCP SYN Flooding and IP Spoofing Attacks
CERT Tech Tip	Denial of Service

Results of the Distributed-Systems Intruder Tools Workshop

Consensus Roadmap for Defeating Distributed Denial of Service Attacks

Meet the CERT® Coordination Center

Overview

The CERT Coordination Center (CERT/CC) is located at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the Internet Worm incident, which brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. Since then, the CERT/CC has helped to establish other response teams and our incident handling practices have been adopted by more than 80 response teams around the world.

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

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

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

Areas of Work

Survivable Network Management

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

Security improvement practices provide concrete, practical guidance that will help organizations improve the security of their networked computer systems. These practices are published as

---

security improvement modules and focus on best practices that address important problems in network security. We have published seven modules, incorporating more than 80 recommended practices and technology-specific implementations. A complete list of the modules, practices, and implementations can be found on the CERT/CC Web site at

http://www.cert.org/security-improvement/

Our self-directed security evaluation method will give organizations a comprehensive, repeatable technique that can be used to identify risk in their networked systems and keep up with changes over time. The method takes into consideration assets, threats, and vulnerabilities (both organizationally and technologically) so that the organization gains a comprehensive view of the state of its systems' security.

Additionally, the adaptive security management process, that we have under development, builds on and incorporates our work on security practices and self-directed security evaluations. The adaptive process presents a structure that an organization can use to develop and execute a plan for continuously improving the security of its networked systems.

Survivable Network Technology

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

http://www.cert.org/research

Incident Response

We provide assistance to computer system administrators in the Internet community who report security problems. When a security breach occurs, we help the administrators of the affected sites to identify and correct the vulnerabilities that allowed the incident to occur. We will also coordinate the response with other sites affected by the same incident. When a site specifically requests, we will facilitate communication with law enforcement agencies.

Since our inception in 1988, we have received more than 260,000 email messages and 17,600 hotline calls reporting computer security incidents or requesting information. We have handled more than 24,300 computer security incidents and received more than 1,500 vulnerability reports.

The scale of emerging networks and the diversity of user communities make it impractical for a

---

CERT Coordination Center description

single organization to provide universal support for addressing computer security issues. Therefore, the CERT/CC staff regularly works with sites to help them form incident response teams and provides guidance to newly formed teams.

FedCIRC - We are responsible for the day-to-day operations of FedCIRC, the Federal Computer Incident Response Capability, an organization that provides incident response and other security-related services to Federal civilian agencies. FedCIRC is managed by the General Services Administration (GSA).

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

Incident and Vulnerability Analysis

Our ongoing computer security incident response activities help the Internet community to deal with its immediate problems while allowing us to understand the scope and nature of the problems and of the community's needs. Our understanding of current security problems and potential solutions comes from first-hand experience with compromised sites on the Internet and subsequent analysis of security incidents, intrusion techniques, configuration problems, and software vulnerabilities.

The CERT/CC has become a major reporting center for incidents and vulnerabilities because we have an established reputation for discretion and objectivity. Organizations trust us with sensitive information about security compromises and network vulnerabilities because we have proven our ability to keep their identities and other sensitive information confidential. Our connection with the Software Engineering Institute and Carnegie Mellon University contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias. As a result of the community's trust, we are able to obtain a broad view of incident and vulnerability trends and characteristics.

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

To achieve long-term benefit from vulnerability analysis, we have begun to identify the underlying software engineering and system administration practices that lead to vulnerabilities and, conversely, practices that prevent vulnerabilities. We will broadly disseminate this information to practitioners and consumers and influence educators to include it in courses for future software engineers and system administrators. Only when software is developed and installed using defensive practices will there be a decrease in the expensive, and often haphazard, reactive use of patches and workarounds.

CERT Coordination Center description

Knowledgebase Development

We are developing a knowledgebase that will help to capture and effectively use information related to network survivability and security. The work includes developing processes and tools to support the increasing complexity of handling incidents, analyzing vulnerabilities, and managing the volume of information that is essential to the CERT/CC mission. We are forming collaborative relationships with other organizations to support this work.

Education and Training

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

http://www.cert.org/training/index.html

Information Dissemination

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

- telephone and email
  hotline: (412) 268-7090
  email:cert@cert.org
  mailing list: cert-advisory-request@cert.org
- USENET newsgroup: comp.security.announce
- World Wide Web: http://www.cert.org
- anonymous FTP:ftp://ftp.cert.org/pub/

Since beginning operation in 1988, the we have handled more than 17,600 hotline calls and 260,600 mail messages. We have published 290 security alerts (advisories, vendor-initiated bulletins*, incident notes, vulnerability notes, and CERT summaries).

* Publication of vendor-initiated bulletins was discontinued in 1999.

Publications

Advisories - CERT/CC advisories address Internet security problems. They offer an explanation of the problem, information that helps you determine if your site has the problem, fixes or workarounds, and vendor information. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and the existence of a software

---

CERT Coordination Center description

patch or workaround. On the day of release, we send advisories to a mailing list, post them to the USENET newsgroup comp.security.announce and make them available on the CERT Web site at http://www.cert.org/advisories/.

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

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

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

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

Advocacy and Other Interactions with the Community

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

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

The CERT/CC was a founding member of FIRST, and staff members continue to be active participants in FIRST. A current list of FIRST members is available from www.first.org/team-info/. More than 80 teams belonged to FIRST, and membership applications for additional teams

---

CERT Coordination Center description

are pending.

Internet Engineering Task Force

Members of our staff influence the definition of Internet protocols through participation in the Internet Engineering Task Force (IETF); a member of our staff sits on the Security Area Advisory Group to ensure that the CERT/CC perspective is brought to bear on all new standards activities.

Vendor Relations

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

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

External Events

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

Media Relations

Internet security issues increasingly draw the attention of the media. The headlines, occasionally sensational, report only a small fraction of the events that are reported to the CERT/CC. Even so, accurate reporting on security issues can raise the awareness of a broad population to the risks they face on the Internet and steps they can take to protect themselves. Ultimately, the increased visibility of security issues may lead consumers to demand increased security in the computer systems and network services they buy.

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

In 1999, the CERT/CC has been covered in radio, television, print, and online media around the world, including *US News and World Report*, *USA Today*, the *San Jose Mercury News*, *The New York Times*, *The Wall Street Journal*, *The Washington Post*, the *Chicago Sun-Times*, *The Toronto Star*, the *Ottowa Citizen*, Agence France Presse, Deutsche Presse-Agentur, the Xinhua News Agency, MSNBC, Ziff-Davis ZDNET, BBC London, National Public Radio, ABC, CNN, NBC, and more.

CERT Coordination Center description

Appendix A: The CERT/CC Charter

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

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

Appendix B: The CERT/CC and the Internet Community

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

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

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

---

CERT Coordination Center description

the absence of a major threat, we do not publicly disclose vulnerabilities until a repair or workaround has been developed.

Last updated February 16, 2000

CERT Coordination Center description

A Chronology of CERT® Coordination Center Involvement with Distributed Denial-of-Service Tools

The CERT® Coordination Center (CERT/CC) has handled ongoing reports of intruders installing distributed denial-of-service (DDoS) intruder tools. The tools that we have encountered use distributed technology to create large networks of hosts capable of launching large coordinated packet flooding denial-of-service attacks. We have seen distributed tools installed on hosts that have been compromised through the exploitation of known vulnerabilities. In particular, various RPC services have been exploited.

Since the use of DDoS tools was first detected, we have been engaged in collaboration with technical experts from around the world to develop mitigation strategies. A brief chronology of CERT/CC activity follows.

- Early 1998
  The CERT/CC begins to see signs of the use of distributed systems in tools such as "Fapi." Reports of its use "in the wild" first begin to surface.

- Late July 1999
  The CERT/CC begins receiving reports of sites finding Trinoo "daemons" (and have continued to receive reports as of the date of this chronology).

- 09 September 1999
  A discussion of DSoS appears in an issue of the "hacker" magazine *Phrack* (Vol 9, Issue 55, File 09 and Vol 9, Issue 55, File 16).
  Please see http://www.phrack.com/search.phtml?issueno=55&r=0

- October 1999
  The CERT/CC begins receiving reports of sites finding Tribal Flood Net (TFN) "daemons" (and have continued to receive reports).

- 01 October 1999
  The CERT/CC issues a special communication[1] (SC-99.41) describing Trinoo activity.

- 08 October 1999
  The CERT/CC issues another special communication (SC-99.42) describing Trinoo activity in further detail as well as distributed sniffer activity.

- 25 October 1999
  The CERT/CC publishes an incident note (IN-99-06: Distributed Network Sniffer) on reports of distributed tools being used to exploit systems.
  Please see attached or http://www.cert.org/incident_notes/IN-99-06.html

- 02-04 November 1999
  The CERT/CC hosts the Distributed-Systems Intruder Tools (DSIT) Workshop in Pittsburgh.
  Please see attached or http://www.cert.org/reports/dsit_workshop.pdf

- 18 November 1999
  The CERT/CC publishes an incident note (IN-99-07: Distributed Denial of Service Tools) on reports of DSIT being used to exploit systems.
  Please see attached or http://www.cert.org/incident_notes/IN-99-07.html

[1] Special Communications are informal descriptions of problems, which we send to CERT/CC sponsors.

- 08 December 1999
  The CERT/CC publishes a report (*Results of the Distributed Systems Intruder Tools Workshop*) produced by participants in the DSIT Workshop.
  Please see attached or http://www.cert.org/reports/dsit_workshop.html

- 20 December 1999
  The CERT/CC issues a special communication (SC-99.54) describing Tribal Flood Net 2000 (TFN2K).

- 22 December 1999
  The CERT/CC issues another special communication (SC-99.55) further describing TFN2K activity.

- 23 December 1999
  The CERT/CC issues a special communication (SC-99.56) with updated information on TFN2K activity and one on another denial-of-service attack method (SC-99.57).

- 27 December 1999
  The CERT/CC issues a special communication (SC-99.58) providing information regarding TFN2K and Mac Attack.

- 28 December 1999
  The CERT/CC issues advisory CA-99-17 discussing denial-of-service tools.
  Please see attached or http://www.cert.org/advisories/CA-99-17.html

- 31 December 1999
  The CERT/CC issues two special communications (SC-99.59 and SC-99.59a) on Stacheldraht and one (SC-99.60) update on denial-of-service activities.

- 3 January 2000
  The CERT/CC publishes advisory CA-2000-01 describing recent developments in denial-of-service attacks, sending a preliminary version early in the day in a Special Communication to sponsors (SC-2000.01).
  Please see attached or http://www.cert.org/advisories/CA-2000-01.html

- 7 January 2000
  The CERT/CC issues a special communication (SC-2000.01) providing an update on denial-of-service attacks.

- 9 January 2000
  Another update on denial-of-service attacks is issued in special communication SC-2000.08.

- 10 January 2000
  The CERT/CC issues a special communication to sponsors (SC-2000.09) discussing packet processing performance issues.

- 18 January 2000
  The CERT/CC issues a special communication (SC-2000.11) on another possible distributed denial-of-service tool.

- 28 February 2000
  The CERT/CC publishes an incident note (IN-2000-01) on Windows-based distributed denial-of-service agents.
  Please see attached or http://www.cert.org/incident_notes/IN-2000-01.html

CERT® Incident Note IN-2000-01

Windows Based DDOS Agents

Date: Monday February 28, 2000

Description:

We have received reports indicating intruders are beginning to deploy and utilize windows based denial of service agents to launch distributed denial of service attacks. On Feburary 16th we began receiving reports of a program called "service.exe" that appears to be a Windows version of trinoo. This program listens on UDP port 34555. More details about this tool are available on Gary Flynn's web site at:

http://www.jmu.edu/info-security/engineering/issues/wintrino.htm

We have seen two almost identical versions of the "service.exe" program to date (they vary by 12 bytes but produce the same results for strings(1)). The binaries we have seen have one of the following MD5 checksums:

MD5 (service.exe) = 03fe58987d7dc07e736c13b8bee2e616

MD5 (service.exe) = 1d45f8425ef969eba40091e330921757

In at least one incident, machines runing the "service.exe" program were also running backoriface. We have also received reports of administrators finding other "remote administration" intruder tools on machines that were running "service.exe".

Note that the tool TFN2K, first released in December 1999, will run on Windows NT. The existance of distributed denial of service tools for Windows platforms is not new; however, we are beginning to receive reports of these tools being installed on compromised systems.

Impact:

Windows machines have been used as intermediaries in various types of denial of service attacks for years; however, the development and deployment of the technology to use Windows machines as agents in a distributed denial of service attacks represents an overall increase in the threat of denial of service attacks.

Solution:

Standard safe computing practices will prevent intruders from installing the service.exe program on your machine(s).

- Don't run programs of unknown origin, regardless of who sent you the program. Likewise, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- it might be a Trojan horse.

- Before opening any email attachments, be sure you know what the source of the attachment was. It is not enough that the mail originated from an address you recognize. The Melissa virus spread precisely because it originated from a familiar address. Malicious code might be distributed in amusing or enticing programs. If you must open an attachment before you can verify the source, do so in an isolated environment. If you are unsure how to proceed, contact your local technical support organization.
- Be sure your anti-virus software is, and remains, up-to-date.
- Some products, such as Microsoft Office, Lotus Notes and others, include the ability to execute code embedded in documents. For any such products you use, disable the automatic execution of code embedded in documents. For example, in Microsoft Word 97, enable the "Macro Virus Protection" feature by choosing Tools-Options-General and selecting the appropriate checkbox. In Lotus Notes 4.6, set a restrictive Execution Control List (ECL) by setting the options found in File-Tools-User Preferences-Security Options to restrict the execution of code to trusted signers. For other products, consult your documentation.
- Use data-integrity tools. Data-integrity tools use strong cryptography to help you determine which files, if any, may have changed on a system. This may be crucial information to determine the most appropriate response to a security event. The use of these tools requires that they be installed before a security event has taken place.
- Avoid the use of MIME types that cause interpreters or shells to be invoked.
- Be aware of the risks involved in the use of "mobile code" such as Active X, Java, and JavaScript. It is often the case that electronic mail programs use the same code that web browsers use to render HTML. Vulnerabilities that affect ActiveX, Java, and Javascript often are applicable to electronic mail as well as web pages.

Author: Jed Pickel

This document is available from: http://www.cert.org/incident_notes/IN-2000-01.html

---

CERT/CC Contact Information

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

CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890

U.S.A.

CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

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

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

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

Getting security information

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

http://www.cert.org/

To be added to our mailing list for advisories and bulletins, send email to cert-advisory-request@cert.org and include `SUBSCRIBE your-email-address` in the subject of your message.

CERT® Advisory CA-2000-01 Denial-of-Service Developments

This advisory is being published jointly by the CERT Coordination Center and the Federal Computer Incident Response Capability (FedCIRC).

Original release date: January 3, 2000
Source: CERT/CC and FedCIRC

Systems Affected

- All systems connected to the Internet can be affected by denial-of-service attacks.

I. Description

Continued Reports of Denial-of-Service Problems

We continue to receive reports of new developments in denial-of-service tools. This advisory provides pointers to documents discussing some of the more recent attacks and methods to detect some of the tools currently in use. Many of the denial-of-service tools currently in use depend on the ability of an intruder to compromise systems first. That is, intruders exploit known vulnerabilities to gain access to systems, which they then use to launch further attacks. For information on how to protect your systems, see the solution section below.

Security is a community effort that requires diligence and cooperation from all sites on the Internet.

Recent Denial-of-Service Tools and Developments

One recent report can be found in CERT Advisory CA-99-17.

A distributed denial-of-service tool called "Stacheldraht" has been discovered on multiple compromised hosts at several organizations. In addition, one organization reported what appears to be more than 100 different connections to various Stacheldraht agents. At the present time, we have not been able to confirm that these are connections to Stacheldraht agents, though they are consistent with an analysis provided by Dave Dittrich of the University of Washington, available at

http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

Also, Randy Marchany of Virginia Tech released an analysis of a TFN-like toolkit, available at

http://www.sans.org/y2k/TFN_toolkit.htm

The ISS X-Force Security Research Team published information about trin00 and TFN in their December 7 Advisory, available at

http://xforce.iss.net/alerts/advise40.php3

A general discussion of denial-of-service attacks can be found in a CERT/CC Tech Tip available at

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

II. Impact

Denial-of-service attacks can severely limit the ability of an organization to conduct normal business on the Internet.

III. Solution

Solutions to this problem fall into a variety of categories.

Awareness

We urge all sites on the Internet to be aware of the problems presented by denial-of-service attacks. In particular, keep the following points in mind:

- Security on the Internet is a community effort. Your security depends on the overall security of the Internet in general. Likewise, your security (or lack thereof) can cause serious harm to others, even if intruders do no direct harm to your organization. Similarly, machines that are not part of centralized computing facilities and that may be managed by novice or part-time system administrators or may be unmanaged, can be used by intruders to inflict harm on others, even if those systems have no strategic value to your organization.
- Systems used by intruders to execute denial-of-service attacks are often compromised via well-known vulnerabilities. Keep up-to-date with patches and workarounds on all systems.
- Intruders often use source-address spoofing to conceal their location when executing denial-of-service attacks. We urge all sites to implement ingress filtering to reduce source address spoofing on as many routers as possible. For more information, see RFC2267.
- Because your security is dependent on the overall security of the Internet, we urge you to consider the effects of an extended network or system outage and make appropriate contingency plans where possible.
- Responding to a denial-of-service attack may require the cooperation of multiple

parties. We urge all sites to develop the relationships and capabilities described in the results of our recent workshop *before* you are a victim of a distributed denial-of-service attack. This document is available at

http://www.cert.org/reports/dsit_workshop.pdf

Detection

A variety of tools are available to detect, eliminate, and analyze distributed denial-of-service tools that may be installed on your network.

The National Infrastructure Protection Center has recently announced a tool to detect trin00 and TFN on some systems. For more information, see

http://www.fbi.gov/nipc/trinoo.htm

Part of the analysis done by Dave Dittrich includes a Perl script named *gag* which can be used to detect stacheldraht agents running on your local network. See Appendix A of that analysis for more information.

Internet Security Systems released updates to some of their tools to aid sites in detecting trin00 and TFN. For more information, see

http://www.iss.net/cgi-bin/dbt-display.exe/db_data/press_rel/release/122899199.plt

Prevention

We urge all sites to follow sound security practices on all Internet-connected systems. For helpful information, please see

http://www.cert.org/security-improvement

http://www.sans.org

Response

For information on responding to intrusions when they do occur, please see

http://www.cert.org/nav/recovering.html

http://www.sans.org/newlook/publications/incident_handling.htm

The United States Federal Bureau of Investigation is conducting criminal investigations involving TFN where systems appears to have been compromised. U.S. recipients are encouraged to contact their local FBI Office.

We thank Dave Dittrich of the University of Washington, Randy Marchany of Virginia Tech, Internet Security systems, UUNet, the http://www.y2k.gov/Y2K-ICC, the National Infrastructure Protection Center, Alan Paller and Steve Northcutt of The SANS Institute, The MITRE Corporation, Jeff Schiller of The Massachusetts Institute of Technology, Jim

Ellis of Sun Microsystems, Vern Paxson of Lawrence Berkeley National Lab, and Richard Forno of Network Solutions.

This document is available from: http://www.cert.org/advisories/CA-2000-01.html

---

CERT/CC Contact Information

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

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

CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

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

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

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

Getting security information

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

http://www.cert.org/

To be added to our mailing list for advisories and bulletins, send email to cert-advisory-request@cert.org and include `SUBSCRIBE your-email-address` in the subject of your message.

Trademark Office.

CERT® Advisory CA-99-17 Denial-of-Service Tools

Original release date: December 28, 1999, 15:00 EST (GMT -0500)
Last Updated: December 28, 1999, 20:00 EST (GMT -0500)
Source: CERT/CC

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

Systems Affected

- All systems connected to the Internet can be affected by denial-of-service attacks. Tools that run on a variety of UNIX and UNIX-like systems and Windows NT systems have recently been released to facilitate denial-of-service attacks. Additionally, some MacOS systems can be used as traffic amplifiers to conduct a denial-of-service attack.

I. Description

New Distributed Denial-of-Service Tools

Recently, new techniques for executing denial-of-service attacks have been made public. A tool similar to Tribe FloodNet (TFN), called Tribe FloodNet 2K (TFN2K) was released. Tribe FloodNet is described in http://www.cert.org/incident_notes/IN-99-07.html#tfn.

Like TFN, TFN2K is designed to launch coordinated denial-of-service attacks from many sources against one or more targets simultaneously. It includes features designed specifically to make TFN2K traffic difficult to recognize and filter, to remotely execute commands, to obfuscate the true source of the traffic, to transport TFN2K traffic over multiple transport protocols including UDP, TCP, and ICMP, and features to confuse attempts to locate other nodes in a TFN2K network by sending "decoy" packets.

TFN2K is designed to work on various UNIX and UNIX-like systems and Windows NT.

TFN2K obfuscates the true source of attacks by spoofing IP addresses. In networks that employ ingress filtering as described in [1], TFN2K can forge packets that appear to come from neighboring machines.

Like TFN, TFN2K can flood networks by sending large amounts of data to the victim machine. Unlike TFN, TFN2K includes attacks designed to crash or introduce instabilities in systems by sending malformed or invalid packets. Some attacks like this are described in

http://www.cert.org/advisories/CA-98-13-tcp-denial-of-service.html

http://www.cert.org/advisories/CA-97.28.Teardrop_Land.html

Also like TFN, TFN2K uses a client-server architecture in which a single client, under the control of an attacker, issues commands simultaneously to a set of TFN2K servers. The servers

then conduct the denial-of-service attacks against the victim(s). Installing the server requires that an intruder first compromise a machine by different means.

Asymmetric traffic from MacOS 9

MacOS 9 can be abused by an intruder to generate a large volume of traffic directed at a victim in response to a small amount of traffic produced by an intruder. This allows an intruder to use MacOS 9 as a "traffic amplifier," and flood victims with traffic. According to [3], an intruder can use this asymmetry to "amplify" traffic by a factor of approximately 37.5, thus enabling an intruder with limited bandwidth to flood a much larger connection. This is similar in effect and structure to a "smurf" attack, described in

http://www.cert.org/advisories/CA-98.01.smurf.html

Unlike a smurf attack, however, it is not necessary to use a directed broadcast to achieve traffic amplification.

II. Impact

Intruders can flood networks with overwhelming amounts of traffic or cause machines to crash or otherwise become unstable.

III. Solution

The problem of distributed denial-of-service attacks is discussed at length in [2], available at

http://www.cert.org/reports/dsit_workshop.pdf

Managers, system administrators, Internet Service Providers (ISPs) and Computer Security Incident Response Teams (CSIRTs) are encouraged to read this document to gain a broader understanding of the problem.

For the ultimate victim of distributed denial-of-service attacks

Preparation is crucial. The victim of a distributed denial-of-service attack has little recourse using currently available technology to respond to an attack in progress. According to [2]:

> *The impact upon your site and operations is dictated by the (in)security of other sites and the ability of of a remote attackers to implant the tools and subsequently to control and direct multiple systems worldwide to launch an attack.*

Sites are strongly encouraged to develop the relationships and capabilities described in [2] *before* you are a victim of a distributed denial-of-service attack.

For all Internet Sites

System and network administrators are strongly encouraged to follow the guidelines listed in [2]. In addition, sites are encouraged to implement ingress filtering as described in [1]. CERT/CC recommends implementing such filtering on as many routers as practical. This method is not foolproof, as mentioned in [1]:

While the filtering method discussed in this document does absolutely nothing to protect against flooding attacks which originate from valid prefixes (IP addresses), it will prohibit an attacker within the originating network from launching an attack of this nature using forged source addresses that do not conform to ingress filtering rules.

Because TFN2K implements features designed specifically to take advantage of the granularity of ingress filtering rules, the method described in [1] means that sites may only be able to determine the network or subnet from which an attack originated.

Sites using manageable hubs or switches that can track which IP addresses have been seen at a particular port or which can restrict which MAC addresses can be used on a particular port may be able to further identify which machine(s) is responsible for TFN2K traffic. For further information, consult the documentation for your particular hub or switch.

The widespread use of this type of filtering can significantly reduce the ability of intruders to use spoofed packets to compromise or disrupt systems.

Preventing your site from being used by intruders

TFN2K and similar tools rely on the ability of intruders to install the client. Preventing your system from being used to install the client will help prevent intruders from using your systems to launch denial-of-service attacks (in addition to whatever damage they may cause to your systems).

Popular recent attacks can be found at

http://www.cert.org/current/current_activity.html

Sites are encouraged to regularly visit this page and address any issues found there.

For the "Mac Attack"

Apple has developed a patch, as described in Appendix A. Please see the information there.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive or develop more information. If you do not see your vendor's name in Appendix A, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A. Vendor Information

Apple Computer

OT Tuner 1.0 switches off an option in Open Transport that would cause a Macintosh to respond to certain small network packets with a large Internet Control Message Protocol (ICMP) packet. This update prevents Macintosh computers from being the cause of certain types of Denial of Service (DOS) issues.

The update is available from our software update server at

http://asu.info.apple.com/swupdates.nsf/artnum/n11559

In addition, it will soon be available via the automatic update feature that is part of Mac OS 9.

References

[1] RFC2267, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing , P. Ferguson, D. Senie, The Internet Society, January, 1998, available at http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2267.txt

[2] Results of the Distributed-Systems Intruder Tools Workshop, The CERT Coordination Center, December, 1999, available at http://www.cert.org/reports/dsit_workshop.pdf

[3] The "Mac Attack," a Scheme for Blocking Internet Connections, John A. Copeland, December, 1999, available at http://www.csc.gatech.edu/~copeland. Temporary alternate URL: http://people.atl.mediaone.net/jacopeland

---

The CERT Coordination Center thanks Jeff Schiller of the Massachusetts Institute of Technology, Professor John Copeland and Jim Hendricks of the Georgia Institute of Technology, Jim Ellis of Sun Microsystems, Wietse Venema of IBM, Rick Forno of Network Solutions, Inc., Dave Dittrich of the University of Washington, Steve Bellovin of AT&T, Jim Duncan and John Bashinski of Cisco Systems, and MacInTouch for input and technical assistance used in the construction of this advisory.

This document is available from: http://www.cert.org/advisories/CA-99-17-denial-of-service-tools.html

---

CERT/CC Contact Information

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

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

CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

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

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

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

Getting security information

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

http://www.cert.org/

To be added to our mailing list for advisories and bulletins, send email to cert-advisory-request@cert.org and include `SUBSCRIBE your-email-address` in the subject of your message.

Revision History

```
December 28, 1999:  Initial release
December 28, 1999: Added information regarding a patch from Apple
```

CERT® Incident Note IN-99-07

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

Distributed Denial of Service Tools

Updated: December 8, 1999 (added DSIT Workshop paper and IN-99-05)
Thursday, November 18, 1999

Overview

We have received reports of intruders installing distributed denial of service tools. Tools we have encountered utilize distributed technology to create large networks of hosts capable of launching large coordinated packet flooding denial of service attacks.

We have seen distributed tools installed on hosts that have been compromised due to exploitation of known vulnerabilities. In particular, we have seen vulnerabilities in various RPC services exploited. For more information see the following CERT Incident Notes:

IN-99-04, Similar Attacks Using Various RPC Services

IN-99-05, Systems Compromised Through a Vulnerability in am-utils

Two of the tools we have seen are known as ***trinoo*** (or trin00) and ***tribe flood network (or TFN)***. These tools appear to be undergoing active development, testing, and deployment on the Internet.

Descriptions

- Trinoo
- Tribe Flood Network

Trinoo

Trinoo is a distributed tool used to launch coordinated UDP flood denial of service attacks from many sources. For more information about various UDP flood attacks, please see CERT Advisory CA-96.01. A trinoo network consists of a small number of servers, or *masters*, and a large number of clients, or *daemons*.

A denial of service attack utilizing a trinoo network is carried out by an intruder connecting to a trinoo master and instructing that master to launch a denial of service attack against one or more IP addresses. The trinoo master then communicates with

the daemons giving instructions to attack one or more IP addresses for a specified period of time.

1. intruder ------- master; destination port 27665/tcp
2. master ------- daemons; destination port 27444/udp
3. daemons ------- UDP flood to target with randomized destination ports

The binary for the trinoo daemon contains IP addresses for one or more trinoo master. When the trinoo daemon is executed, the daemon announces it's availability by sending a UDP packet containing the string "*HELLO*" to it's programmed trinoo master IP addresses.

daemon ------- masters; destination port 31335/udp

The trinoo master stores a list of known daemons in an encrypted file named "..." in the same directory as the master binary. The trinoo master can be instructed to send a broadcast request to all known daemons to confirm availability. Daemons receiving the broadcast respond to the master with a UDP packet containing the string "PONG".

1. intruder ------- master; destination port 27665/tcp
2. master ------- daemons; destination port 27444/udp
3. daemons ------- master; destination port 31335/udp

All communications to the master on port 27665/tcp require a password, which is stored in the daemon binary in encrypted form. All communications with the daemon on port 27444/udp require the UDP packet to contain the string "l44" (that's a lowercase L, not a one).

The source IP addresses of the packets in a trinoo-generated UDP flood attack are not spoofed in versions of the tool we have seen. Future versions of the tool could implement IP source address spoofing. Regardless, a trinoo-generated denial of service attack will most likely appear to come from a large number of different source addresses.

We have seen trinoo daemons installed under a variety of different names, but most commonly as

- ns
- http
- rpc.trinoo
- rpc.listen
- trinix

- rpc.irix
- irix

Running *strings* against the daemon and master binaries produces output similar to this (we have replaced master IP address references in the daemon binary with X.X.X.X)

trinoo daemon	**trinoo master**
socket	---v
bind	v1.07d2+f3+c
recvfrom	trinoo %s
%s %s %s	l44adsl
aIf3YWfOhw.V.	sock
PONG	OnmlVNMXqRMyM
HELLO	15:08:41
X.X.X.X	Aug 16 1999
X.X.X.X	trinoo %s [%s:%s]
X.X.X.X	bind
	read
	HELLO
	... rest omitted

Tribe Flood Network

TFN, much like Trinoo, is a distributed tool used to launch coordinated denial of service attacks from many sources against one or more targets. In additional to being able to generate UDP flood attacks, a TFN network can also generate TCP SYN flood, ICMP echo request flood, and ICMP directed broadcast (e.g., smurf) denial of service attacks. TFN has the capability to generate packets with spoofed source IP addresses. Please see the following CERT Advisories for more information about these types of denial of service attacks.

CA-96.01, TCP SYN Flooding and IP Spoofing Attacks

CA-98.01, "smurf" IP Denial of Service Attacks

A denial of service attack utilizing a TFN network is carried out by an intruder instructing a client, or *master*, program to send attack instructions to a list of TFN servers, or *daemons*. The daemons then generate the specified type of denial of service attack against one or more target IP addresses. Source IP addresses and source ports can be randomized, and packet sizes can be altered.

A TFN master is executed from the command line to send commands to TFN daemons. The master communicates with the daemons using ICMP echo reply packets with 16 bit binary values embedded in the ID field, and any arguments embedded in the data portion of packet. The binary values, which are definable at compile time, represent the various instructions sent between TFN masters and daemons.

Use of the TFN master requires an intruder-supplied list of IP addresses for the daemons. Some reports indicate recent versions of TFN master may use blowfish encryption to conceal the list of daemon IP addresses. Reports also indicate that TFN may have remote file copy (e.g., rcp) functionality, perhaps for use for automated deployment of new TFN daemons and/or software version updating in existing TFN networks.

We have seen TFN daemons installed on systems using the filename ***td***. Running strings on the TFN daemon binary produces output similar to this.

```
%d.%d.%d.%d
ICMP
Error sending syn packet.
tc: unknown host
3.3.3.3
mservers
randomsucks
skillz
rm -rf %s
ttymon
rcp %s@%s:sol.bin %s
nohup ./%s
X.X.X.X
X.X.X.X
lpsched
sicken
in.telne
```

Solutions

Distributed attack tools leverage bandwidth from multiple systems on diverse networks to produce very potent denial of service attacks. To a victim, an attack may appear to come from many different source addresses, whether or not IP source address spoofing is employed by the attacker. Responding to a distributed attack requires a high degree of communication between Internet sites. Prevention is not straight forward because of the interdependency of site security on the Internet; the tools are typically installed on compromised systems that are outside of the administrative control of eventual denial of service attack targets.

There are some basic suggestions we can make regarding distributed denial of service attacks:

- **Prevent installation of distributed attack tools on your systems**

  Remain current with security-related patches to operating systems and applications software. Follow security best-practices when administrating networks and systems.

- **Prevent origination of IP packets with spoofed source addresses**

For a discussion of network ingress filtering, refer to

RFC 2267, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

- **Monitor your network for signatures of distributed attack tools**

  Sites using intrusion detection systems (e.g., IDS) may wish to establish patterns to look for that might indicate trinoo or TFN activity based on the communications between master and daemon portions of the tools. Sites who use pro-active network scanning may wish to include tests for installed daemons and/or masters when scanning systems on your network.

- **If you find a distributed attack tool on your systems**

  It is important to determine the role of the tools installed on your system. The piece you find may provide information that is useful in locating and disabling other parts of distributed attack networks. We encourage you to identify and contact other sites involved.

- **If you are involved in a denial of service attack**

  Due to the potential magnitude of denial of service attacks generated by distributed networks of tools, the target of an attack may be unable to rely on Internet connectivity for communications during an attack. Be sure your security policy includes emergency out-of-band communications procedures with upstream network operators or emergency response teams in the event of a debilitating attack.

In November 1999, experts addressed issues surrounding distributed-systems intruder tools. The DSIT Workshop produced a paper where workshop participants examine the use of distributed-system intruder tools and provide information about protecting systems from attack by the tools, detecting the use of the tools, and responding to attacks.

Results of the Distributed-Systems Intruder Tools Workshop

Acknowledgments

The CERT/CC would like to acknowledge and thank our constituency and our peers for important contributions to the information used in this Incident Note.

CERT® Incident Note IN-99-06

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

Distributed Network Sniffer

Monday, October 25, 1999

Overview

We have received reports of intruders using distributed network sniffers to capture usernames and passwords. The distributed sniffer consists of a client and a server portion. The sniffer clients have been found exclusively on compromised Linux hosts.

Description

The following characteristics may be present on compromised hosts running the sniffer client:

- The sniffer clients have been found exclusively on compromised Linux hosts. Some reports indicate a vulnerability in the cron daemon may be used to leverage privileged access. We suspect user accounts with compromised passwords may be used to gain initial access.
- The executing sniffer binary may appear in the process list using a deceptive name, such as in.telnetd. Here is an example of the client as found in a process list of a compromised host:

```
in.telnetd ARGS=/sbin/init 59300 NO_MOD_PARMS=install
ARGS=/USR/SBIN/CRON EMB= ARG=/tmp/passwd LOGHOST=xxx.xxx.xxx.xxx
```

  The value of LOGHOST appears to be one or more IP addresses for remote sniffer servers.

- The binary /sbin/init may be replaced with an intruder-supplied binary, with the original moved to /dev/init. The malicious /sbin/init binary makes use of kernel modules to conceal system changes. An existing /dev/init copy may be visible to stat() if it's full path is given (e.g., "ls -l /dev/init").
- UDP packets containing username and password information may be sent to one or more remote sniffer servers using source port 21845/udp.

The characteristics of the sniffer server include these:

- Appears to listen for incoming UDP packets from sniffer clients on port

21845/udp.

- May run as an ordinary user without privileges.

Solutions

If you believe a host has been compromised, we encourage you to disconnect the host from the network and review our steps for recovering from a root compromise:

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

We encourage you to ensure that your hosts are current with security patches or work-arounds for well-known vulnerabilities.

CERT* Advisory CA-98.01

Original issue date: Jan. 05, 1998
Last revised: August 24, 1998 Updated vendor information for Data General Corporation.

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

"smurf" IP Denial-of-Service Attacks

This advisory is intended primarily for network administrators responsible for router configuration and maintenance.

The attack described in this advisory is different from the denial-of-service attacks described in CERT advisory CA-97.28.

The CERT Coordination Center has received reports from network service providers (NSPs), Internet service providers (ISPs), and other sites of continuing denial-of-service attacks involving forged ICMP echo request packets (commonly known as "ping" packets) sent to IP broadcast addresses. These attacks can result in large amounts of ICMP echo reply packets being sent from an intermediary site to a victim, which can cause network congestion or outages. These attacks have been referred to as "smurf" attacks because the name of one of the exploit programs attackers use to execute this attack is called "smurf."

The CERT/CC urges you to take the steps described in Section III to reduce the potential that your site can be used as the origination site (Sec. III.C) or an intermediary (Sec. III.A.) in this attack. Although there is no easy solution for victim sites, we provide some recommendations in Sec. III.B.

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

The two main components to the smurf denial-of-service attack are the use of forged ICMP echo request packets and the direction of packets to IP broadcast addresses.

The Internet Control Message Protocol (ICMP) is used to handle errors and exchange

control messages. ICMP can be used to determine if a machine on the Internet is responding. To do this, an ICMP echo request packet is sent to a machine. If a machine receives that packet, that machine will return an ICMP echo reply packet. A common implementation of this process is the "ping" command, which is included with many operating systems and network software packages. ICMP is used to convey status and error information including notification of network congestion and of other network transport problems. ICMP can also be a valuable tool in diagnosing host or network problems.

On IP networks, a packet can be directed to an individual machine or broadcast to an entire network. When a packet is sent to an IP broadcast address from a machine on the local network, that packet is delivered to all machines on that network. When a packet is sent to that IP broadcast address from a machine outside of the local network, it is broadcast to all machines on the target network (as long as routers are configured to pass along that traffic).

IP broadcast addresses are usually network addresses with the host portion of the address having all one bits. For example, the IP broadcast address for the network 10.0.0.0 is 10.255.255.255. If you have subnetted your class A network into 256 subnets, the IP broadcast address for the 10.50 subnet would be 10.50.255.255. Network addresses with all zeros in the host portion, such as 10.50.0.0, can also produce a broadcast response.

In the "smurf" attack, attackers are using ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. There are three parties in these attacks: the attacker, the intermediary, and the victim (note that the intermediary can also be a victim).

The intermediary receives an ICMP echo request packet directed to the IP broadcast address of their network. If the intermediary does not filter ICMP traffic directed to IP broadcast addresses, many of the machines on the network will receive this ICMP echo request packet and send an ICMP echo reply packet back. When (potentially) all the machines on a network respond to this ICMP echo request, the result can be severe network congestion or outages.

When the attackers create these packets, they do not use the IP address of their own machine as the source address. Instead, they create forged packets that contain the spoofed source address of the attacker's intended victim. The result is that when all the machines at the intermediary's site respond to the ICMP echo requests, they send replies to the victim's machine. The victim is subjected to network congestion that could potentially make the network unusable. Even though we have not labeled the intermediary as a "victim," the intermediary can be victimized by suffering the same types of problem that the "victim" does in these attacks.

Attackers have developed automated tools that enable them to send these attacks to multiple intermediaries at the same time, causing all of the intermediaries to direct their responses to the same victim. Attackers have also developed tools to look for network routers that do not filter broadcast traffic and networks where multiple hosts respond.

These networks can the subsequently be used as intermediaries in attacks.

For a more detailed description of the "smurf" attack, please consult this document:

"The Latest in Denial of Service Attacks: 'Smurfing':
Description and Information to Minimize Effects"
Author: Craig Huegen <chuegen@quadrunner.com>
URL: http://www.quadrunner.com/~chuegen/smurf.txt

II. Impact

Both the intermediary and victim of this attack may suffer degraded network performance both on their internal networks or on their connection to the Internet. Performance may be degraded to the point that the network cannot be used.

A significant enough stream of traffic can cause serious performance degradation for small and mid-level ISPs that supply service to the intermediaries or victims. Larger ISPs may see backbone degradation and peering saturation.

III. Solution

A.Solutions for the Intermediary

1. Disable IP-directed broadcasts at your router.

One solution to prevent your site from being used as an intermediary in this attack is to disable IP-directed broadcasts at your router. By disabling these broadcasts, you configure your router to deny IP broadcast traffic onto your network from other networks. In almost all cases, IP-directed broadcast functionality is not needed.

Appendix A contains details on how to disable IP-directed broadcasts for some router vendors. If your vendor is not listed, contact that vendor for instructions.

You should disable IP-directed broadcasts on all of your routers. It is not sufficient to disable IP-directed broadcasts only on the router(s) used for your external network connectivity. For example, if you have five routers connecting ten LANs at your site, you should turn off IP-directed broadcasts on all five routers.

2. Configure your operating system to prevent the machine from responding to ICMP packets sent to IP broadcast

addresses.

If an intruder compromises a machine on your network, the intruder may try to launch a smurf attack from your network using you as an intermediary. In this case, the intruder would use the compromised machine to send the ICMP echo request packet to the IP broadcast address of the local network. Since this traffic does not travel through a router to reach the machines on the local network, disabling IP-directed broadcasts on your routers is not sufficient to prevent this attack.

Some operating systems can be configured to prevent the machine from responding to ICMP packets sent to IP broadcast addresses. Configuring machines so that they do not respond to these packets can prevent your machines from being used as intermediaries in this type of attack.

Appendix A also contains details on how to disable responding to ICMP packets sent to IP broadcast addresses on some operating systems. If your operating system is not listed, contact your vendor for instructions.

B.Solutions for the Victim

Unfortunately, there is no easy solution for victims receiving the potentially large number of ICMP echo reply packets. ICMP echo reply traffic (the traffic from the intermediary) could be blocked at the victim's router; however, that will not necessarily prevent congestion that occurs between the victim's router and the victim's Internet service provider. Victims receiving this traffic may need to consult with their Internet service provider to temporarily block this type of traffic in the ISP's network.

Additionally, victims in this position should contact the intermediaries and inform them of the attack and of the steps described in the previous section. (Please refer them to http://www.cert.org/nav/alerts.html or ftp://ftp.cert.org/pub/cert_advisories/ for the most recent version of this advisory.)

Victims can use the "whois" command to obtain contact information for the sites. More information on using whois is available in

ftp://ftp.cert.org/pub/whois_how_to

C.Solution for the Site Where Attacks Originate

We recommend filtering outgoing packets that contain a source address from a different network.

Attacks like the smurf attack rely on the use of forged packets, that is, packets for

which the attacker deliberately falsifies the origin address. With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, you can use filtering to reduce the likelihood of your site's networks being used to initiate forged packets.

As we mentioned in CERT advisory CA-97.28 on Teardrop and Land denial-of-service attacks, the best current method to reduce the number of IP-spoofed packets exiting your network is to install filtering on your routers that requires packets leaving your network to have a source address from your internal network. This type of filter prevents a source IP-spoofing attack from your site by filtering all outgoing packets that contain a source address from a different network.

A detailed description of this type of filtering is available in RFC 2267, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" by Paul Ferguson of Cisco Systems, Inc. and Daniel Senie of Blazenet, Inc. We recommend it to both Internet Service Providers and sites that manage their own routers. The document is currently available at

ftp://ftp.isi.edu/in-notes/rfc2267.txt

Appendix A - Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact the vendor directly.

Cray Research - A Silicon Graphics Company

Current versions of Unicos and Unicos/mk do not have the ability to reject ICMP requests send to broadcast addresses. We are tracking this problem through SPR 709733.

Cisco Systems

Cisco recommends the following configuration settings as protection against being used as an intermediary in smurf attacks:

1. Disabling IP directed broadcast for all interfaces on which it is not needed. This must be done on all routers in the network, not just on the border routers. The command "no ip directed-broadcast" should be applied to each interface on which directed broadcasts are to be disabled.

   Very few IP applications actually need to use directed broadcasts, and it's extremely rare for such an application to be in use in a network without the knowledge of the network administrator. Nonetheless, as when any functionality

is disabled, you should be alert for possible problems.

This is the preferred solution for most networks.

2. If your network configuration is simple enough for you to create and maintain a list of all the directed broadcast addresses in your network, and if you have a well-defined perimeter separating your own network from potentially hostile networks, consider using a filter at the perimeter to prevent directed broadcasts from entering the network. For example, if your network number is 172.16.0.0, and you uniformly use a subnet mask of 255.255.255.0, then you might use Cisco access list entries like

```
    access-list 101 deny ip 0.0.0.0 255.255.255.255 172.16.0.255
0.0.255.0
    access-list 101 deny ip 0.0.0.0 255.255.255.255 172.16.0.0
0.0.255.0
```

Note that this is not a complete access list; it's simply two entries. See the Cisco documentation for more information on configuring access lists. The best place to apply such a filter is usually on the incoming side of each router interface that connects to the potentially hostile network.

This solution may be administratively infeasible for networks using variable-length subnet masks, or which have complex external connectivity. There is also some possibility that legitimate directed broadcasts may be being sent into your network from the outside, especially if you're working in a research environment.

In addition to these protections against being used as an intermediary in a smurf attack, Cisco recommends that you take steps to prevent users within your own network from launching such attacks. For "stub" networks which do not provide transit connectivity (most corporate and institutional networks, many smaller ISPs), this is usually best done by installing filters at the network perimeter to prevent any packets from leaving your network unless their IP source addresses actually lie within your network's address space. For the example network above, you might place the following entry in the incoming access lists on the interface(s) facing your internal network:

```
access-list 101 permit ip 172.16.0.0 0.0.255.255 0.0.0.0 255.255.255.255
access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Data General Corporation

DG/UX has an option to enable/disable the forwarding of IP broadcast packets. It is disabled by default. This means that if DG/UX is used along the path, it will not forward the attack packets.

DG/UX B2 with Security Option has a 'netctrl' facility which enables the administrator to disable the response to a broadcast ICMP ping message.

DIGITAL EQUIPMENT CORPORATION

Currently DIGITAL products do not deny individual ICMP service to a host. That, outside the intranet, firewalls should protect from this kind of spoof/attack.

If the problem has to be dealt with inside the firewall and the intranet, then policy should address "malicious acts"and the individuals responsible.

FreeBSD, Inc.

In FreeBSD 2.2.5 and up, the tcp/ip stack does not respond to icmp echo requests destined to broadcast and multicast addresses by default. This behaviour can be changed via the sysctl command via mib net.inet.icmp.bmcastecho.

IBM Corporation

AIX 4

There is a network attribute called "bcastping" that controls whether or not responses to ICMP echo packets to the broadcast address are allowed. A value of zero turns off responses and a value of one turns them on. The default is zero (i.e., by default AIX version 4 is not vulnerable to the described denial-of-service attack).

Use the following command to check the value of the bcastping attribute:

```
$ no -o bcastping
```

Use the following command to turn off responses to ICMP broadcast packets (as root):

```
# no -o bcastping=0
```

AIX 3

The "bcastping" attribute does not exist in version 3.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Livingston Enterprises, Inc.

Livingston Enterprises products don't respond to ICMP packets not sent to their own address, but do forward them. They're currently examining the problem to see what kind of solution they can provide.

The NetBSD Project

Under NetBSD you can disable forwarding of directed broadcast packets with this command, as root:

```
# sysctl -w net.inet.ip.directed-broadcast=0
```

NetBSD will always respond to broadcast ICMP packets. In the future, NetBSD may

allow this to be disabled.

Sun Microsystems

To prevent incoming broadcast packets from entering your network (III. A. 1. in this advisory)

Solaris 2.6, 2.5.1, 2.5, 2.4, and 2.3:

```
Use the command:  ndd -set /dev/ip ip_forward_directed_broadcasts 0
```

SunOS 4.1.3_U1 and 4.1.4:

Do the following:

```
Add ''options DIRECTED_BROADCAST=0'' to system configuration
file and rebuild kernel
```

To prevent systems from responding to broadcast ICMP packets (III. A. 2. in this advisory)

Solaris 2.6, 2.5.1, 2.5, 2.4, and 2.3:

```
Use the command: ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

A corresponding variable for ip_respond_to_echo_broadcast does not exist in SunOS 4.1.x.

The CERT Coordination Center thanks Craig A. Huegen. Much of the content in this advisory has been derived from his document on "smurf" attacks. The CERT Coordination Center also thanks Paul Ferguson and Daniel Senie for providing information on network ingress filtering, and John Bashinski of Cisco for his contributions.

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/)

CERT/CC Contact Information

Email cert@cert.org

Phone +1 412-268-7090 (24-hour hotline)

CERT personnel answer 8:30-5:00 p.m. EST(GMT-5) / EDT(GMT-4) and are on call for emergencies during other hours.

Fax +1 412-268-6989

Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
USA

Using encryption

We strongly urge you to encrypt sensitive information sent by email. We can support a shared DES key or PGP. Contact the CERT/CC for more information.

Location of CERT PGP key

ftp://ftp.cert.org/pub/CERT_PGP.key

Getting security information

CERT publications and other security information are available from

http://www.cert.org/
ftp://ftp.cert.org/pub/

CERT advisories and bulletins are also posted on the USENET newsgroup comp.security.announce
To be added to our mailing list for advisories and bulletins, send email to

cert-advisory-request@cert.org

In the subject line, type

SUBSCRIBE your-email-address

Revision history

```
Aug. 24, 1998 Updated vendor information for Data General Corporation.

Aug. 14, 1998 Updated vendor information for Sun Microsystems.

Apr. 28, 1998 Updated vendor information for Cisco Systems and
              Sun Microsystems.
              Corrected URL for obtaining RFCs
```

Apr. 10, 1998 Updated vendor information for Cisco Systems

Feb. 10, 1998 Updates to Appendix A - Vendor Information

Jan. 29, 1998 Updated reference to the filtering document (now an RFC) in Section III-C.

Jan. 13, 1998 Updated vendor information for NetBSD.

Jan. 7, 1998 Updated or added vendor information for Digital Equipment Corporation
and Livingston Enterprises, Inc.

CERT* Advisory CA-96.21

Original issue date: September 19, 1996
Last Revised: August 24, 1998 Updated vendor information for Silicon Graphics, Inc.

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

Topic: TCP SYN Flooding and IP Spoofing Attacks

This advisory supersedes the IP spoofing portion of CA-95.01.

Two "underground magazines" have recently published code to conduct denial-of-service attacks by creating TCP "half-open" connections. This code is actively being used to attack sites connected to the Internet. There is, as yet, no complete solution for this problem, but there are steps that can be taken to lessen its impact. Although discovering the origin of the attack is difficult, it is possible to do; we have received reports of attack origins being identified.

Any system connected to the Internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is potentially subject to this attack. Note that in addition to attacks launched at specific hosts, these attacks could also be launched against your routers or other network server systems if these hosts enable (or turn on) other TCP services (e.g., echo). The consequences of the attack may vary depending on the system; however, the attack itself is fundamental to the TCP protocol used by all systems.

If you are an Internet service provider, please pay particular attention to Section III and Appendix A, which describes step we urge you to take to lessen the effects of these attacks. If you are the customer of an Internet service provider, please encourage your provider to take these steps.

This advisory provides a brief outline of the problem and a partial solution. We will update this advisory as we receive new information. If the change in information warrants, we may post an updated advisory on comp.security.announce and redistribute an update to our cert-advisory mailing list. As always, the latest information is available at the URLs listed at the end of this advisory.

I. Description

When a system (called the client) attempts to establish a TCP connection to a system providing a service (the server), the client and server exchange a set sequence of messages. This connection technique applies to all TCP connections--telnet, Web, email, etc.

The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message. The connection between the client and the server is then open, and the service-specific data can be exchanged between the client and the server. Here is a view of this message flow:

```
Client                  Server
------                  ------
SYN--------------------->
<----------------------SYN-ACK
ACK--------------------->

Client and server can now
send service-specific data
```

The potential for abuse arises at the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message. This is what we mean by half-open connection. The server has built in its system memory a data structure describing all pending connections. This data structure is of finite size, and it can be made to overflow by intentionally creating too many partially-open connections.

Creating half-open connections is easily accomplished with IP spoofing. The attacking system sends SYN messages to the victim server system; these appear to be legitimate but in fact reference a client system that is unable to respond to the SYN-ACK messages. This means that the final ACK message will never be sent to the victim server system.

The half-open connections data structure on the victim server system will eventually fill; then the system will be unable to accept any new incoming connections until the table is emptied out. Normally there is a timeout associated with a pending connection, so the half-open connections will eventually expire and the victim server system will recover. However, the attacking system can simply continue sending IP-spoofed packets requesting new connections faster than the victim system can expire the pending connections.

In most cases, the victim of such an attack will have difficulty in accepting any new incoming network connection. In these cases, the attack does not affect existing incoming connections nor the ability to originate outgoing network connections.

However, in some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

The location of the attacking system is obscured because the source addresses in the SYN packets are often implausible. When the packet arrives at the victim server system, there is no way to determine its true source. Since the network forwards packets based on destination address, the only way to validate the source of a packet is to use input source filtering (see Appendix A).

II. Impact

Systems providing TCP-based services to the Internet community may be unable to provide those services while under attack and for some time after the attack ceases. The service itself is not harmed by the attack; usually only the ability to provide the service is impaired. In some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

III. Solution

There is, as yet, no generally accepted solution to this problem with the current IP protocol technology. However, proper router configuration can reduce the likelihood that your site will be the source of one of these attacks.

Appendix A contains details about how to filter packets to reduce the number of IP-spoofed packets entering and exiting your network. It also contains a list of vendors that have reported support for this type of filtering.

NOTE to Internet Service Providers:

We STRONGLY urge you to install these filters in your routers to protect your customers against this type of an attack. Although these filters do not directly protect your customers from attack, the filters do prevent attacks from originating at the sites of any of your customers. We are aware of the ramifications of these filters on some current Mobile IP schemes and are seeking a position statement from the appropriate organizations.

NOTE to customers of Internet service providers:

We STRONGLY recommend that you contact your service provider to verify that the necessary filters are in place to protect your network.

Many networking experts are working together to devise improvements to existing IP implementations to "harden" kernels to this type of attack. When these improvements become available, we suggest that you install them on all your systems as soon as possible. This advisory will be updated to reflect changes made by the vendor

IV. Detecting an Attack

Users of the attacked server system may notice nothing unusual since the IP-spoofed connection requests may not load the system noticeably. The system is still able to establish outgoing connections. The problem will most likely be noticed by client

systems attempting to access one of the services on the victim system.

To verify that this attack is occurring, check the state of the server system's network traffic. For example, on SunOS this may be done by the command:

```
netstat -a -f inet
```

Note that use of the above command depends on the OS version, for example for a FreeBSD system use

```
netstat -s |grep "listenqueue overflows"
```

Too many connections in the state "SYN_RECEIVED" could indicate that the system is being attacked.

Appendix A - Reducing IP Spoofed Packets

1. Filtering Information

With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, you can take steps to reduce the number of IP-spoofed packets entering and exiting your network.

Currently, the best method is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network to prevent a source IP spoofing attack from originating from your site.

The combination of these two filters would prevent outside attackers from sending you packets pretending to be from your internal network. It would also prevent packets originating within your network from pretending to be from outside your network. These filters will *not* stop all TCP SYN attacks, since outside attackers can spoof packets from *any* outside network, and internal attackers can still send attacks spoofing internal addresses.

We STRONGLY urge Internet service providers to install these filters in your routers.

In addition, we STRONGLY recommend customers of Internet service providers to contact your service provider to verify that the necessary filters are in place to protect your network.

2. Vendor Information

The following vendor(s) have reported support for the type of filtering we recommend and provided pointers to additional information that describes how to configure your router. If we hear from other vendors, we will add their information to the "Updates" section at the end of this advisory.

If you need more information about your router or about firewalls, please contact your vendor directly.

Cisco

Refer to the section entitled "ISP Security Advisory" on http://www.cisco.com for an up-to-date explanation of how to address TCP SYN flooding on a Cisco router.

NOTE to vendors:

If you are a router vendor who has information on router capabilities and configuration examples and you are not represented in this list, please contact the CERT Coordination Center at the addresses given in the Contact Information section below. We will update the advisory after we hear from you.

3. Alternative for routers that do not support filtering on the inbound side

If your vendor's router does not support filtering on the inbound side of the interface or if there will be a delay in incorporating the feature into your system, you may filter the spoofed IP packets by using a second router between your external interface and your outside connection. Configure this router to block, on the outgoing interface connected to your original router, all packets that have a source address in your internal network. For this purpose, you can use a filtering router or a UNIX system with two interfaces that supports packet filtering.

Note: Disabling source routing at the router does not protect you from this attack, but it is still good security practice to follow.

On the input to your external interface, that is coming from the Internet to your network, you should block packets with the following addresses:

- Broadcast Networks: The addresses to block here are network 0 (the all zeros broadcast address) and network 255.255.255.255 (the all ones broadcast network).
- Your local network(s): These are your network addresses
- Reserved private network numbers: The following networks are defined as reserved private networks, and no traffic should ever be received from or transmitted to these networks through a router:

```
10.0.0.0     - 10.255.255.255    10/8           (reserved)
127.0.0.0    - 127.255.255.255   127/8          (loopback)
172.16.0.0   - 172.31.255.255    172.16/12      (reserved)
192.168.0.0 - 192.168.255.255   192.168/16     (reserved)
```

The CERT Coordination Center staff thanks the team members of NASIRC for

contributing much of the text for this advisory and thanks the many experts who are devoting time to addressing the problem and who provided input to this advisory.

UPDATES

3COM

Please refer to the "Network Security Advisory" for a thorough discussion of how to address TCP SYN flooding attacks on a 3Com router:

http://www.3com.com/

Berkeley Software Design, Inc.

BSDI has patches available.

PATCH

K210-021 (ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/K210-021)

md5 checksum: c386e72f41d0e409d91b493631e364dd K210-021

This patch adds two networking features that can help defeat and detect some types of denial of service attacks.

This patch requires U210-025 which provides new copies of *sysctl(8)* and *netstat(1)* for configuration and monitoring of these new features.

PATCH

K210-022 (ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/K210-22)

md5 checksum: 9ec62b5e9cc424b9b42089504256d926 K210-022

This patch adds a TCP SYN cache which reduces and/or eliminates the effects of SYN-type denial of service attacks such as those discussed in CERT advisory CA 96.21.

PATCH

U210-025 (ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-025)

md5 checksum: d2ee01238ab6040e9b7a1bd2c3bf1016 U210-025

This patch should be installed in conjunction with IP source address check and IP fragmentation queue limit patch (K210-021) and SYN flooding patch (K210-022).

Additional details about these patches are available from

http://www.bsdi.com
ftp://ftp.bsdi.com

Hewlett-Packard Company

HPSBUX9704-060

Description: SYN Flooding Security Vulnerability in HP-UX

HEWLETT-PACKARD SECURITY BULLETIN: #00060

Security Bulletins are available from the HP Electronic Support Center via electronic mail.

User your browser to get to the HP Electronic Support Center page at:

http://us-support.external.hp.com
(for US, Canada, Asia-Pacific, & Latin-America)

http://europe-support.external.hp.com
(for Europe)

IBM Corporation

Any system that is connected to a TCP/IP-based network (Internet or intranet) and offers TCP-based services is vulnerable to the SYN flood attack. The attack does not distinguish between operating systems, software version levels, or hardware platforms; all systems are vulnerable. IBM has released AIX operating system fixes for the SYN flood vulnerability.

NOTE: If you are using the IBM Internet Connection Secured Network Gateway (SNG) firewall software, you must also apply the fixes listed in the next section.

The following Automated Program Analysis Reports (APARs) for IBM AIX are now available to address the SYN flood attack:

AIX 3.2.5

No APAR available; upgrade to AIX 4.x recommended

AIX 4.1.x

APAR - IX62476

AIX 4.2.x

APAR - IX62428

Fixes for IBM SNG Firewall

The following Automated Program Analysis Reports (APARs) for the IBM Internet Connection Secured Network Gateway firewall product are now available to address the SYN flood and "Ping o' Death" attacks:

NOTE: The fixes in this section should ONLY be applied to systems running the IBM Internet Connection Secured Network Gateway (SNG) firewall software. They should be applied IN ADDITION TO the IBM AIX fixes listed in the previous section.

IBM SNG V2.1

APAR - IR33376 PTF UR46673

IBM SNG V2.2

APAR - IR33484 PTF UR46641

Obtaining Fixes

IBM AIX APARs may be ordered using Electronic Fix Distribution (via the FixDist program), or from the IBM Support Center. For more information on FixDist, and to obtain fixes via the Internet, please reference

http://service.software.ibm.com/aixsupport/

or send electronic mail to "aixserv@austin.ibm.com " with the word "FixDist" in the "Subject:" line.

Linux

A patch for the linux kernel source is available from:

http://www.dna.lth.se/~erics/software/tcp-syncookies-patch-1.gz

The patch allows tcp/ip processing to continue as normal, until the queue gets close to full. Then, instead of just sending the synack back, it sends a syn cookie back, and waits for a response to IT before sending the synack. When it sends the cookie, it clears the syn from the queue, so while under attack, the queue will never fill up. Cookies expire shortly after they are sent. Basically this prevents people from filling up the queue completely. No one flooding from a spoof will be able to reply to the cookie, so nothing can be overloaded. And if they aren't flooding from a spoof, they would be getting a cookie they would have to respond to, and would have a hard time responding to all the cookies and continuing the flood.

Livingston Enterprises, Inc.

Refer to the following Applications Note for more information on configuring a Livingston IRX or PortMaster to help block outgoing SYN attacks from an ISP's users:

ftp://ftp.livingston.com/pub/le/doc/notes/filters.syn-attack

Silicon Graphics, Inc.

Updated Silicon Graphics information concerning SYN attacks can be found in SGI Security Advisory, "IRIX IP Spoofing/TCP Sequence Attack Update," 19961202-01-PX, issued on August 6, 1998.

Patches are available via anonymous FTP and your service/support provider.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at:

http://www.sgi.com/Support/security

Sun Microsystems, Inc.

Sun published a bulletin on October 9, 1996--Sun security bulletin number 00136. Sun Security Bulletins are available via the security-alert@sun.com alias and on SunSolve.

Note: Advisories from vendors listed in this section can also be found at ftp://ftp.cert.org/pub/vendors/

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in the Forum of Incident Response and Security Teams (see http://www.first.org/team-info/)

CERT/CC Contact Information

Email cert@cert.org

Phone +1 412-268-7090 (24-hour hotline)

CERT personnel answer 8:30-5:00 p.m. EST(GMT-5) / EDT(GMT-4) and are on call for emergencies during other hours.

Fax +1 412-268-6989

Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
USA

Using encryption

We strongly urge you to encrypt sensitive information sent by email. We can support a shared DES key or PGP. Contact the CERT/CC for more information.

Location of CERT PGP key

ftp://ftp.cert.org/pub/CERT_PGP.key

Getting security information

CERT publications and other security information are available from

http://www.cert.org/
ftp://ftp.cert.org/pub/

CERT advisories and bulletins are also posted on the USENET newsgroup comp.security.announce
To be added to our mailing list for advisories and bulletins, send email to

cert-advisory-request@cert.org

In the subject line, type

SUBSCRIBE your-email-address

Revision history

```
Aug. 24, 1998  Updated vendor information for Silicon Graphics, Inc.
Sep, 24, 1997  Updated copyright statement
July 18, 1997  Updates - added information
May  08, 1997  Updates - updated vendor information for Hewlett-Packard.
Jan. 02, 1997  Updates - added or modified vendor information for SGI,
               Livingston, HP, 3COM.
Dec. 19, 1996  Updates - corrected Sun Microsystems security-alert email
               address.
Dec. 10, 1996  Appendix A, #3 - corrected next to last reserved private
               network number entry.
Dec. 09, 1996  Updates - added IBM patch information.
Nov. 12, 1996  Introduction, paragraph 2 - added some clarification.
Oct. 10, 1996  Updates - added a pointer to Sun Microsystems advisory.
               added a pointer to the CERT /pub/vendors directory.
Oct. 08, 1996  Appendix A, #3 - revised the last item, reserved private
               network numbers
               Updates - added BSDI patch information.
Oct. 07, 1996  Updates - added a pointer to Silicon Graphics advisory.
Sep. 24, 1996  Modified the supersession statement.
```

CERT® Coordination Center

Denial of Service

1. Description

   This document provides a general overview of attacks in which the primary goal of the attack is to deny the victim(s) access to a particular resource. Included is information that may help you respond to such an attack.

   A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include

   - attempts to "flood" a network, thereby preventing legitimate network traffic
   - attempts to disrupt connections between two machines, thereby preventing access to a service
   - attempts to prevent a particular individual from accessing a service
   - attempts to disrupt service to a specific system or person

   Not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack.

   Illegitimate use of resources may also result in denial of service. For example, an intruder may use your anonymous ftp area as a place to store illegal copies of commercial software, consuming disk space and generating network traffic

2. Impact

   Denial-of-service attacks can essentially disable your computer or your network. Depending on the nature of your enterprise, this can effectively disable your organization.

   Some denial-of-service attacks can be executed with limited resources against a large, sophisticated site. This type of attack is sometimes called an "asymmetric attack." For example, an attacker with an old PC and a slow modem may be able to disable much faster and more sophisticated machines or networks.

3. MODES OF ATTACK

   Denial-of-service attacks come in a variety of forms and aim at a variety of services. There are three basic types of attack:

- consumption of scarce, limited, or non-renewable resources
- destruction or alteration of configuration information
- physical destruction or alteration of network components

A. Consumption of Scarce Resources

Computers and networks need certain things to operate: network bandwidth, memory and disk space, CPU time, data structures, access to other computers and networks, and certain environmental resources such as power, cool air, or even water.

1. Network Connectivity

Denial-of-service attacks are most frequently executed against network connectivity. The goal is to prevent hosts or networks from communicating on the network. An example of this type of attack is the "SYN flood" attack described in

ftp://info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding

In this type of attack, the attacker begins the process of establishing a connection to the victim machine, but does it in such a way as to prevent the ultimate completion of the connection. In the meantime, the victim machine has reserved one of a limited number of data structures required to complete the impending connection. The result is that legitimate connections are denied while the victim machine is waiting to complete bogus "half-open" connections.

You should note that this type of attack does not depend on the attacker being able to consume your network bandwidth. In this case, the intruder is consuming kernel data structures involved in establishing a network connection. The implication is that an intruder can execute this attack from a dial-up connection against a machine on a very fast network. (This is a good example of an asymmetric attack.)

2. Using Your Own Resources Against You

An intruder can also use your own resources against you in unexpected ways. One example is described in

ftp://info.cert.org/pub/cert_advisories/CA-96.01.UDP_service_denial

In this attack, the intruder uses forged UDP packets to connect the echo service on one machine to the chargen service on another machine. The result is that the two services consume all available network bandwidth between them. Thus, the network connectivity for all machines on the same networks as either of the targeted machines may be affected.

3. Bandwidth Consumption

   An intruder may also be able to consume all the available bandwidth on your network by generating a large number of packets directed to your network. Typically, these packets are ICMP ECHO packets, but in principle they may be anything. Further, the intruder need not be operating from a single machine; he may be able to coordinate or co-opt several machines on different networks to achieve the same effect.

4. Consumption of Other Resources

   In addition to network bandwidth, intruders may be able to consume other resources that your systems need in order to operate. For example, in many systems, a limited number of data structures are available to hold process information (process identifiers, process table entries, process slots, etc.). An intruder may be able to consume these data structures by writing a simple program or script that does nothing but repeatedly create copies of itself. Many modern operating systems have quota facilities to protect against this problem, but not all do. Further, even if the process table is not filled, the CPU may be consumed by a large number of processes and the associated time spent switching between processes. Consult your operating system vendor or operating system manuals for details on available quota facilities for your system.

   An intruder may also attempt to consume disk space in other ways, including

   - generating excessive numbers of mail messages. For more information, please see

     ftp://info.cert.org/pub/tech_tips/email_bombing_spamming

   - intentionally generating errors that must be logged
   - placing files in anonymous ftp areas or network shares, For information on proper configuration for anonymous ftp,

please see

ftp://info.cert.org/pub/tech_
tips/anonymous_ftp_config

In general, anything that allows data to be written to disk can be used to execute a denial-of-service attack if there are no bounds on the amount of data that can be written.

Also, many sites have schemes in place to "lockout" an account after a certain number of failed login attempts. A typical set up locks out an account after 3 or 5 failed login attempts. An intruder may be able to use this scheme to prevent legitimate users from logging in. In some cases, even the privileged accounts, such as root or administrator, may be subject to this type of attack. Be sure you have a method to gain access to the systems under emergency circumstances. Consult your operating system vendor or your operating systems manual for details on lockout facilities and emergency entry procedures.

An intruder may be able to cause your systems to crash or become unstable by sending unexpected data over the network. An example of such an attack is described in

ftp://info.cert.org/pub/cert_advisories/CA
-96.26.ping

If your systems are experiencing frequent crashes with no apparent cause, it could be the result of this type of attack.

There are other things that may be vulnerable to denial of service that you may wish to monitor. These include

- printers
- tape devices
- network connections
- other limited resources important to the operation of your organization

B. Destruction or Alteration of Configuration Information

An improperly configured computer may not perform well or may not operate at all. An intruder may be able to alter or destroy configuration information that prevents you from using your computer or network.

For example, if an intruder can change the routing information in your routers, your network may be disabled. If an intruder is able to modify the registry on a Windows NT machine, certain functions may be unavailable.

For information on configuring UNIX machines, see

ftp://info.cert.org/pub/tech_tips/UNIX_configuration_guidelines

For information on configuring Microsoft Windows NT machines, please see

http://www.microsoft.com/security/

C. Physical Destruction or Alteration of Network Components

The primary concern with this type of attack is physical security. You should guard against unauthorized access to computers, routers, network wiring closets, network backbone segments, power and cooling stations, and any other critical components of your network.

Physical security is a prime component in guarding against many types of attacks in addition to denial of service. For information on securing the physical components of your network, we encourage you to consult local or national law enforcement agencies or private security companies.

4. Prevention and Response

Denial-of-service attacks can result in significant loss of time and money for many organizations. We strongly encourage sites to consider the extent to which their organization could afford a significant service outage and to take steps commensurate with the risk.

We encourage you to consider the following options with respect to your needs:

- Implement router filters as described in Appendix A of CA-96.21.tcp_syn_flooding, referenced above. This will lessen your exposure to certain denial-of-service attacks. Additionally, it will aid in preventing users on your network from effectively launching certain denial-of-service attacks.
- If they are available for your system, install patches to guard against TCP SYN flooding as described in CA-96.21.tcp_syn_flooding, referenced above. This will substantially reduce your exposure to these attacks but may not eliminate the risk entirely.
- Disable any unused or unneeded network services. This can limit the ability of an intruder to take advantage of those services to execute a

denial-of-service attack.

- Enable quota systems on your operating system if they are available. For example, if your operating system supports disk quotas, enable them for all accounts, especially accounts that operate network services. In addition, if your operating system supports partitions or volumes (i.e., separately mounted file systems with independent attributes) consider partitioning your file system so as to separate critical functions from other activity.
- Observe your system performance and establish baselines for ordinary activity. Use the baseline to gauge unusual levels of disk activity, CPU usage, or network traffic.
- Routinely examine your physical security with respect to your current needs. Consider servers, routers, unattended terminals, network access points, wiring closets, environmental systems such as air and power, and other components of your system.
- Use Tripwire or a similar tool to detect changes in configuration information or other files. For more information, see

  ftp://info.cert.org/pub/tech_tips/security_tools
- Invest in and maintain "hot spares" - machines that can be placed into service quickly in the event that a similar machine is disabled.
- Invest in redundant and fault-tolerant network configurations.
- Establish and maintain regular backup schedules and policies, particularly for important configuration information.
- Establish and maintain appropriate password policies, especially access to highly privileged accounts such as UNIX root or Microsoft Windows NT Administrator.

Many organizations can suffer financial loss as a result of a denial-of-service attack and may wish to pursue criminal or civil charges against the intruder. For legal advice, we recommend that you consult with your legal counsel and law enforcement.

U.S. sites interested in an investigation of a denial-of-service attack can contact their local FBI field office for guidance and information. For contact information for your local FBI field office, please consult your local telephone directory or see the FBI's field offices web page:

http://www.fbi.gov/fo/fo.htm

For more information, please see the web page of the FBI National Computer Crime Squad (NCCS):

http://www.fbi.gov/programs/nccs/compcrim.htm

Non-U.S. sites may want to discuss the activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

If you are interested in determining the source of certain types of denial-of-service attack, it may require the cooperation of your network service provider and the administration of the networks involved. Tracking an intruder this way may not always be possible. If you are interested in trying do to so, contact your service provider directly. The CERT(*) Coordination Center is not able to provide this type of assistance. We do encourage you to report your experiences, however. This helps us understand the nature and scope of security incidents on the Internet, and we may be able to relate your report to other activity that has been reported to us.

This document is available from: http://www.cert.org/tech_tips/denial_of_service.html

---

CERT/CC Contact Information

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

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

CERT personnel answer the hotline 08:00-20:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

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

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

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

Getting security information

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

http://www.cert.org/

To be added to our mailing list for advisories and bulletins, send email to cert-advisory-request@cert.org and include `SUBSCRIBE your-email-address` in the subject of your message.

Revision History

Oct 02, 1997	Initial Release
Feb 12, 1999	Converted to new web format

Results of the
Distributed-Systems Intruder Tools Workshop

Pittsburgh, Pennsylvania USA

November 2-4, 1999

Published at the
CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

December 7, 1999

Contributors

The ideas in this paper were jointly developed by participants in the Distributed-Systems Intruder Tools Workshop. Their intellectual contributions and their spirit of cooperation made the workshop a success. Among the many participants who contributed to this paper are the following:

Jon David
AT&T Information Security Center

Cory Cohen, Kathy Fithen,
Kevin Houle, Tom Longstaff,
John McHugh, Eric Mitchell,
Rich Pethia, Jed Pickel,
Tim Shimeall, Dara Sewell (resident affiliate)
CERT® Coordination Center

Bradley Frank
Ken Rowe
Cisco Systems, Inc.

Brian Dunphy
Sean McAllis**ter**
DoD CERT

Sammy Migues
Infrastructure Defense

Pat Becker
Internet Security Systems, Inc.

Sven Dietrich
Aghadi Shraim
NASA Goddard Space Flight Center

John Green
NSWC (Naval Surface Warfare Center) SHADOW Team

Richard Forno
Network Solutions, Inc.

Kenneth R. van Wyk
Para-Protect®, Inc.

Kathleen Kimball
George Weaver
Penn State University

Clarissa Cook
Robert Stone
UUNET

Richard A. Kemmerer
University of California, Santa Barbara

David Dittrich
University of Washington

N.L.

Results of the Distributed-Systems Intruder Tools Workshop

Pittsburgh, Pennsylvania USA November 2-4, 1999

Executive Summary

On November 2-4, 1999, the CERT® Coordination Center invited 30 experts from around the world to address a category of network attack tools that use distributed systems. Several tools are in use now, and the technology is maturing. As a result, a single, simple command from an attacker could result in tens of thousands of concurrent attacks on one or a set of targets. The attacker can use unprotected Internet nodes around the world to coordinate the attacks. Each attacking node has limited information on who is initiating the attack and from where; and no node need have a list of all attacking systems. Damaged systems include those used in the attack as well as the targeted victim. For the victim, the impact can be extensive. For example, in a denial-of-service attack using distributed technology, the attacked system observes simultaneous attacks from all the nodes at once – flooding the network normally used to communicate and trace the attacks and preventing any legitimate traffic from traversing the network.

Distributed intruder technology is not entirely new; however, it is maturing to the point that even unsophisticated intruders could do serious damage. The Distributed-Systems Intruder Tools (DSIT) Workshop provided a venue for experts around the world to share experiences, gain a common understanding, and creatively brainstorm possible responses and solutions *before* the dissemination of the maturing attack tools – and attacks themselves – become widespread.

One consideration is the approach typically taken by the intruder community. There is (loosely) organized development in the intruder community, with only a few months elapsing between "beta" software and active use in attacks. Moreover, intruders take an open-source approach to development. One can draw parallels with open system development: there are many developers and a large, reusable code base. Intruder tools become increasingly sophisticated and also become increasingly user friendly and widely available. As a result, even unsophisticated intruders can use them.

There has already been some public discussion in the intruder community about distributed attack tools while development continues. In their development, intruders are using currently available technology to develop new technology. For example, they are building on previous scanning technology and automated intrusion tools to create more

powerful intrusion tools. One concern of workshop participants is that in a relatively short time, it may be possible for unsophisticated intruders to gain control of and use systems distributed across significant portions of the Internet for their attacks.

This paper is one outcome of the DSIT Workshop. In it, workshop participants examine the use of distributed-system intruder tools and note that current experiences have highlighted the need for better forensic techniques and training, the importance of close cooperation, and a concern for the rapid evolution of intruder tools. They provide information about protecting systems from attack by the tools, detecting the use of the tools, and responding to attacks. The paper includes suggestions for specific groups in the Internet community:

- managers
- system administrators
- Internet service providers (ISPs)
- incident response teams (IRTs)

The suggestions address actions each group should take immediately, along with actions for the short term and long term. They also remind readers that the security of any network on the Internet depends on the security of every other network. The widely varying implementation of security measures is what often makes a distributed attack successful.

The workshop participants hope that the information offered here will help reduce the impact of distributed attack tools on the Internet as those tools mature.

Results of the Distributed-Systems Intruder Tools Workshop

1. Introduction

On November 2-4, 1999, the CERT® Coordination Center (CERT/CC) invited 30 experts from around the world to address a category of network attack tools that use distributed systems in increasingly sophisticated ways. Intruders are maturing an attack technology that goes beyond using individual systems as the starting point for an attack. Rather, they can potentially use tens of thousands of unprotected Internet nodes together in order to coordinate an attack against selected targets. Each attacking node has limited information on who is initiating the attack and from where; and no node need have a list of all attacking systems. For the victim, the impact can be extensive. For example, in a denial-of-service attack using distributed technology, the attacked system observes simultaneous attacks from all the nodes at once – flooding the network normally used to communicate and trace the attacks and preventing any legitimate traffic from traversing the network.

Distributed intruder technology is not entirely new; however, it is maturing to the point that even unsophisticated intruders could do serious damage. In the past, intruders have used IRC robots to control remotely networks of compromised machines. In addition, fapi, a denial-of-service (DoS) tool that appeared early in 1998, works in a similar way to some of the tools we are now seeing, but it was not as sophisticated or as widely used.

During the Distributed-Systems Intruder Tools (DSIT) Workshop, participants discussed a large number of approaches to preventing, detecting, and responding to distributed-systems attacks. The CERT/CC specifically invited technical personnel that could contribute technically to the solutions regardless of their position in their home organization or political stature in the community. Thus, the workshop effectively provided a venue for experts around the world to share experiences, gain a common understanding, and creatively brainstorm possible responses and solutions to this category of attack *before* the dissemination of the attack tools – and the attacks themselves – become widespread.

One consideration is the approach typically taken by the intruder community. There is (loosely) organized development in the intruder community, with only a few months elapsing between "beta" software and active use in attacks. Intruders are actively developing distributed tools to use the many resources on the network; this has become easier because of the large number of machines "available for public use" – that is, vulnerable to compromise and, thus, available for use by anyone who can exploit the vulnerabilities. Moreover, intruders typically take an open-source approach to development. One can draw parallels with open system development: there are many developers and a large, reusable code base. Intruder tools become increasingly sophisticated and also become increasingly user friendly and widely available. As a result, even unsophisticated intruders can use the available tools to identify and take advantage of a large number of vulnerable machines.

There has already been some public discussion in the intruder community about the distributed attack tools while development continues. Intruders are using currently available technology to develop new technology. For example, they are building on previous scanning technology and automated intrusion tools to create more powerful intrusion tools. One concern of workshop participants is that in a relatively short time, it may be possible for unsophisticated intruders to gain control of and use systems distributed across significant portions of the Internet for their attacks.

As noted in the letter of invitation to the participants,

> *So far, we have seen only limited use of these new tools, but we believe it won't be long before the tools will move from the development by sophisticated intruders into wide use by the large population of less sophisticated intruders. When this happens, all of us will face new issues with impact on security, incident response, and future technology. ...*
>
> *I believe that security experts need to act now, before the tools are in widespread use. During the workshop, we hope to analyze these new attack tools; explore their possible evolution and kinds of impact we might see from their use; and outline techniques that can be used to detect, respond to, and recover from attacks.*

One strong response to the workshop from the participants is that prior to the workshop, there was no way for the technical staff at important critical infrastructure sites to communicate the threat to management. The participants could understand the problem from an isolated perspective, but it was not until the workshop brought them together that the true nature of the threat was understood and could then be communicated to the management at their home organizations. In many cases, the resulting briefs given to the home organization (including government agencies, critical commercial providers, and university researchers) provided the first and best view of the nature of the changing threat in using networked systems. Finally, this paper, which summarizes output from the workshop, enables the Internet community to gain similar understanding and to take action.

In the next section, workshop participants examine the use of distributed-system intruder tools. Later sections provide information for specific groups in the Internet community:

- managers
- system administrators
- Internet service providers (ISPs)
- incident response teams (IRTs)

The workshop participants hope that the information offered here will help reduce the impact of the attack tools on the Internet as those tools mature.

2. Recent Activity Involving Distributed Attack Systems

Distributed systems based on the client/server model have become increasingly common. In recent months, we have seen an increase in the development and use of distributed sniffers, scanners, and denial-of-service tools. Attacks using these tools can involve a large number of sites simultaneously and be focused to attack one or more victim hosts or networks.

During the second half of 1999, several sites reported denial-of-service attacks involving distributed intruder tools. While some of the details presented here are specific to the incidents that were observed, the overall distributed strategy can be applied to attacks other than denial of service. The description in this section concentrates on the distributed aspects of the incidents while omitting unnecessary details.

As shown in the figure below, in a typical distributed attack system, the "intruder" controls a small number of "masters," which in turn control a large number of "daemons." These daemons can be used to launch packet flooding or other attacks against "victims" targeted by the intruder.

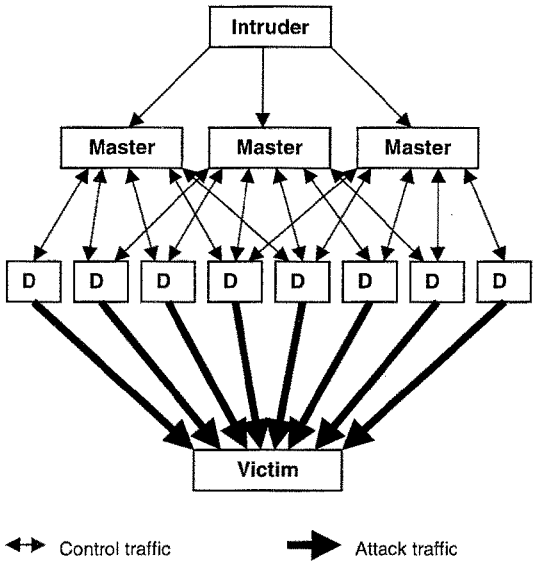


Figure 1 – Distributed-Systems Attack

In the incidents that have occurred so far, daemons were installed at several hundred sites, typically through the exploitation of well-known vulnerabilities that lead to root privileges on the compromised machines. Though some implementations of the daemon program do not require root privileges to launch attacks, in practice most of the daemons were concealed by the installation of "root kits" designed to hide evidence of the intrusion. Intruders have also sometimes used system facilities such as "cron" to ensure that a daemon would continue to run even if one instance of it were deleted or the system was rebooted.

There are indications that the processes for discovering vulnerable sites, compromising them, installing daemons, and concealing the intrusion are largely automated, with each step being performed in "batch" mode against many machines in one "session." Daemons have been discovered on a variety of operating systems with varying levels of security and system management.

Once installed and operating, the daemon announces its presence to several (usually three or four) predefined masters and awaits further commands. The master program records that the daemon is ready to receive commands in an internal list, which can be retrieved by the intruder. Lists recovered from incidents have included hosts in several different nations. Masters can cause daemons in the list to launch attacks, shut down gracefully, or even announce themselves to a new master server. Intruders have used cryptographic techniques to conceal the information recorded by the master daemons.

Upon command from an intruder, the master can issue attack requests to the daemons in its list. These requests contain information about the requested attack, such as the address of the victim, the duration, and other parameters. Upon receipt of the request, the daemon proceeds to attack the victim, usually by flooding the victim with packets. No further contact from the master is necessary.

The master programs frequently operate as ordinary user programs on compromised hosts, where their activity can easily be hidden. Unlike the daemon programs, which are intended to be run on sites with a substantial network capacity, traffic to and from the master program is limited to control messages.

In one incident reported to the CERT Coordination Center, a flooding attack was aimed at a major university. This attack involved several hundred daemons scattered over a wide variety of locations, and it generated enough traffic to disable the university's Internet connectivity for a period of several days.

Several incidents have indicated that intruders are actively seeking systems with good network connectivity for compromise and installation of the daemon program. The indiscriminate installation of daemons on any system with a significant network capacity has included systems whose compromise could have life-threatening consequences.

The experiences of those who reported early attacks highlight the need for better forensic techniques and training, the importance of close cooperation, and concern for the rapid evolution of intruder tools.

- **Better forensic techniques and training** – Detecting and eliminating master programs is a critical part of disabling a distributed intruder system, but unfortunately the masters often do not leave obvious signs of intrusion on the system where they are installed. In most cases, the master hosts were identified after forensic examination of daemons involved in a denial-of-service attack. This forensic analysis was expensive and limited to a few knowledgeable people with experience in the field, but ultimately most of what we know today about how the systems work is a result of this analysis. Forensic techniques and training must be available to a much larger audience to respond to these attacks in the future.

- **Close cooperation and communication** – Prior to the workshop, many participants had incomplete information regarding the tools and methods used by intruders in this kind of attack. By sharing their knowledge, they were able to establish a more complete understanding of distributed intruder tools.

- **Rapid evolution of intruder tools** – The intruder tools encountered in the incidents leading to the creation of this document changed substantially during the planning of the workshop and have continued to evolve since then. As intruders learn to use established technologies to their advantage, the incident response community needs to be better prepared to meet this challenge.

3. Audience-Specific Information

Managers

For management, the issues related to the ongoing development of distributed attack tools, such as trinoo and tribe flood network (for details, see CERT/CC incident note IN-99-07: http://www.cert.org/incident_notes/IN-99-07.html), center largely around the need to understand fully the ramifications of the intruder tools and to perform impact and organizational risk assessments on a priority basis. The results of these assessments then need to be incorporated into plans such as those for operational guidance, equipment acquisition, service contracts, and equipment configuration.

Planning and coordination before an attack are critical to ensuring adequate response when the attack is in progress. Since the attack methodology is complex and there is no single-point solution or "silver bullet," resolution and restoration of your systems may be time-consuming. The bottom line for management is that your systems may be subject at any time to distributed attacks that are extremely difficult to trace or defend against.

Although an organization may be able to harden its own systems to help prevent implantation of the daemon portion of a distributed attack tool, there is essentially nothing a site can do with currently available technology to prevent becoming a victim of, for

example, a coordinated network flood. The impact upon your site and operations is dictated by the (in)security of other sites and the ability of a remote attacker to implant the tools and subsequently to control and direct multiple systems worldwide to launch an attack. The result may be reduced or absent network connectivity to your enterprise for extended periods of time, possibly days or even weeks depending upon the number of sites attacking and the number of possible attack networks that could be activated in parallel or sequentially. Therefore, to minimize the effect on business operations, it is important to know and document *in advance* the actions the enterprise will take and the primary contingency contacts who must be notified.

Below are some recommend actions for coping with the potential for an attack using distributed-system intruder tools:

- Become fully informed with regard to the nature of the attacks and the potential ramifications. Senior management should receive direct briefings from security staff in an effort to facilitate full understanding.

- Be cognizant of your own site's security posture. If your site is capable of being easily compromised due to inattention to security issues and your systems are used as either master(s) or daemon(s) for such an attack, it is possible you may share liability for damage caused to victim sites. (Consult with your organization's legal advisors and inform them of the attacks.) The reputation of your enterprise may also be at risk from the adverse publicity that may result.

- Assess the services that are mission critical for your particular business. Determine the impact upon mission-critical services if Internet connectivity is unavailable for an extended period. Develop contingency plans for continuity of operations in the event of an extended Internet outage. Consider and plan to insure against possible revenue loss due either to lost opportunity (for example, the absence of connectivity to your site for staff members, external customers, and business partners) and in lost sales (for example, an electronic commerce site is flooded and orders cannot be received). Read insurance policies carefully, and seek legal opinion on coverage for distributed-systems attacks.

- Develop an augmentation strategy to provide staff and other resources in the event of an attack. Determine which staff may be needed and where they should report. Be sure there are phone or alternative communications since electronic communication may be difficult or impossible.

- Be sure your staff have the time and resources needed to perform traffic analysis, intrusion detection, coordination with upstream providers, and other activities described under "System Administrators" below.

- Ensure privacy issues associated with log retention and review have been addressed in policy and that adequate analytical information is readily available to critical staff in the event an attack occurs.

- Examine your current policy requirements. In particular, ensure responsibility is defined for 1) enforcing minimum security standards; 2) cutting off users (even executive-level users) whose accounts may have been compromised or are at risk; and 3) disconnecting uncontrolled Internet connections.

- Be sure that all levels of management understand and are held accountable for security planning and implementation. Be sure that an adequate and enforceable acceptable use policy exists enterprise-wide.

- Realize that the escalating Internet threat environment must be matched by corresponding investments in security. Define security resources in the budget.

- Examine your current network and security architecture. Many sites have optimized connectivity for speed of access, making decisions that complicate security measures. In the escalating threat environment, speed and reliability can be denied unless security is included in the architecture.

- Aggressively develop cooperative relationships to support security across organizations and policy to govern those relationships. To deal effectively with distributed agents, your organization may need to cooperatively support security at other Internet sites. Internet service providers and incident response organizations should be supported.

- Pressure vendors to provide more security in their default services and configurations. Simply correcting known vulnerabilities in new releases would reduce the population of candidate sites for intruders. Ask your vendors specifically if they support the capabilities listed in the "Internet Service Providers" section.

Finally, managers need to consider these trends:

- The intruder community is actively developing distributed technology.

- There are multiple categories of existing distributed-systems tools, including distributed sniffers, denial of service, and information gathering.

- In a relatively short amount of time, unsophisticated intruders can acquire sophisticated tools, enabling them to control and use significant portions of the Internet for their attacks.

System Administrators

With the increased sophistication of intruder tools comes the critical need for action. The following table lists actions identified at the Distributed-System Intruder Tools Workshop, along with a suggested time frame for dealing with attacks using distributed-system tools.

	Immediately (< 30 days)	Near Term (30 – 180 days)	Long Term (> 6 months)
Protect	▪ Apply anti-spoofing rules at the network boundary. (This makes your site a less appealing target for intruders.) ▪ Keep systems up to date on patches. ▪ Follow CERT/CC & SANS best practices. ▪ Review boundary security policy to ensure outbound packets are restricted appropriately.	▪ Establish reference systems using cryptographic checksum tools such as Tripwire®. ▪ Scan your network periodically for systems with well-known vulnerabilities & correct problems that you find. ▪ Evaluate & (possibly) deploy an intrusion detection system (IDS).	▪ Identify a system administrator with responsibility for each system, who has the authority, training & resources to secure the system. ▪ Deploy resources for host-based intrusion detection. ▪ Provide security training for users. ▪ If you do not have sufficient resources or support to effectively protect systems, lobby for them.
Detect	▪ Look for evidence of intrusions in logs, etc. ▪ Look for distributed tool footprints as described in documents from the CERT/CC or your incident response team. ▪ Enable detection of unsolicited ICMP echo replies & unusually high traffic levels.	▪ Periodically compare systems to your reference system using cryptographic checksum tools such as Tripwire®. ▪ Run host-based software to detect vulnerabilities & intrusions.	▪ Develop a system for profiling traffic flows & detecting anomalies, suitable for real-time detection & prevention. ▪ Create and practice a response plan.
React	▪ Report to a predefined list of contacts, approved by management. ▪ Establish detailed, written, management-approved plans for communicating with IRTs, ISPs, & law enforcement. Include out-of-band contacts. ▪ Obtain training & experience in forensic techniques required to analyze compromised systems & identify other hosts involved, such as the master hosts in a distributed network.	▪ Ensure ability to capture, analyze, & collect forensic evidence accurately & quickly by developing a "forensic toolkit" of tools & programs to assist in forensic analysis. ▪ Work with your ISP to establish a good business relationship, with service-level agreements that identify the ISP's responsibilities in tracking & blocking traffic during DoS attacks.	▪ Work with management to ensure that policies are in place that allow appropriate measures against suspect systems. ▪ Work with your ISP to implement improved security requirements & capabilities in your service-level agreement.

Table 1 – Suggestions for System Administrators

Additional comments for system administrators:

When you set up intrusion detection software, ensure that it is both fault tolerant and capable of maintaining logs on a highly saturated network. The definition of a highly saturated network varies from organization to organization. A good metric is the amount of traffic seen divided by the maximum bandwidth available to the organization. Expect to see near 100% capacity during a distributed denial-of-service attack.

In setting up logs, have the ability to parse log information at a high rate. Workshop participants recommend attention be paid to searching based on host name/IP number.

Be able to search at least packet headers for attack signatures.

Finally, look to an incident response team for techniques and information for dealing with distributed attacks and the evolving attack tools.

Internet Service Providers (Network Operators)

For the purposes of this report, an Internet service provider (ISP) is considered to be an entity that operates an Internet backbone that is used to carry traffic between two or more other Internet-connected networks. The term *ISP* refers to commercial network operators, research and education networks, government-operated networks, etc.

The transport and access portions of networks characterize the unique role of an ISP in the context of a distributed-system attack. Packets generated from multiple sources during a distributed denial-of-service attack, for example, are likely to be transported across one or more ISP network backbones en route to the victim site. The access portions of an ISP's network (physical connection points of downstream hosts and networks) may be either components of an attack or the end victim.

Considering only the transport and access portions of ISP networks, a network operator's role in a distributed attack is essentially composed of two things:

1. Identifying and controlling traffic flows from the point the traffic enters the network (ingress) to the point the traffic leaves the network (egress).
2. Ingress filtering at the network edge and/or network borders to prevent origination of packets with spoofed source IP addresses.

In addition to the unique characteristics of the ISP networks, the networked computer systems used by ISPs to deliver services such as DNS, email, and web hosting may be attractive locations for intruders to install distributed-system tools for several reasons:

- Active traffic patterns may obscure the use of attack tools.
- Close proximity to high-capacity network backbones enables attacks to have a high impact.

ISP systems themselves may also be high-impact targets for distributed-system attacks. People and systems depending on an ISP's services tend to use shared resources at some level. A carefully targeted attack on one or more critical shared resources may affect a large number of Internet users.

The issues facing an ISP with regard to its networked computer systems being used in an attack, or being the target of an attack, are otherwise not unique and can be considered to be on par with issues faced by system and network administrators at other Internet sites (see the section for system administrators).

During an ongoing attack, an ISP may need to trace traffic flows from the point the traffic leaves the network (egress) to the point the traffic enters the network (ingress). This is especially true in cases where distributed attacks are launched using packets with spoofed source IP addresses.

Distributed attacks are likely to involve many source addresses, possibly from many diverse physical network paths. Near the target, traffic flows are likely to appear to be from many different source addresses and relatively few physical network paths. Near a point of origin, traffic flows may appear to be from a small number of source addresses and relatively few physical network paths. When tracing from a victim back to multiple attack sources, the traffic flows will probably deaggregate into many separate source addresses and physical network paths. The proximity of an ISP to the victim and the origin of an attack will determine the scope of an attack's traffic flow that is visible to the ISP.

Because distributed intruder systems may originate traffic from a number of different network backbones, it is likely that a global network operator will have a more complete view of the distributed nature of the attack. Smaller regional network operators are likely to see distributed attacks in aggregated form based on the number of upstream network connections.

In a distributed bandwidth denial-of-service attack, the proximity of an ISP to the end victim may have an indirect impact on the ISP and other downstream sites sharing the ISP's network resources. It is possible for portions of an ISP backbone to be overwhelmed, causing degradation and/or denial of service for sites that are not directly targeted in an attack.

Coordination among network operators and among sites involved in incidents is essential for diagnosis, tracing, and control of distributed attacks.

The following table summarizes actions the ISP community can take to better deal with distributed attacks, some actions particularly for distributed denial-of-service attacks. After the table are further explanations.

	Immediate	Short Term	Long Term
Protect	Establish crisis policy and procedures. Maintain and enforce an acceptable use policy.	Do ingress filtering. Disable directed broadcasts.	Educate customers. Implement automated anti-DoS policy enforcement.
Detect	Establish an incident response team.	Review high-profile target systems.	Automate scanning/patching of high-profile target systems. Move detection closer to the source of attack.
React	Do case-by-case egress filtering. Share information with others involved.	Establish a method for tracing back ongoing attacks to their source. Do case-by-case ingress filtering.	Establish a method for tracing back attacks in real time. Perform historical traffic flow analysis.

Table 2 – Suggestions for Internet Service Providers

Protective Measures

Immediate Actions

- Establish crisis policies and procedures.
  Communicate policies and procedures to your constituency and staff. Include procedures for handling reports of attacks from the constituency and from the Internet community. Include provisions for an out-of-band emergency reporting channel in case network communication is unavailable.

- Maintain and enforce an acceptable use policy.
  Include provisions to allow the ISP to track and limit service to those machines and/or networks that participate in attacks resulting from distributed-systems tools.

Short-Term (6 months) Actions

- Do ingress filtering.
  Use ingress filtering to limit origination of IP packets with spoofed source addresses. The goal is to increase the ability to identify components of distributed systems.

- Disable directed broadcasts.
  Prevent the use of networks in packet amplification denial-of-service attacks such as "smurf" attacks.

Long-Term (12+ months) Actions

- Educate customers.
  Educate customers about potential security threats and about security best practices.

- Implement automated anti-denial-of-service policy enforcement.
  Work toward an infrastructure that is able to provide automatic enforcement of policies designed to prevent denial-of-service attacks.

Detecting Attacks

Immediate Actions

- Establish an incident response team.
  Pre-allocate resources to respond to security incidents.

Short-Term (6 months) Action

- Review high-profile target systems.
  Establish the practice of reviewing infrastructure systems that may be highly visible targets for hosting distributed systems.

Long-Term (12+ months) Actions

- Automate the review and patching of high-profile target systems.
  This automation helps to reduce the risk of having critical systems compromised due to well-known vulnerabilities for which there are patches.

- Move the initial detection point closer to the source(s) of attack.
  Rather than detecting attacks close to the victim, work toward an infrastructure that makes it possible to detect attacks closer to the attack source(s).

Reacting to Attacks

Immediate Actions

- Do case-by-case egress filtering.
  Apply egress filtering to identifiable packet streams to stop attacks from leaving the network backbone and to limit the immediate effects of an attack on a victim site. "Blackholing" the victim host or network might be necessary if filtering is not possible. This should usually be done only if it does not do more harm than good. It will, of course, deny service to the null-routed host or network but will probably stop the attack closer to the source and possibly restore service to other hosts or network elements.

- Share information with others involved.
  Working with other involved sites and sharing information is essential to disabling an entire distributed attack network.

Short-Term (6 months) Actions

- Establish a method for tracing back ongoing attacks to their source.
  Enhance your ability to trace distributed attacks back to the source(s) or ingress point(s) using existing features and tools.

- Do case-by-case ingress filtering.
  Once an attack has been traced back to a source or an ingress point, use ingress filtering to prevent the attack from entering the network backbone. Filters should be tailored to stop the particular attack rather than being general anti-spoofing filters.

Long-Term (12+ months) Actions

- Establish a method to trace back attacks in real-time.
  Establish a method for real-time trace back attacks traffic flows from the victim or egress point to the source(s) or ingress point(s).

- Perform historical traffic flow analysis.
  Establish a method for historical traffic flow analysis to gain global visibility for identifying distributed attack systems.

Incident Response Teams (IRTs)

This section highlights issues for incident response teams to consider for detecting, responding to, and protecting against distributed attacks. Because IRTs generally collect and process incident information from a large constituency consisting of one or more large distributed networks, they play a crucial role in the detection of and response to distributed attacks.

Because of the variation among response teams, it is difficult to provide suggestions that apply to all. When developing this section, workshop participants considered incident response teams that have one or more of the following responsibilities:

1. Coordinating and distributing security information (CERT/CC)
2. Setting and implementing site security policy (serve as a corporate IRT)
3. Coordinating response to incidents (university response teams)
4. Maintaining data integrity (audit teams)
5. Protecting very large networks (large ISPs)
6. Identifying and tracking intruders (law enforcement)

Regardless of a team's responsibilities, the best protection against attacks is to be prepared. General information about incident response teams, procedures, and policies can be found in the following sources:

Handbook for Computer Security Incident Response Teams (CSIRTs), by Moira J. West-Brown, Don Stikvoort, and Klaus-Peter Kossakowski.
http://www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html

Forming an Incident Response Team, by Danny Smith
http://www.auscert.org.au/Information/Auscert_info/Papers/Forming_an_Incident_Response_Team.html

In addition, general security advice can be found on the web sites of members of the Forum of Incident Response and Security Teams (FIRST). Links can be found on the FIRST web site: http://www.first.org/

The suggestions below focus more specifically on attacks using distributed-systems intruder tools. The table provides highlights, and further details follow the table.

	Immediate	Short Term	Long Term
Protect	Determine chain of command. Be aware that your infrastructure may experience consequences of an attack.	Open communication channels with your constituency: provide attack signatures; encourage reporting; provide information. Encourage your constituency to implement filters.	
Detect	Develop criteria for detecting distributed-systems attacks.	Develop procedures/ algorithms for dealing with large amounts of traffic.	Develop procedures/ algorithms for handling automated incident reports.
React	Scope the extent of the attack. Escalate the priority of identifying machines acting as masters. Block traffic from known masters. Distribute information to appropriate IRTs or law enforcement.	Encourage your constituency to capture, log, & report suspicious traffic. Deploy temporary sensors such as network sniffers or intrusion detection systems.	Provide tools & methods for detecting installation of masters & daemons if possible.

Table 3 – Suggestions for Incident Response Teams

Protecting Systems

The best step a response team can take to prevent distributed-systems attacks is to raise awareness within your constituency. They need to be aware of the concept that the security of any network on the Internet depends on the security of all other networks. The widely varying implementation of security measures is what often makes a distributed attack successful.

Some of the suggestions below are not unique to distributed attacks, but as intruder tools become more distributed these issues become more important. The appropriate time frame for action depends on the mission of the IRT, so the time frames below are suggestions.

Immediate Actions

- Determine chain of command both internally for your team and externally for providers of critical infrastructure within your constituency.

  This is not specific to distributed attacks but is important to understand when handling a crisis. The information should be available ahead of time to avoid delays when the IRT is working under pressure.

- Be aware that your own infrastructure may experience consequences of distributed-systems attacks, such as denial-of-service attacks, if your network or one near your network is targeted.

  Consider developing contingency plans, and establish immediate, short, and long term goals to handle distributed attacks. Use the points in this section as guidelines or a starting point.

Short-Term Actions

- Open communication channels with your constituency.
  1. Provide attack signatures – Providing signatures of known distributed attacks helps members of your constituency become sensors, contributing to your successful detection, scoping, and diagnosis of these attacks.

  2. Encourage members of your constituency to report incidents – Receiving reports of attacks and anomalies is a fundamental and necessary piece of detecting distributed attacks.

  3. Distribute information about ongoing attacks – Communication about ongoing attacks needs to flow in both directions. Informing members of your constituency about significant ongoing attacks raises awareness and provides incentive for continuing to report incident data.

- Encourage constituency to implement filters (both inbound and outbound) that can stop potential attacks.

  At a minimum, encourage members of your constituency to block outbound spoofed traffic, inbound traffic associated with well-known vulnerabilities that are commonly used in tools for widespread compromise and allocation of resources, and ports that are used for communication and control in distributed intruder networks.

Detecting Attacks

Immediate Actions

- Develop criteria for detecting distributed-systems attacks.

  Because response teams are often in the unique position of processing incident data from one or more very large networks, they are one of the few entities capable of detecting and understanding the scope of an attack distributed across multiple networks. Thus, we encourage response teams to carefully examine data, reports of incidents, and output from intrusion detection systems looking for signs of distributed attacks. Ultimately, response teams should strive to distinguish distributed attacks from other activity.

  Relying on signatures for identifying specific distributed attacks is not enough since teams receive data about new and novel tools and attacks. It is important to consider how future attacks may be detected, considering that the intruder community is moving toward distributed models for many types of tools.

Short-Term Action

- Develop procedures/algorithms for dealing with large amounts of traffic, and share them with other teams.

  A problem not unique to distributed attacks is finding mechanisms to efficiently process large amounts of data received from diverse sources without missing anything important. As intruder tools continue to develop toward distributed models, it becomes increasingly important to use mechanisms for automatic processing of incident data. IRTs can benefit from sharing tools and effective algorithms for detecting distributed attacks.

Long-Term Action

- Develop procedures/algorithms for handling automated incident reports.

  In the long term, a community effort is needed to develop procedures and algorithms for handling automated incident reports. An important component of that is developing a common language for representing incidents. Several efforts are under way both in the IDS community and within the CERT/CC that will enable automated incident reporting in the near future.

Responding to Attacks

Some of the distributed attacks that workshop participants have seen thus far have involved bandwidth consumption denial-of-service attacks. When responding to this specific type of distributed attack, keep in mind that resources that depend on available bandwidth (such as email) may not be reliable. In responding to attacks using distributed intruder tools, teams should take the following actions:

Immediate Actions

- Scope the extent of attack, both locally and with other response teams.

  One of the most important components in determining appropriate response is finding the scope of an attack. Determining scope may require communication with multiple sites within your constituency and, often, with other response teams.

- Escalate the priority of identifying machines acting as masters.
  Identifying masters is a key component of response to distributed attacks. Teams need to obtain contact information for those sites, and communicate with them to solve the problem. Depending on the situation, the optimal strategy may involve either immediately disabling masters or leaving them up to monitor and collect additional data.

- Block traffic from known masters when possible.
  If it is possible, block traffic from machines known to be acting as masters. This option may be useful in situations where machines within your constituency are actively involved in an ongoing distributed attack.

- When appropriate, distribute information to appropriate response teams or law enforcement authorities.

Short-Term Actions

- Encourage members of your constituency to capture, log, and report suspicious traffic.

- Deploy temporary sensors such as network sniffers or intrusion detection systems as appropriate.

Long-Term Action

- Provide tools and methods for detecting installation of masters and daemons, if possible.

4. A Final Word

Participants in the Distributed-Systems Intruder Tools Workshop spent two-and-a-half intensive days on distributed tools and ways to address this evolving threat. This paper contains the outcome of that work. Though we have described aspects of a response for separate audiences, it is clear that coordinated action by management, system administrators, Internet service providers and network operators, and incident response teams is needed to deal effectively with the threat of these tools. To a greater extent than previously, there is a systemic cause and the need for a systemic solution as reflected in many of the recommendations in this report.

Distributed-system intruder tools demonstrate that the security of any site on the Internet depends, in part, on the security of all other sites on the Internet. Coordinated attacks across national boundaries have been observed. The tools and attacks demonstrate that a network that optimizes its technology for speed and reliability at the expense of security may experience neither speed nor reliability, as intruders abuse the network or deny its services. The intruder technology is evolving, and future tools may be more difficult to defeat.

Workshop participants encourage readers to distribute this paper widely, but also to be vigilant, keeping informed about further developments and checking web sites of organizations such as the CERT/CC, other members of the response community, and vendors.

This paper was last updated on December 10, 1999

Consensus Roadmap for Defeating Distributed Denial of Service Attacks

A Project of the Partnership for Critical Infrastructure Security
Version 1.10 - February 23, 2000**

Prepared for the Partnership By:

CERT/CC at Carnegie Mellon University (Rich Pethia*),

The SANS Institute (Alan Paller*), and

The Center for Education & Research in Information Assurance & Security (CERIAS) at Purdue University (Gene Spafford*)

Reflecting the active participation, shared experience and insights of:

Stephen Northcutt of the Global Incident Analysis Center
Bill Cheswick of Lucent Technologies
Steve Kent* of BBN Technologies
Kelly Cooper from GTE Internetworking
Randy Marchany, Phil Benchoff, Valdis Kletnieks and Ron Jarrell of Virginia Tech University CIRT
David Dittrich of the University of Washington
Mudge* of The L0pht and @Stake
Neal Ziring of the National Security Agency
Eric Cole of Vista IT
Gary Gagnon, Steven Christey, and David Mann of MITRE
Andre Frech of Internet Security Services
Kevin Ziese of Cisco
David LeBlanc of Microsoft
Craig Ozancin of Axent
Adam Shostack of BindView
Diego Zamboni, Tom Daniels and Pascal Meunier of Purdue University
Henry Kluepfel of SAIC

---

*Participants in the meeting on cybersecurity with President Clinton on February 15.
** This document is being updated. Before implementing the recommendations, email info@sans.org with the subject Roadmap. The latest version will be emailed to you.

Defeating Distributed Denial of Service Attacks

Version 1.10 February 23, 2000

Contents

Introduction

The distributed denial of service attacks during the week of February 7 highlighted security weaknesses in hosts and software used in the Internet that put electronic commerce at risk. These attacks also illuminated several recent trends and served as a warning for the kinds of high-impact attacks that we may see in the near future. This document outlines key trends and other factors that have exacerbated these Internet security problems, summarizes near-term activities that can be taken to help reduce the threat, and suggests research and development directions that will be required to manage the emerging risks and keep them within more tolerable bounds. For the problems described, activities are listed for user organizations, Internet service providers, network manufacturers, and system software providers.

Key Trends and Factors

The recent attacks against e-commerce sites demonstrate the opportunities that attackers now have because of several Internet trends and related factors:

- Attack technology is developing in an open-source environment and is evolving rapidly. Technology producers, system administrators, and users are improving their ability to react to emerging problems, but they are behind and significant damage to systems and infrastructure can occur before effective defenses can be implemented. As long as defensive strategies are reactionary, this situation will worsen.

- Currently, there are tens of thousands – perhaps even millions – of systems with weak security connected to the Internet. Attackers are (and will) compromising these machines and building attack networks. Attack technology takes advantage of the power of the Internet to exploit its own weaknesses and overcome defenses.

- Increasingly complex software is being written by programmers who have no training in writing secure code and are working in organizations that sacrifice the safety of their clients for speed to market. This complex software is then being deployed in security-critical environments and applications, to the detriment of all users.

- User demand for new software features instead of safety, coupled with industry response to that demand, has resulted in software that is increasingly supportive of subversion, computer viruses, data theft, and other malicious acts.

- Because of the scope and variety of the Internet, changing any particular piece of technology usually cannot eliminate newly emerging problems; broad community action is required. While point solutions can help dampen the effects of attacks, robust solutions will come only with concentrated effort over several years.

- The explosion in use of the Internet is straining our scarce technical talent. The average level of system administrator technical competence has decreased dramatically in the last 5 years as non-technical people are pressed into service as system administrators. Additionally, there has been little organized support of higher education programs that can train and produce new scientists and educators with meaningful experience and expertise in this emerging discipline.

- The evolution of attack technology and the deployment of attack tools transcend geography and national boundaries. Solutions must be international in scope.

- The difficulty of criminal investigation of cybercrime coupled with the complexity of international law mean that successful apprehension and prosecution of computer crime is unlikely, and thus little deterrent value is realized.

- The number of directly connected homes, schools, libraries and other venues without trained system administration and security staff is rapidly increasing. These "always-on, rarely-protected" systems allow attackers to continue to add new systems to their arsenal of captured weapons.

Immediate Steps to Reduce Risk And Dampen the Effects of Attacks

There are several steps that can be taken immediately by user organizations, Internet service providers, network manufacturers, and system software providers to reduce risk and decrease the impact of attacks. We hope that major users, including the governments (around the world) will lead the user community by setting examples – taking the necessary steps to protect their computers. And we hope that industry and government will cooperate to educate the community of users – about threats and potential courses of action – through public information campaigns and technical education programs.

In all of these recommendations, there may be instances where some steps are not feasible, but these will be rare and requests for waivers within organizations should be granted only on the basis of substantive proof validated by independent security experts.

Problem 1: Spoofing

Attackers often hide the identity of machines used to carry out an attack by falsifying the source address of the network communication. This makes it more difficult to identity the sources of attack traffic and sometimes shifts attention onto innocent third parties. Limiting the ability of an attacker to spoof IP source addresses will not stop attacks, but will dramatically shorten the time needed to trace an attack back to its origins.

Solutions:

- User organizations and Internet service providers can ensure that traffic exiting an organization's site, or entering an ISP's network from a site, carries a source address consistent with the set of addresses for that site. Although this would still allow addresses to be spoofed within a site, it would allow tracing of attack traffic to the site from which it emanated, substantially assisting in the process of locating and isolating attacks traffic sources. Specifically user organizations should ensure that all packets leaving their sites carry source addresses within the address range of those sites. They should also ensure that no traffic from "unroutable addresses" listed in RFC 1918 are sent from their sites. This activity is often called *egress filtering*. User organizations should take the lead in stopping this traffic because they have the capacity on their routers to handle the load. ISPs can provide backup to pick up spoofed traffic that is not caught by user filters. ISPs may also be able to stop spoofing by accepting traffic (and passing it along) only if it comes from authorized sources. This activity is often called *ingress filtering*.

- Dial-up users are the source of some attacks. Stopping spoofing by these users is also an important step. ISPs, universities, libraries and others that serve dial-up users should ensure that proper filters are in place to prevent dial-up connections from using spoofed addresses. Network equipment vendors should ensure that no-IP-spoofing is a user setting, and the default setting, on their dial-up equipment.

Problem 2: Broadcast Amplification

In a common attack, the malicious user generates packets with a source address of the site he wishes to attack (site A) (using spoofing as described in problem 1) and then sends a series of network packets to an organization with lots of computers (Site B), using an address that broadcasts the packets to every machine at site B. Unless precautions have been taken, every machine at Site B will respond to the packets and send data to the organization (Site A) that was the target of the attack. The target will be flooded and people at Site A may blame the people at Site B. Attacks of this type often are referred to as Smurf attacks. In addition, the echo and chargen services can be used to create oscillation attacks similar in effect to Smurf.

Solutions:

- Unless an organization is aware of a legitimate need to support broadcast or multicast traffic within its environment, the forwarding of directed broadcasts should be turned off. Even when broadcast applications are legitimate, an organization should block certain types of traffic sent to "broadcast" addresses (e.g., ICMP Echo Reply) messages so that its systems cannot be used to effect these Smurf attacks.

- Network hardware vendors should ensure that routers can turn off the forwarding of IP directed broadcast packets as described in RFC 2644 and that this is the default configuration of every router.

- Users should turn off echo and chargen services unless they have a specific need for those services. (This is good advice, in general, for all network services – they should be disabled unless known to be needed.)

Problem 3: Lack of Appropriate Response To Attacks

Many organizations do not respond to complaints of attacks originating from their sites or to attacks against their sites, or respond in a haphazard manner. This makes containment and eradication of attacks difficult. Further, many organizations fail to share information about attacks, giving the attacker community the advantage of better intelligence sharing.

Solutions:

- User organizations should establish incident response policies and teams with clearly defined responsibilities and procedures.

- ISPs should establish methods of responding quickly and staffing to support those methods when their systems are found to have been used for attacks on other organizations.

- User organizations should encourage system administrators to participate in industry-wide early warning systems, where their corporate identities can be protected (if necessary), to counter rapid dissemination of information among the attack community.

- Attacks and system flaws should be reported to appropriate authorities (e.g., vendors, response teams) so that the information can be applied to defenses for other users.

Problem 4. Unprotected Computers

Many computers are vulnerable to take-over for distributed denial of service attacks because of inadequate implementation of well-known "best practices." When those computers are used in attacks, the carelessness of their owners is instantly converted to major costs, headaches, and embarrassment for the owners of computers being attacked. Furthermore, once a computer has been compromised, the data may be copied, altered or destroyed, programs changed, and the system disabled.

Solutions:

- User organizations should check their systems periodically to determine whether they have had malicious software installed, including DDOS Trojan Horse programs. If such software is found, the system should be restored to a known good state.
- User organizations should reduce the vulnerability of their systems by installing firewalls with rule sets that tightly limit transmission across the site's periphery (e.g. deny traffic, both incoming and outgoing, unless given specific instructions to allow it).
- All machines, routers, and other Internet-accessible equipment should be periodically checked to verify that all recommended security patches have been installed.
- The security community should maintain and publicize a current "Top-20 Exploited vulnerabilities" and the "Top 20 Attacks" list of currently most-often-exploited vulnerabilities to help system administrators set priorities.
- Users should turn off services that are not required and limit access to vulnerable management services (e.g., RPC-based services).
- Users and vendors should cooperate to create "system-hardening" scripts that can be used by less sophisticated users to close known holes and tighten settings to make their systems more secure. Users should employ these tools when they are available.
- System software vendors should ship systems where security defaults are set to the highest level of security rather than the lowest level of security. These "secure out-of –the-box" configurations will greatly aid novice users and system administrators. They will furthermore save critically-scarce time for even the most experienced security professionals.
- System administrators should deploy "best practice" tools including firewalls (as described above), intrusion detection systems, virus detection software, and software to detect unauthorized changes to files. This will reduce the risk that systems are compromised and used as a base for launching attacks. It will increase confidence in the correct functioning of the systems. Use of software to detect unauthorized changes may also be helpful in restoring compromised systems to normal function.
- System and network administrators should be given time and support for training and enhancement of their skills. System administrators and auditors should be periodically certified to verify that their security knowledge and skills are current.

Longer Term Efforts to Provide Adequate Safeguards

The steps listed above are needed now to allow us to begin to move away from the extremely vulnerable state we are in. While these steps will help, they will not adequately reduce the risk given the trends listed above. These trends hint at new security requirements that will only be met if information technology and community attitudes about the Internet are changed in fundamental ways. In addition, research is needed in the areas of policy and law to enable us to deal with aspects of the problem that technology improvements will not be able to address by themselves. The following are some of the items that should be considered:

- Establish load and traffic volume monitoring at ISPs to provide early warning of attacks.
- Accelerate the adoption of the IPsec components of Internet Protocol Version 6 and Secure Domain Name System.
- Increase the emphasis on security in the research and development of Internet II.
- Support the development of tools that automatically generate router access control lists for firewall and router policy.
- Encourage the development of software and hardware that is engineered for safety with possibly vulnerable settings and services turned off, and encourage vendors to automate security updating for their clients.
- Sponsor research in network protocols and infrastructure to implement real-time flow analysis and flow control.
- Encourage wider adoption of routers and switches that can perform sophisticated filtering with minimal performance degradation.
- Sponsor continuing topological studies of the Internet to understand the nature of "choke points."
- Test deployment and continue research in anomaly-based, and other forms of intrusion detection
- Support community-wide consensus of uniform security policies to protect systems and to outline security responsibilities of network operators, Internet service providers, and Internet users.
- Encourage development and deployment of a secure communications infrastructure that can be used by network operators and Internet service providers to enable real-time collaboration when dealing with attacks.

- Sponsor research and development leading to safer operating systems that are also easier to maintain and manage.

- Sponsor research into survivable systems that are better able to resist, recognize, and recover from attacks while still providing critical functionality.

- Sponsor research into better forensic tools and methods to trace and apprehend malicious users without forcing the adoption of privacy-invading monitoring.

- Provide meaningful infrastructure support for centers of excellence in information security education and research to produce a new generation of leaders in the field.

- Consider changes in government procurement policy to emphasize security and safety rather than simply cost when acquiring information systems, and to hold managers accountable for poor security.

A Living Document

This Roadmap is a living document and will be updated periodically when new or altered threats require changes to the document. Furthermore it is a consensus document – a product of the joint thinking of some of the best minds in security – and it will continue to improve if you share your experiences in implementing the prescriptions. Please send feedback and suggestions to sansro@sans.org with the subject: DDOS Roadmap.

Mr. HORN. Thank you very much.

We will now go to questioning. It will be 5 minutes to a side. We will get everybody in here in three rounds, if you need them.

[Pause.]

Mr. HORN. This looks like a vote.

What I want to do is start on one issue. Then I will yield to Mr. Turner. As I listened to the comment about maybe we need a tzar in this area, usually my spinal column starts wiggling. As a student of Russian history, I keep wondering what happened to a lot of tzars and who is Rasputin in this operation? So, I guess I would ask, is the Koskinen model a good one for this?

Now, with the Koskinen model, then when Mrs. Maloney and I wrote the President, then talked to him and said, look, you have got to get somebody to coordinate this effort. Some were waving the flag for a tzar. I was not. The way it worked out, one, the President picked a person that he had known before he was President and had trust in.

No. 2, we made him assistant to the President, which is the highest rank you can have in the White House hierarchy. No. 3, he was not in OMB. He was housed near there. The President had him and the President spread the word to the Cabinet that this is serious business, when they finally got around to it.

No. 4, they called on each of the Deputy Secretaries that really run departments and obviously involved the Chief Information Officers, who are the people we ought to be spending the time to be the managers they are supposed to be of communications and information in their particular agencies. So, I guess I would simply like to get the feeling of you as to whether that was a successful model that we could also apply to computer security and not have some tzar in OMB.

Of course, as you know, I am trying to split the management part out of OMB. It might well roost there, but the fact is the model I think worked the way it did. I do not know if any of you want to take that and say, hey, there is another way to look at this. Go ahead. Mr. Gilligan.

Mr. GILLIGAN. Sir, let me give you some perspectives. I think the model with the particular individual, John Koskinen, worked extremely well. I think there were a number of factors that made it work well, one of which was the personal characteristics and strength of John Koskinen. I think there were also some other factors that made it effective. That was the urgency and the immediacy of Y2K heightened the interest across the board.

There was a need and a willing acceptance of someone to help lead the effort across government and across really the country. It is not clear to me that an exact parallel to that would work as effectively in computer security. I know that there has been some frustration, and there continues to be at all levels, with our difficulty of pulling together across-government activities in this area.

So, it is clear that we need to emphasize and we need to work in that area. Obviously it is something the CIO Council is trying to address, and yet we realize that we have limited abilities as well. So, while I would not specifically endorse the exact model, I think we need to continue to look for some way to better leverage our across-government efforts in this area as a part of our solution.

Mr. HORN. Any other thoughts on this? Mr. Tritak.

Mr. TRITAK. I would agree with those comments.

Mr. HORN. So, you would like that model?

Mr. TRITAK. I think what is intriguing about the Koskinen and the Y2K effort generally is, in many respects, the Y2K was your first critical infrastructure challenge to the United States. It had a lot of things going for it. First of all, there was a recognition. In fact, industry actually led the way. The government took a little while to get onboard.

There was an acknowledgment of what the challenge was. There was a known problem. The people rallied for it. I think that when you look at the Koskinen model, it is important to look at what the factors of success were. You have identified quite a few of them. He was viewed as having the authority. He worked very closely with the Cabinet. The Cabinet knew that when he walked into the room, who he was, and what he stood for.

We certainly cannot under-emphasize the importance of a leadership and view it as someone who is speaking with authority on behalf of the President; especially when you are talking about across-agency issues, which critical infrastructure really is all about. If you look at the way this has evolved, there was a time probably when the Computer Security Act was actually passed where you could talk about a computer system within an agency. It was that agency's system.

Now, you are looking more at an interconnected set of systems. You have to ensure, in terms of the government as a whole providing a service to the Nation, that you have strong links across government agencies, as well as within them, so that you do not create weak links in the chain. Now, with that said, I think that we have to look very closely about how the challenges, as ongoing, differ from the Y2K experience before you talk about institutionalizing a new position.

I think certainly some of the ingredients that you indicated bear close scrutiny and attention on that. In fact, you could make the case that, that kind of leadership becomes even more essential in some regards when the known threats are not as immediate, but you know they are out there and they could happen at any time as opposed to a date-specific.

Mr. HORN. Any other comments on this?

I will yield 5 minutes to the gentleman from Texas. If you would like, we could recess now to go vote, and then come back, and then start with your 5 minutes. Is that OK with you?

Mr. TURNER. That is fine.

Mr. HORN. OK. We are going to be in recess then for 20 minutes so we can get these two votes.

[Recess.]

Mr. HORN. This subcommittee will be in order. We will proceed with the questioning. It is 5 minutes for Mr. Turner, the ranking member from Texas.

Mr. TURNER. Thank you, Mr. Chairman.

I appreciated your comments. I really get the impression that what you were saying to us is that there is a lot of work that has got to be done in the area of new technology before we will ever have any hope of really having a secure Internet. I guess I was

kind of curious as to what types of things you are talking about? We made the comparison a minute ago to the Y2K problem.

To me, what we are talking about today dwarfs the Y2K problem. In that arena, we had a date certain we were working toward. We knew if we made it past that date, we had succeeded. The government was able to provide a coordinating role for both the public and the private sector. This challenge seems to be so much greater. When you say we need better technologies, what kinds of things are we talking about?

Mr. PETHIA. First of all, the driving factor behind my belief is that more and more devices attached to Internet are going to become consumer items. I think we are already there with personal computers. We are almost there, even with some devices like routers and fire walls, when you think about having these things installed in libraries, in doctors' offices, and in places where you would not expect to find someone with a degree in computer science.

That is going to continue. We are going to have all kinds of devices at home. We are going to have hand-held portable units. We are going to have cell phones connected, as we already do, into the Internet. So, from one perspective what we need to do is to make security much simpler than it is today. You can configure a very secure personal computer, be it a Unix box or a Microsoft Windows box.

All of the mechanics are there to do that, but it is not easy. It takes a lot of understanding and a lot of knowledge. Not only do you have to get it right the first time, you have to keep it that way over time as you add new applications into your personal computer. So, if you think back to the 1960's when all computers were hard to use in all kinds of ways, the industry responded very well with a lot of research and development in easy-to-use, in fact ease of use was the buzz word for the industry back then.

We need the same effort today, in terms of security controls and security mechanisms. Bring those controls and mechanisms to the point where the average user could use them. I think that is sort of a near-term, by "near-term" I mean a 2- to 3-year effort that could show some results, significant results, major results in that period of time.

Mr. TURNER. I forget the name of the group or company that is certifying whether something is secure or not. I read about it somewhere. Is that the kind of thing that would motivate the private sector to be sure they develop their products in a way that they can be secure?

Mr. PETHIA. I think that kind of thing will certainly help. I think the tension is going to be between the length of time it takes to do the evaluations and the market forces that keep driving new products. Very often, the situation of doing an exhaustive evaluation takes time. By the time you are through with that evaluation, the marketplace has already moved on to the next generation of products. I think we have to struggle with that issue.

Mr. TURNER. That seems to be one of my greater concerns because this field moves so fast. It is always the private sector that is moving forward. We had some government effort over there, though it is not in one place right now. It seems that the govern-

ment effort, even if we consolidate it, is always going to be a step behind what is really going on in the private sector.

So, it is forcing you to try to think of private sector incentives to try to make this all happen. I cannot get it in my mind that the government is going to be able to keep up with it.

Mr. PETHIA. I think the private sector interest is rising. I think as more and more damage happens on the Internet, people are going to begin to understand that investing in security is something they are going to need to do in order to keep their businesses operational. So, I think that is happening. I see a big increase in private sector interest today, over just a year ago. That trend has been going on for several years.

I think the marketplace, in my opinion, has become complacent. The marketplace is currently accepting whatever the vendors produce. I think an awareness campaign and an understanding that technology can be changed; technology does not have to be the way it is today is something that would help move, first of all, the consumer to a better understanding of the kind of quality the consumer should expect from a product.

Then finally, the technology producers, as they begin to see a marketplace for that new product, to begin to produce. There is a place where I think government campaigns focused on broad-scale awareness, understanding, helping the consumer, both in government and outside government, understand that technology possibilities exist beyond what we have available to us today, I think, would go a long way to spur that kind of effort.

Mr. TURNER. Is it a reasonable suggestion to think in terms of a second Internet? After all, we are even getting to the point where much of what takes place can even be done in a wireless mode. Is there a reason to consider that there could be more than one Internet? That there are secure Internets so that we can solve some of our national security type problems and others in a way that we know that we are protected?

Me. PETHIA. Certainly, I think there are some needs for high security in some applications where those networks and systems will remain isolated and should remain isolated from the broad Internet. I think the last 10 years of history has told us that the Internet is going to continue to evolve. It is going to continue to lure people because of the broad connectivity that is available over the Internet, and also because of the dramatic lower cost of operating on this huge network where everybody shares the expense.

I think the economics are going to continue to push most organizations toward the Internet. I think the challenge as to rather than trying to isolate from the Internet, the question is how do we go about fixing the Internet so that we can all enjoy the level of security that we need?

Mr. TURNER. Your effort at Carnegie Mellon, through the Computer Emergency Response Team, seems to me to be an excellent private sector initiative. Do you think government is capable of duplicating that or will it be best left to efforts like yours?

Mr. PETHIA. I think it is going to take a combination of efforts. There are within the government a number of computer emergency response teams in the DOD, in the Department of Energy, and in some of the other agencies. There is the FedCIRC activity which

we actually participate in. So, I think there is a large government effort there. One of the advantages that I think we have is that in addition to the reactive work that we do, we are also housed in a research university.

So, in the private sector where you can have these kinds of reactive capabilities to help us understand what the problem is, but also marry with that a research and development capability we can move toward solution. That, I think, is a good combination. So, there perhaps is a way where government can team with organizations in the private sector, with the government doing some of the response reactive work, ensuring that they have close working relationships with technology researchers so that the researchers really understand what the real problems are.

Mr. TURNER. Thank you, Mr. Chairman.

[The prepared statement of Hon. Jim Turner follows:]

Statement of the Honorable Jim Turner
GMIT Hearing: "Computer Security: Are We Prepared for Cyberwar?"
03/09/00

Thank you, Mr. Chairman. The issue of computer security is broader and potentially poses a greater threat to our country than the Y2K challenge. More than any other nation, the United States depends on interconnected computer systems -- including the Internet -- to support critical operations and services both in the public and private sectors. Federal agencies increasingly rely on computers and electronic data to perform functions that are essential to the national welfare and directly affect the lives of millions of individuals.

While beneficial, this reliance has increased the risks of computer-based fraud, inappropriate disclosure of sensitive data, and disruption of critical computer-supported operations and

services. Recent attacks by computer hackers on several of the nation's largest Internet sites, which rendered these sites inaccessible for hours, illustrate the damage that could occur if the federal computer system was invaded.

With this in mind, it is alarming to know that the federal government is not adequately protecting critical federal operations and assets from computer-based attacks. Recent audits conducted by the General Accounting Office and agency inspectors general show that 22 of the largest federal agencies have significant computer security weaknesses, ranging from poor controls over access to sensitive systems and data, to poor control over software development, and nonexistent or weak continuity of service plans. While a number of factors have contributed to weak federal information security, the

fundamental underlying problem is poor security management.

In May 1998, the Administration issued Presidential Decision Directive 63 (PDD-63), calling for a national effort to ensure the security of the United States' increasingly vulnerable and interconnected infrastructure. On January 7, 2000, in response to PDD-63 and in an effort to better safeguard against computer disruptions within critical sectors, the Administration introduced the "National Plan for Information Systems Protection." The plan calls for new initiatives to strengthen the nation's defense against threats to public and private sector information systems that are critical to the country's economic and social welfare.

The purpose of this hearing is to focus on the federal

efforts being undertaken to protect the nation's critical cyber-based infrastructures. I am pleased that the Congress has made this issue a priority. Only yesterday, the House Committee on Armed Services, of which I am a member, held a hearing on the threats posed to our security by cyber-terrorism. The end goal of this process is to develop a comprehensive national strategy for infrastructure assurance. We definitely have our work cut out for us.

I thank the chairman for his focus on this issue and thank the witnesses that have come here today for their time and expertise.

Mr. HORN. I thank the gentleman.

Now, I yield to the gentlewoman, the vice chairman from Illinois, Mrs. Biggert to question the witnesses for 5 minutes.

Mrs. BIGGERT. Thank you, Mr. Chairman.

If I could ask unanimous consent to include my opening statement.

Mr. HORN. Without objection, it will be so ordered as read at the beginning, after Mr. Turner's opening remarks.

Mrs. BIGGERT. Thank you.

This is a question for all of you. What is the real threat from cyber terrorists to the Federal agencies' mission critical systems? I know that is a broad question, but how does the administration's recently released National Plan for Information Systems Protection address the plans to mitigate these terrorist threats? I think when we were talking about Y2K, we had our mission critical systems. I think that was what was really addressed there. First of all, is there a threat from the terrorists?

Mr. TRITAK. Well, I think the national plan makes clear that the threats posed by cyber terrorists as well as nation states is growing. I would urge you, if you have not already, to get a briefing by Mr. Michael Vaddis at the National Infrastructure Protection Center who could give you a lot more detail, an appropriate level of detail than I can get into. One of the reasons for PDD–63 stemmed from a Presidential commission which asked the question, what are the new threats to the Nation? The cold war is over. It is unlikely that anyone would be foolish enough again to take on the United States with armed forces. So, what are they?

That question was initially prompted, of course, by a number of events that were happening in the mid-1990's, the Towers' bombing, Oklahoma City. What is going on here? The recommendation of that commission was to say that the critical infrastructure of this country are increasingly becoming vulnerable to types of attacks that could be delivered over the information super highway.

Why? Because as was indicated earlier, traditional infrastructures are increasingly relying on computer networks, not only to receive e-mail, but actually perform operational functions of their business. As you move further and further into deregulation, the need to cut your costs to make the margins up, you are going to be relying more and more on information technologies to perform functions which traditionally may have been performed by manual labor for example.

Also, in the past, if a computer operational system went down, say in the electric power industry, they have ways of shifting over to manual type responses in order to keep the flow of services going. Now, over the long-term, more and more of those primary functions are performed by information technology, and if those systems are then networked either through the Internet or some wide area network systems, the potential for someone being able to get in and cause damage increases.

Now, I am glad you also mentioned the critical systems because this is a very important thing about critical infrastructure assurance. What we are concerned about are those systems within our critical infrastructures which, if disrupted, could cause immediate and significant harm to the Nation's security, its economy, or the

health and welfare of its people. If someone means to do harm, they are going to want to leverage their efforts to find weak links in the chain.

So, one of the purposes of the effort that is outlined in the national plan is to begin to raise this issue with industry to make clear that this is more than just a hacking problem. Frankly, they deal with that now. They know that they are being hacked. Their websites are being looked at. The idea that if more and more of their business relies on information technology, for example, banking and finance, e-commerce, where the very nature of the revenue stream turns on information technologies. This is a different problem.

The same thing within the Federal Government. There was a time when you could talk about a computer system within the Federal Government and it was the agency's system. It was insular. It was self-contained. Now, like everywhere else, you are getting inter-connectivity between agencies. They are depending on different services, both within government as well as outside of government.

This inter-dependency is one of the newer challenges. An agency can get their security concerns right, but if they are dependent upon systems which do not have their security right, that is where the vulnerability lies. Your types of attacks which, again, Mr. Vaddis will be in a better position to talk to you about this, they are looking for the weak links. They are not simply going to willy-nilly take on any piece of the information infrastructure. They are going to look for where the highest value payoff is going to come from.

Mr. GILLIGAN. I think Mr. Tritak has done a good job of summarizing the significance of the threat and many of the characteristics that contribute to it. I would only add a couple of thoughts. One, I think it is not just linkages between agencies, but linkages within sites and within agencies where you find I think unknowingly our interconnection.

We are just about intermeshed in our network connectivity among systems that we have the same vulnerabilities. I think second, we really, in my view, have kind of two tiers of threat. Unfortunately, a lot of our emphasis and visibility is on what I will call the lower tier, which is a very unsophisticated, but today, because of the vulnerabilities, is ineffective and gets a lot of visibility.

Now, I think there is one that is much more sophisticated. We only get glimpses of it. In many cases, that is something we do not share a lot of insight. It is almost masked. That is, we are seeing some of these lower sophistication threats. That is what we are focusing a lot of attention. I think we need to because you need to dampen those out of the system before you can really start to focus and then get the protection that you need to address the more sophisticated attack.

Ms. BROWN. Well, I think both gentlemen have done a really good job. I would only add that I think one of the key challenges is not just today's problem, but the ongoing problem. There is new software every month. There are new systems every month. So, there is not a single fix, as in the Y2K, as Mr. Turner and everyone

has talked about. There was a single crisis. There was a single thing that we had to fix.

This is going to be an ongoing problem, and ever more difficult in many ways to stay on top of as we become more and more global. So, we need to look at what can we do today, but also on the more fundamental things to make our systems fundamentally secure. How do we design the systems and how do we design the software so it is not up to the user to fix and put the patches, which will always be there? Somehow, how do we fundamentally make the system more robust?

Mr. PETHIA. I am building briefly on Mr. Gilligan's remarks; this idea of two tiers of threat. At the lowest level, and one of my big concerns, and the reason that I am advocating for increased emphasis on analysis, capability, and data collection is that the low-level threat, the amount of noise generated by that threat is now so huge. We literally get 50 new incidents reported to us every day. We are only 1 of 90 emergency response teams, as well as a number of government agencies who focus on this issue.

There is so much activity out on the network today. It is very difficult to pull out from all of that noise the one or two key things that you really need to pay attention to. In order to stay ahead of this problem, I think we are going to need to become much more sophisticated in the way we collect and analyze incidents data. So we can look for those key indicators that there is something really significant going.

Mrs. BIGGERT. Thank you. Thank you, Mr. Chairman.

Mr. HORN. Thank you. May I suggest that if we have some additional questions, that we have a time problem here. A number of us are involved in things that just go every 15 minutes, starting at around 12:05 p.m. So, if you do not mind, we would like to submit some of these questions, I know that I have, to you. Take your time, but we would love to have them in the record at this point, your best thoughts, if that is OK with you.

[The information referred to follows:]

Questions for Witnesses

1) (**ALL**) What is the real threat from cyber terrorists to Federal agencies' mission-critical systems?

   a) How does the administration's recently released "National Plan for Information Systems Protection" address plans to mitigate these terrorist threats?

2) (**ALL**) How involved is the private sector, which produces virtually all computer equipment and peripheral devices (e.g., modems, fax machines), in discussing and leading computer security initiatives?

3) (**ALL**) What guidance are Federal agencies following to develop computer security plans and procedures (e.g., National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB))?

4) (**ALL**) Is there a need for a Federal Chief Information Officer to coordinate efforts, disseminate guidance, and be the focal point for computer security issues? (analogous to John Koskinen's role in the Year 2000 effort)

Questions for Witnesses

5) (**ALL**) DISPLAY COLORED CHART Before each of you is a chart that illustrates the key participants in managing the Federal Government's computer security initiatives. The yellow bubbles at top and sides represent Executive Branch organizations. The bottom of the chart contains organizations that are also key stakeholders in Federal computer security.

   a) Clearly, it's good that all of these organizations are working on computer security issues. However, the key question remains: Who is coordinating Federal computer security efforts?

6) (**ALL**) What, if any, other policies have Federal agencies or the private sector developed to protect key Federal assets?

Ms. BROWN. Thank you very much for the opportunity.

Mr. HORN. Well, we thank you. The chart here I particularly want your comments. That is our question 5, for the majority. I think you have it. Now, this was prepared by counsel, Mr. Ryan. He is 100 percent Irish. I am only 50 percent Irish. It is not even St. Patrick's Day. I look at that. I looked for Jesse Jackson on the floor. It looks like the Rainbow Coalition. He is serious about this and we are.

So, we would like your best shot at it, in terms of all of these organizations and how they can work on computer security issues. The key question still remains on who is coordinating this operation? Are there various ways, given the private sector, the Federal sector, the State sector, the local sector, the non-profit sector? So, if you would struggle a little with that, we would appreciate it.

Well, thank you very much for coming. We will now swear in the next panel.

Mr. HORN. We have Mr. Jim Gerretson, Director of Operations, Information, Assurance, ACS Defense, Inc.; Mr. Mark Rasch, senior vice president and legal counsel, Global Integrity Corp.; and Mr. James Adams, chief executive officer, iDEFENSE.

Gentlemen if you will just stand and raise your right-hands.

[Witnesses sworn.]

Mr. HORN. The clerk will note all three witnesses affirmed. We will begin, Mr. Gerretson with you. It will be 5 minutes for a summary. We are going to have to stick to that. We all have your papers. If you were not in the room, they automatically go in at this point in full. If you can give us a summary, and then we would like to have some questions before noon. Then we are going to have to break.

So, Mr. Gerretson, it is all yours.

STATEMENTS OF JIM GERRETSON, DIRECTOR OF OPERATIONS, INFORMATION ASSURANCE, ACS DEFENSE, INC.; MARK RASCH, SENIOR VICE PRESIDENT AND LEGAL COUNSEL, GLOBAL INTEGRITY CORP.; AND JAMES ADAMS, CHIEF EXECUTIVE OFFICER, iDEFENSE

Mr. GERRETSON. Mr. Chairman and members of the committee, thank you for giving me the honor of testifying today. I am here today to give you a brief presentation on hacking. We believe that in order to start to fix your systems and networks, that you have to understand the enemy, and hackers really are the enemy. The following presentation will take you briefly through what we call the hacker protocol and demonstrate just some of the tools and techniques used by hackers to gain access to your systems.

All of the tools that you are going to see today are freely available on the Internet or you can go to a local computer show on a weekend and, for $10 per CD, buy a full CD of different types of hacks. The current data base that we have contains over 3 gigabytes of data. What you see on the screen before you is what we call the hacker protocol. Different people may use different terms, but professional hackers in nation states that implement hacking as warfare do follow the same concepts.

The thing that is important to recognize here is this is highly structured in its approach and in its planning. A good hack, for bet-

ter or for worse, is invariably a well-thought-out, well-executed operation.

Mr. HORN. I might add on that very useful chart that, that will be placed in the record at this point, without objection. All other charts will be put in appropriately where they have been used by the witness or the staff. So, all of those charts will go in the final hearing report.

Mr. GERRETSON. Thank you, sir.

[Slide shown.]

Mr. GERRETSON. The first phase of the hacking protocol is intelligence gathering. This is primarily an espionage operation. There are many facets to it. Social engineering is a large part. I may act as a user calling up a help desk and say I have forgotten my password. Help desks are setup to be very helpful. They will frequently say, the default password is, or your network is. So, I get a lot of information that way.

Open source materials such as newspapers, prospectuses, and library magazine articles are also a wonderful way of getting information. You hear the term a lot, but "dumpster diving" is also a very popular way of getting information on your system.

[Slide shown.]

Mr. GERRETSON. Once we have done the intelligence gathering, the next step is to do reconnaissance. Again, to define the target. Your domain host is the name of your computer system on the network. I want to know what I have got, see if I can attack it, and how I can attack it. This is what we are going to show you. It is a freely available program called NMAP. We are going to take that information that we have gathered and scan your network to determine what is there. The program that we are using is called Ping Sweep.

[Slide shown.]

Mr. GERRETSON. In simple terms, my computer is going out to your network and saying, hello, are you there? Your computers are coming back and saying, yes, I am. What you see here, with these being listed, are computer targets that have come back and said, I am here. What we have now done is identified a target set. We are not wasting our time.

[Slide shown.]

Mr. GERRETSON. The next slide, we are going to take one of those targets that we have identified and go and look for additional information. What we are trying to do is find out what services are open, as you see, I am pointing out. These are all considered services on a computer. This one, for example, is finger, which we will talk about in a second.

What we are doing is finding a means to attack your system. We are also going to go out to try to find out the operating system that your computer is running which is again identified. Once we have this information, we can now go and do specific probes. What we are going to do is take that information and look for a way to get into your system.

[Slide shown.]

Mr. GERRETSON. This presentation that we are going to show you now is one of the tools called Finger. It is an information gathering tool, you are seeing it used in a way it was never intended to be

used. In order to attack and control the system, you need three things. You need a valid user name. You need a valid password, and you need a host address from the computer system that is allowed to talk to you.

If you look across here, as I am highlighting "student one," I now have a valid ID and I now have a valid computer system that I am talking from. I have two of the three items that I need to attack this system.

[Slide shown.]

Mr. GERRETSON. This next scan, web servers as we are all aware, are a wonderful target for attack. It used to be that in order to do the attack, I had to know all of the systems and all of the vulnerabilities. Now, I have a tool that will run it for me automatically. It requires very little work on my part. It identifies the server type that is running and will simply go out and scan all of the CGI weaknesses on this web system. I do not even have to know what these systems are now.

I do not have to know what these vulnerabilities are. It just tells me it finds one. I go out to my tool kit, pull in this particular attack and away I go. Once we do that, we are trying to get a toehold on the system. This is basically I just get into your box any way I can. I cannot control the data. I do not need it, but I am on it and it gives me the next step.

[Slide shown.]

Mr. GERRETSON. The next step is to go from just being a user into what we call the root or administrator level of the system then we really do own this box. I am going to skip this example.

[Slide shown.]

Mr. GERRETSON. We are going to go and actually break into this system and take it over. It acts as a user system. What this program does is it shows us actually going in and doing an attack on the system that in a matter of about 15 seconds turns us into the root administrator of the box, simply from being a user. Once we have gotten control of the system, there are a lot things we can do.

We could kill this box. We could take the information. But what we do want to do is use it again later. So, we are going to hide our track. We do not want people to know we are there. We can do that by deleting files or modifying log files. We are going to show you a quick example of how we just simply modify a log file.

[Slide shown.]

Mr. GERRETSON. This is a program called Wipe. We have a user account. We are called "Reacher." We get into the system. If the system administrator were to check his logs, he would say, why is this guy here. But we have gone and wiped it. We are no longer there. We are now invisible to the person that runs this machine.

[Slide shown.]

Mr. GERRETSON. We can put Trojans on the system. A Trojan is a program that will look like something that is a valid program that is supposed to be there, but in effect it is a program that does a lot of bad things. In this brief example, listen. We can record every keystroke you type on the system. We can turn on your sound system. So, if you have a microphone, we can record everything that is said in the area, and you will never know what happened.

[Slide shown.]

Mr. GERRETSON. Now, sounds bad and it gets worse. I will make a bold statement that if you are connected to the network, and if I have enough time and want to make the effort, I can hack you. The only sure fire way to protect your system is to disconnect it from the network. Take out your floppy. Take out your CD and then lock it up in a secure room. Anything short of that, eventually it can be had.

It sounds pretty bad, but there is hope. It is not all bad; just mostly bad. The first thing is you have to have a vulnerability assessment. You have to know what your security posture is. Second, we believe in the defense-in-depth approach. It is vital. There is no single solution to make your system secure. You have to have layered approachs that complement each other.

The next thing, training is the key. As the earlier witnesses said, there are good people out there, but they just do not understand security. One of the key things to recognize is the solution that works today may not work in 6 months. You will never have a final solution. You are constantly reassessing.

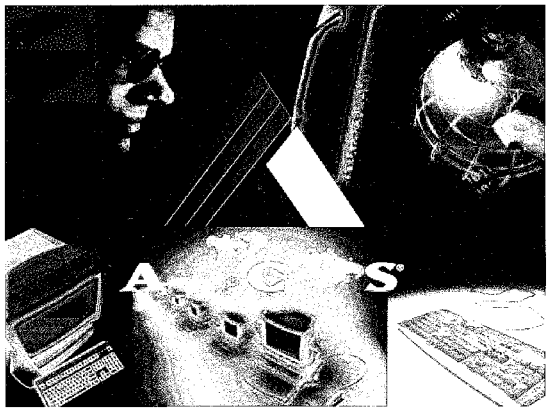
Thank you for your time.

[The prepared statement of Mr. Gerretson follows:]

PREPARED STATEMENT FOR THE

SUBCOMMITTEE ON GOVERNMENT, MANAGEMENT, INFORMATION, AND TECHNOLOGY

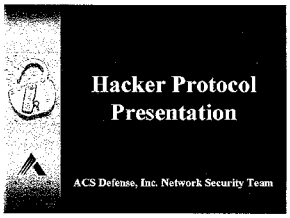
March 9, 2000



Jim Gerretson
Director of Operations
Information Assurance

A C S

ACS DEFENSE WELCOMES THIS OPPORTUNITY to testify before this distinguished Subcommittee on Government Management, Information, and Technology. We believe that Information Assurance is critical to the well being of the United States.

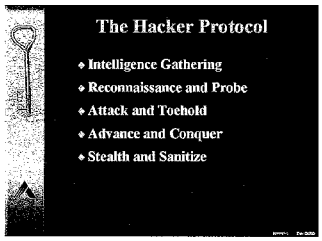


Our presentation today will introduce the members of this committee to the structured nature of hacking. ACS' experience has been that while many people understand the end result of hacking, i.e. a system crashes, or data is damaged or stolen, they don't truly understand ***how*** they were attacked, ***how*** a hacker or team of hackers work, and the ***protocol*** that talented intruders follow. In order for an organization or individual to protect itself, it must know the enemy.

It is important to understand the difference between serious, talented adversaries and so-called "script kiddies," who are proliferating the net today because of easy access to GUI-driven tools. Literally anyone today with limited knowledge of networks and computers can become a hacker. While annoying, this type of hacker activity can be protected against with relative ease. This presentation focuses on the intruder who truly understands networks and computers. Our intent is not to provide a detailed hacker profile, but merely to highlight how they operate.

Slides from today's presentation are included within this document. The slides are a condensed version of the Security Awareness Briefing that ACS provides to customers in order to increase awareness of the hacker's protocol. For readers' convenience, a Glossary of Selected Terms is attached.

THE HACKER PROTOCOL

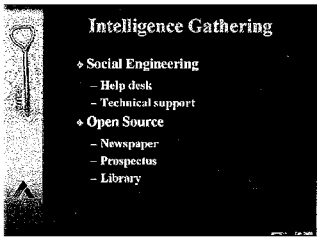


The Protocol consists of five phases:

1) Intelligence Gathering
2) Reconnaissance and Probe
3) Attack and Toehold
4) Advance and Conquer
5) Stealth and Sanitize

Each phase serves a distinct purpose in furthering the ultimate cause of controlling someone else's computer, system or network.

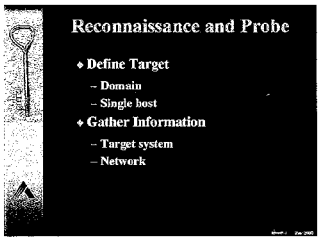
INTELLIGENCE GATHERING

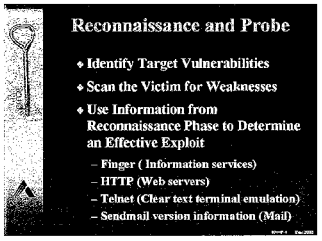


Intelligence gathering begins after attackers have selected a target that meets their specific goals. Attackers will gather intelligence through social engineering, a company prospectus or other open source information. **They will complete this phase before ever touching a computer keyboard**.

RECONNAISSANCE AND PROBE

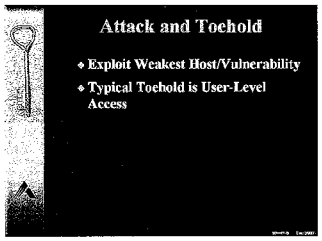
The attackers gather all available information on a selected target in this phase. Methods used include conducting on-line research using tools such as an *internic search, traceroute* and *whois*. This information enables the attacker to determine target parameters including IP address, Host Names, Host Types, User Names and Operating System (OS) types. Attackers begin testing the target for weaknesses or vulnerabilities using information gathered during reconnaissance. Probing methods include port scanning and OS fingerprinting. **Probing determines network architecture, routers and switches, firewall location and system vulnerabilities**.





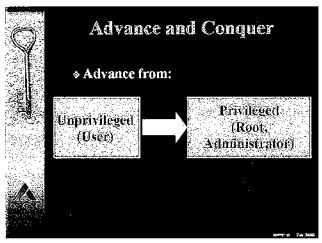
ATTACK AND TOEHOLD

Once attackers have examined the target and identified potential weaknesses, they launch attacks to gain a toehold on the system. The attack usually results in the compromise of a limited access (user) account, at which time the hacker will upload their "Rootkit." A "Rootkit" is an OS specific set of software tools used to continue their attack on the system. **At this stage, a hacker could begin to disrupt network services or use the system in a distributed denial of service attack, such as Trin00**.



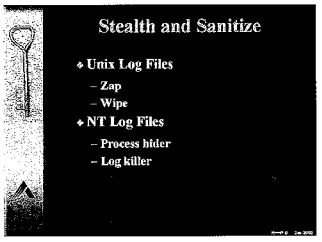
ADVANCE AND CONQUER

In this phase, hackers advance their privileges to system administrator level. This level of access allows hackers complete control of the system and in turn, opens up many more avenues of attacks, exploits, or data manipulation including data theft. **At this point, the entire enterprise network may be at risk.**

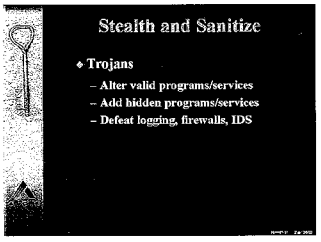


STEALTH AND SANITIZE

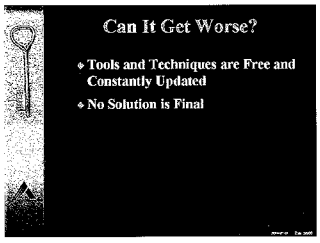
Once hackers have gained root access to the system, the next step is to ensure that their activities go undetected. At a minimum, although in no particular order, a successful intruder will sanitize *logs*, install *trojans*, and place *back doors* on the system. Audit logs that would alert a system administrator to the presence of an unauthorized user or activities are be modified or "wiped."



Trojans, such as "sniffer" programs are installed as legitimate processes that hide the intruder's presence while providing him additional user names and passwords to further compromise the network. *Back doors* are installed to subvert firewalls or provide the intruder with a means of accessing the system undetected by software or hardware protection, even if the original vulnerability is discovered and eliminated.

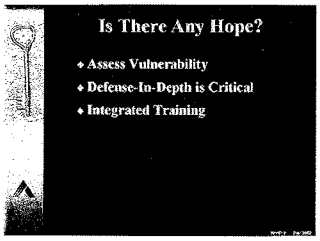


CAN IT GET WORSE?



Yes it can. We are always asked if organizations can completely protect themselves from being hacked. The answer is a qualified "Yes." If they disconnect their network, take out the floppy drive, remove the keyboard and mouse, and lock the system away, the system can not be hacked. Short of that and given enough time, effort and skill, **almost any system can be compromised**.

Is There Any Hope?



Yes, there is. There are several things that can help organizations protect themselves.

First, organizations must understand their specific security posture. *Vulnerability Assessments* are crucial in determining security vulnerabilities and how they could be exploited. An organization must identify the specific threat to their systems and, based upon that threat, determine the risk. They then weigh the cost of not implementing any security measures versus the cost to protect the organization's systems and data. Once those decisions are made, they can begin implementing measures to reduce or eliminate security vulnerabilities. **Government and military organizations are high profile targets and at a much greater risk simply because of what they represent.**

Second, ACS Defense strongly supports a *Defense-in-Depth* approach to protection. No single device or approach can protect your systems. **A layered approach of security measures should be used to protect critical infrastructures**. A combination of security policies, protection devices, detection systems, physical controls, and personnel security is crucial in establishing a sound security posture. This posture gives security personnel the time to either stop or mitigate the effectiveness of an attack before serious damage is done.

Third, ACS Defense supports an integrated training program for system administrators and system security personnel. An integrated program is necessary because the two roles are so intertwined that it is impossible to separate them as individual functions. **A good program must contain periodic training on system security and maintenance to stay current with the changing threat.**

Finally, security is not a one-time event. Just as with training, organizations must conduct routine security assessments and reviews to stay abreast of any threat. **Every day new exploits, viruses, and hacking software tools are released on the Internet**. ACS Defense routinely examines dozens of new tools and exploits each week. We maintain a database of over *3 gigabytes* of selected software tools, exploits, and related documents, and as new information discovered, this database is grows daily.

In conclusion, although an organization's systems may be secure today, there are no guarantees that systems will be secure tomorrow given the constant proliferation of new hacker tools. Only through structured security programs that incorporate a Defense-in-Depth approach can a company maintain the security of their systems and information.

SELECTED GLOSSARY

EXCERPTED FROM:

CRITICAL INFRASTRUCTURE GLOSSARY OF TERMS AND ACRONYMS

Critical Infrastructures – Physical or cyber-based system essential to the minimum operations of the economy and government.

Cyberattack – Exploitation of the software vulnerabilities of information technology-based control components.

Denial of Service – 1) A form of attack that reduces the availability of a resource.
2) Result of any action or series of actions that prevent any part of an information system from providing data or other services to authorized users.

Firewall – 1) An electronic boundary that prevents unauthorized users from accessing certain files on a network; or, a computer used to maintain such a boundary.
2) An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client-server architecture, used to protect internal networks or network segments from unauthorized users or processes.

GUI (Graphical User Interface) – A computer program designed to allow a computer user to interact easily with the computer typically by using a mouse to make choices from menus or groups of icons.

Hacker – Any unauthorized user who gains, or attempts to gain, access to an information system, regardless of motivation.

Information Assurance – Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Network – Information system implemented with a collection of interconnected nodes.

Operating System – Software required by every computer that:
a) enables it to perform basic tasks such as controlling disks, drives, and peripheral devices; and
b) provides a platform on which applications can run.

Mr. HORN. Thank you very much.

We now have our second witness, Mr. Mark Rasch, who is the senior vice president and Legal Counsel for the Global Integrity Corp. Perhaps you would like to tell us a little bit about the corporation.

Mr. RASCH. Yes, thank you, Mr. Chairman.

I work for Global Integrity Corp. It is a company that does information security consulting work for the private sector. So, our clients tend to be things like banks, insurance companies, Fortune 100 companies that take the problem of information protection. Notice I used the term "information protection" and not computer security. They take that problem seriously.

What we are trying to protect here is not the computers themselves, but the information that is contained on those computers. So, the perspective that I bring is what the private sector sees as the problem and what the private sector is trying to do itself to try to solve the problem. One of the things we noticed is that the Commerce Department issued a report in the last couple of days that indicates that U.S. retail e-commerce sales for the fourth quarter of 1999, that is October through December, was about $5.3 billion.

What has happened is this Internet that we created 20 years ago is being asked to do something that it was never designed to do. That is to support a national economy; to support a national infrastructure that it was never designed to do. So, what happens is we have this distributed computer network, which was essentially unsecured. All of the security to that network is essentially added afterwards.

That is being designed now and being asked to protect the critical infrastructure. The attacks that we saw a few weeks ago against Yahoo, Ebay, and others also demonstrated another problem. As a lawyer, this is one that concerns me much more than what concerned me about the year 2000 bug problem, from a litigation standpoint. That is that we are only as secure as everybody else on the Internet.

As the previous panel discussed, these are targets of opportunity. People attack systems because they can get in. They attack the ones that they feel that they can get into. Also, the fact that even if you have done stuff to harden your system, people will break into other people's systems and use those to attack you. So, what we have is a serious looming litigation problem, or what we would call downstream liability.

If you are attacked by somebody and the attack is coming from another corporation that did not secure the systems, and you go to your lawyer and ask, can we sue, which is always the dumbest question to ask a lawyer because the answer is always yes. The question is who are you going to sue, the 17- or 18-year-old hacker, if they are ever identified, or the corporation from whom you are attacked?

So, the idea of a worldwide web that is dependent upon the security of everybody else creates targets of opportunities, not just for hackers, but for lawyers as well. One of the problems also that we have seen is a massive increase, not only in the use of the Internet and the use of the Internet for electronic commerce, but of these types of criminal activity.

For example, from 1998 to 1999, theft of intellectual property increased from 15 percent. Unauthorized access by hackers from inside is up 28 percent. Insider abuse to the Internet is up 17 percent. System penetration by external parties increased 32 percent. Why is this happening? The first reason is that attack technologies are becoming very easy to use. So, as Mr. Gerretson just showed, you can go to any hacker convention, pick up a copy of this disk, put it in your machine, and knowing no more than a lawyer, which is a fairly low standard I would say, put this in your machine and launch an attack on any computer on the Internet.

You do not need to know a lot. It is point and click and you are in. So, the tools are getting easier to use. They are becoming more widely available. In addition, with the growth of the Internet, you have tens of thousands and probably of millions of insecure computers out there that are used as targets of opportunity and methods of attack. The software is becoming increasingly complex and much more difficult to secure.

Software manufactures who are building this software are trying to design it to be functional. If you are coming out with a new word processing program or you are trying to come out with a new operating system, and you are under competitive pressures to get it out to market, you want to make sure that it is functional. Until companies demand security and the government demands security as an integral part of functionality, I do not think the manufacturers are going to ship these things as being at least more secure.

So, these are some of the problems. What is the private sector doing? Well, speaking just for Global integrity, we are doing two things working with the financial services industry, which I think is a model for both the government and for other private sector enterprises. One of them is something called the BITS Laboratory that we are working with the Banking Industry Technology Secretariat and a consortium of banks.

What they are doing is they are developing a series of security standards. We at Global, are testing computer products, hardware, software, and other types of products, against the security criteria. The idea is that the marketplace then will say, for example, banks will say unless your software had been tested against these criteria, we will not buy it. Unless it is pre-configured to be in a secured manner, we will not buy it.

So, we are using the marketplace as a method of trying to ensure security. The second thing is the Financial Services Information Sharing and Analysis Center [FSISA]. This is something that we are doing. Financial services industries, banks, insurance companies, and the like have a secure method of sharing information amongst themselves about attacks and vulnerabilities.

Let us face it, they do not want to tell people that they have been attacked, but they are happy to share information among themselves, if that will lead to more security. These are some of the models that are currently in place. We need to do more in the private sector and in the government sector to help secure the infrastructure.

Thank you.

[The prepared statement of Mr. Rasch follows:]

TESTIMONY OF MARK D. RASCH
VICE PRESIDENT
GLOBAL INTEGRITY CORPORATION

BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

Oversight Hearings on Internet Security

Rayburn House Office Building, Room 2152

March 9, 2000
10:00 A.M

Good morning Chairman Horn, Representative Turner, and members of the Subcommittee. Thank you for inviting me to testify today on the important issue of Internet Security. My name is Mark Rasch, and I am a Vice President of Global Integrity Corporation, a wholly owned subsidiary of Science Applications International Corporation (SAIC) located in Reston, Virginia. Global Integrity works as an information security consulting company and resource for Fortune 100 companies, including online businesses, banks, brokerage houses, insurance companies, telecommunications and entertainment companies and other "dot com" industries. In this capacity, we test the overall computer security of our clients' sites, help them develop secure information architectures, and help them respond to attacks and incidents. We monitor and report to our clients about the most recent threats and vulnerabilities in cyberspace and help them cooperate with regulators and law enforcement agencies where required or where appropriate.

Before joining Global Integrity, I was a trial attorney with the Fraud Section of the Criminal Division of the United States Department of Justice, principally responsible for investigating and prosecuting all computer and high technology crimes, including the prosecution of the Robert Morris Cornell Computer "Worm," and investigations of the Hannover Hackers of Clifford Stoll's "Cuckoo's Egg" fame, and investigations of Kevin Mitnick, the recently released computer hacker from California. When I left the Department of Justice in 1991, I was the sole attorney in the computer crime unit -- and that was on a part-time basis. The Computer Crime and Intellectual Property Section of the Department of Justice today consists of 18 attorneys. In many ways, those were simpler times. The Internet consisted of perhaps 60,000 computers, and the World Wide Web had only begun to emerge as a force to be reckoned with. Moreover, while we were certainly dependent upon computers and computer technologies, electronic commerce was in its nascent stages. Today, it represents a multi-billion dollar industry.

As the Distributed Denial of Service attacks against Yahoo!, Amazon.com, e-Bay and e-Trade last month have made painfully clear, there are few rules in the electronic frontier, and information

security has, for many, been the step-child of electronic commerce. For America to remain competitive, and to foster the growth of electronic commerce, with its concomitant increases in productivity and convenience, protecting the critical electronic infrastructure is imperative. There are genuine threats to electronic commerce and to privacy and security of digital information, but none so significant that they should long deter or delay the growth of this wonderful technology. The same Internet that empowers a single individual to obtain a lower interest rate on a home mortgage by negotiating online empowers an individual hacker in a basement garage in Redmond, California to get information about a transaction in Houston, Texas, or to shut down a dot com business in Falls Church, Virginia. The Internet is no respecter of borders or of sovereignty.

Government in general, and the U.S. government in particular, has a legitimate interest, and therefore a legitimate role in encouraging the development of more secure, more robust, and more dependable computers and computer systems. However, government should not use the general insecurity about online commerce as an opportunity to take upon itself new powers of investigation, new powers to compel cooperation or reporting, or new opportunities to increase the regulatory burden on those doing e-business. The government can, though, do more to be a partner with the commercial sector and to promote trust and confidence in its abilities and its dedication to security.

The first question raised by the recent Distributed Denial of Service (dDOS) attacks is whether this means that e-commerce and the Internet are not secure. The answer is -- yes and no. The recent attacks have emphasized the inherent fragility of the public Internet that we have come to rely upon. The attacks themselves are not new, nor are the methods for perpetuating them. Yet it is important to emphasize the fact that none of the "affected" websites – Yahoo!, e*Trade, e-Bay or CNN -- were themselves "hacked." Nobody broke into these sites, nobody stole sensitive information from these sites, and nobody altered or damaged information resident on these sites. While there is some comfort to be found in these observations, the fact that a hacker or a few hackers, using a well known, and fairly well publicized methodology, could nonetheless cripple these sites (albeit for a short period of time) demonstrates the interdependence of those on the web, and the vulnerability of all netizens to such attacks. This becomes increasingly important, as the U.S. Census Department announced that U.S. retail E-commerce sales for the fourth quarter 1999 (October through December) was $5.3 billion.

The attacks also pointed out a crucial problem long overlooked by the designers of the Internet, and by those who use the net for commerce. The distributed nature of the Internet makes the security of any individual computer or computer system dependent upon the security of the Internet as a whole. While some sites, particularly financial services and e-commerce sites, have done a good job protecting their periphery – through the use of firewalls or other technologies – the denial of service attacks demonstrate the inherent interdependency of users on the net.

Moreover, the attacks raise a significant liability concern that potentially outweighs the concerns initially raised by the Year 2000 "bug." This is the concern about what can be termed "downstream liability." A computer user, or e-commerce site, negatively impacted by the actions of a hacker or other actor may seek to obtain compensation for the injury through litigation. In such a case, the "negligent" party would be the user on the network that failed to have adequate security to prevent or deter the harmful conduct. In much the same way as the owner of an automobile that leaves the

car with the ignition running in the middle of the night in Times Square might be held liable for the actions of joy riders that misuse the vehicle, the owner of a computer system or network that fails to provide a reasonable level of security, knowing the interconnected nature of the network, may be held liable for damages resulting from his or her negligence.

I believe that the reason we have not yet seen this type of litigation is the fact that we have not fully established an effective "standard of care" for computer networks, and the fact that the victims of computer crimes are reluctant to admit the fact that they have been victimized.

According to Department of Justice statistics, cyber crime *cases* have increased 43% from 1977 to 1999. Reports and analyses conducted by the Computer Security Institute, the FBI, the Computer Emergency Response Team, SANS, as well as Global Integrity Corporation's data confirm the increase of computer related incidents and cyber attacks. By incorporating and synthesizing all available data from government studies, private industry surveys, research/academic research, information security reports, law enforcement statistics, public data and media reports and, most importantly, the live data, intelligence, and incidents worked by GLOBAL INTEGRITY, we have identified the following trends in cyber attacks:

- Distributed attacks are increasing, specifically indicated by the activity in late 1999 through the events of last month.

- Compromising the same vulnerabilities in systems is the predominant method of attack. Attackers are using the known and publicized security holes to compromise systems.

- Most incidents and penetrations seem to be attacks of opportunity.

- The release of point and click tools (complete programs, scripts and virus recipes) has made the ability to hack very easy and accessible to everyone. The numbers of attacks and door knocking have reflected this increase in accessibility and ability. The attacks can be perpetuated by so called "script kiddies" who can download these tools, or by more sophisticated hackers who can create or modify these tools to be more malicious or more difficult to detect.

- Generally speaking, attack coding is more sophisticated and some of it has been very creative.

- There has been an increasing number and sophistication of attacks against Microsoft systems; UNIX based attacks are remaining the same.

- Media exposure appears to be the catalyst for many attacks and appears to correlate to web attacks and hacks. Organizations appearing prominently in the news, launching new advertising campaigns, announcing IPO status, or holding press conferences seem to attract penetration attempts, hacks, and web defacement.

- Those attacks perpetrated by an insider seem to be driven by an internal change within the organization. Management changes, an acquisition or merger, or a changed employment

policy (i.e., benefits, retirement, stock options) seemed to be the catalyst (or at least one of the major precursors) to an attack.

In general, all types of attacks increased to some degree during 1999. However, the greatest increases have been noted in theft of intellectual property, unauthorized insider access, insider abuse, and system penetration by an external party.

- Theft of Proprietary Information and Intellectual Property has increased 15% from 1998.
- Unauthorized Access by an Insider has increased 28% from 1998.
- Insider Abuse of Internet (i.e., e-trading, pornography, e-mail abuse) has increased 17% since 1998.
- System Penetration by External Parties has increased 32% from 1998.

The FBI indicated that virus damage in the first two quarters of 1999 exceeded $7 billion; the Melissa virus cost U.S. businesses $75 million. Virus reporting and denial of service reporting may have reflected a decrease in some surveys due to the fact that some denial of service attacks were caused by a virus. The attack categories are becoming less exclusive and exhaustive and more mutually inclusive. In addition to the above mentioned attack types, we have seen as many as ten different attack types:

- Theft of Intellectual Property;
- Sabotage to systems and networks;
- System Penetration by an external party;
- Insider Abuse;
- Financial Fraud;
- Denial of Service;
- Virus;
- Unauthorized Insider Use of systems;
- Web Attacks and Defacement; and
- Other.

In addition to the attack types directly on corporate systems and networks described above, a secondary type of attack has been occurring. Employees and external personnel have caused damage to companies by their postings and communication on the Internet and World Wide Web. Either originating from inside their workplace or from home, human communication on-line has increased the vulnerability of corporate information assets. Global Integrity has assessed the on-line threat to include seven major categories:

- the disclosure of client related information;
- overt threats to personnel or facilities;
- disclosure of stock pricing and stock manipulation;
- the disclosure of technical information about corporate system and network architecture;
- disclosure of intellectual property information and/ or research and developments secrets;
- trademark violations; and
- other.

We anticipate that the level of cyber attacks will continue to increase. As Mr. Pethia has pointed out, the CERT team at Carnegie Mellon University has seen a rapid increase in the number of reported incidents and attacks. A number of trends indicate why the problem of computer security generally, and Internet related security in particular, will continue to be a problem for businesses, individuals and government alike.

- Attack technologies are developing in an open-source environment and are evolving rapidly. Hackers are able to quickly and efficiently develop and distribute new software and new attack methodologies. These range from tools to exploit known vulnerabilities to sophisticated new techniques to guess or crack passwords, obtain unauthorized levels of access, or to simply deny access to computer resources. The tools are becoming easier to use and more efficient. Technology producers, system administrators, and users are improving their ability to react to emerging problems, but they are behind and significant damage to systems and infrastructure can occur before effective defenses can be implemented.

- Currently, there are tens of thousands – perhaps even millions – of systems with weak security connected to the Internet. Attackers are (and will) compromising these machines and building attack networks. Attack technology takes advantage of the power of the Internet to exploit its own weaknesses and overcome defenses. The systematic attacks on the e-commerce sites utilized vulnerabilities that were well known in the information security industry. However, unless ALL users on the web secured their computers, the exploits would be successful. Even if success is measured in terms of a small fraction of a percent, with millions of computers on the Internet, such a result could prove devastating.

- Increasingly complex software is being written by programmers who have no training in writing secure code and are working in organizations that sacrifice the safety of their clients for speed to market. This complex software is then being deployed in security-critical environments and applications, to the detriment of all users. Moreover, industry itself has not demanded that security be an essential component of new technologies. There is and has always been a perceived security/functionality trade-off. Working in Internet time, attempting to get goods to market quickly, software and hardware manufacturers are not pressured to increase security in the same manner that the marketplace creates competitive pressures toward functionality.

- User demand for new software features instead of safety, coupled with industry response to that demand, has resulted in software that is increasingly supportive of subversion, computer viruses, data theft, and other malicious acts.

- Because of the scope and variety of the Internet, changing any particular piece of technology usually cannot eliminate newly emerging problems; broad community action is required. While point solutions can help dampen the effects of attacks, robust solutions will come only with concentrated effort over several years.

- The explosion in use of the Internet is straining our scarce technical talent. The average level of system administrator technical competence has decreased dramatically in the last 5 years as non-technical people are pressed into service as system administrators. Additionally, there has been little organized support of higher education programs that can train and produce new scientists and educators with meaningful experience and expertise in this emerging discipline.

- The evolution of attack technology and the deployment of attack tools transcend geography and national boundaries. It has been suggested that some attack tools are developed and deployed by state-sponsored agents, although we have no reliable evidence to support this. Solutions must be international in scope.

- The difficulty of criminal investigation of cyber crime coupled with the complexity of international law mean that successful apprehension and prosecution of computer crime is unlikely, and thus little deterrent value is realized.

- The number of directly connected homes, schools, libraries and other venues without trained system administration and security staff is rapidly increasing. These "always-on, rarely-protected" systems allow attackers to continue to add new systems to their arsenal of captured weapons.

The major new trends in computer crime include:

- Increased "disappearance" of intellectual property for personal benefit to spin off a new company or business as well as to sell to a competitor or other interested buyer

- An increase in attacks from out of the U.S., particularly from Eastern Europe

- An increase in the use of social engineering to acquire intellectual property, proprietary information, and sensitive information from commercial industries

- An increase in attacks, due to the proliferation of on-line banking, which will lead to the compromise of personal and home systems. As the value of data on the home systems increase, so will the probability of attack. Those employees who work out of their homes on a personal or corporate system will become more vulnerable.

- An increase in coordinated and distributed DOS attacks

- A lowering of security standards and hiring standards, due to a shortage of IT professionals. Other security and HR standards such as criminal checks and background checks may be overlooked in order to hire quickly with the needed skill sets. If these vetting and screening procedures are not maintained, an increase in insider attacks will most likely occur.

- An increase in number and sophistication of self-mailing viruses as well as copycat or mutated viruses.

Adding to these problems are technical difficulties in detecting, locating and preventing these types of attacks. For example, through the use of Internet Protocol or "IP" spoofing, attackers can hide the identity of machines used to carry out an attack by falsifying the source address of the network communication. This makes it more difficult to identity the sources of attack traffic and sometimes shifts attention onto innocent third parties. Limiting the ability of an attacker to spoof IP source addresses will not stop attacks, but will dramatically shorten the time needed to trace an attack back to its origins. However, anonymity or pseudonimity promotes free and open discussions, particularly in repressive regimes such as Cuba, North Korea or the People's Republic of China, all of which limit access to the Internet. Indeed, the State Department's most recent report on human rights abuses lists limitation of or governmental monitoring of Internet use as a pervasive form of human rights violation in such nations. We must effectively balance the need for privacy with the need for accountability.

Computer systems are also vulnerable because malicious computer users can use multiple vulnerable computers as a launching point for attacks, effectively hiding their tracks and amplifying the seriousness of the attack. All affected sites must respond in concert, something that is difficult if not impossible to accomplish.

Many organizations do not respond to complaints of attacks originating from their sites or to attacks against their sites, or respond in a haphazard manner. One reason for this is the lack of any comprehensive definition of an "attack." Intrusion Detection Software (IDS) works by looking for patterns that may represent unusual activity, and therefore an attack. However, a company does not know whether or how to respond to each and every bad password, difficult log in, or malicious computer program. Most companies and government agencies lack effective computer emergency response plans. This makes containment and eradication of attacks difficult. Further, many organizations fail to share information about attacks, giving the attacker community the advantage of better intelligence sharing.

In addition, many computers are vulnerable attacks because of inadequate implementation of well-known "best practices." Hackers' tools frequently exploit well-known security vulnerabilities, which have not been fixed due to a lack of knowledge, commitment or resources by the host computer operator. When those computers are used in attacks, the carelessness of their owners is instantly converted to major costs, headaches, and embarrassment for the owners of computers being attacked. Furthermore, once a computer has been compromised, the data may be copied, altered or destroyed, programs changed, and the system disabled.

What the Private Sector Is Doing

There are several steps that can be, and to some extent are being, taken by the private sector to coordinate a response to computer security. I stress that none of these steps will eradicate the problem, and none are a panacea. The private sector is working to (1) share information about security vulnerabilities, threats and incident to more effectively coordinate responses; (2) develop and test new security technologies, including encryption, digital certificates, token based

authentication and biometric devices; (and (3) coordinate responses with appropriate law enforcement or other governmental agencies.

One of the concerns addressed in Presidential Decision Directive (PDD) 63 about the state of the critical infrastructure is the problem of information sharing in the private sector. This is of particular concern since the bulk of the nation's critical infrastructure – the computers and computer networks that make the nation run – are in the hands of the regulated private sector. The financial services, energy, transportation, and telecommunications industries are not owned by the government, but rather by the private sector. With deregulation and competition, information protection could be used as a competitive tool, allowing one company to keep secret tools for protecting itself, at the expense of the industry as a whole.

The FS/ISAC Model

In order to combat this problem, and to help promote an overall secure infrastructure, the financial services industry has been the first to create a formalized mechanism to share information about computer security threats, vulnerabilities and incidents between and among its members. The Financial Services Information Sharing and Analysis Center – FS/ISAC – formally launched on October 1, 1999, and hosted by Global Integrity, is a tool that permits its members to anonymously share information that could help protect the industry as a whole. Fears of publicity, fears of inviting additional attacks, fears of confidentiality, and fears of anti-trust liabilities have, in the past, limited the willingness of industry members to share information. Nobody wants it to be reported in the front page of "The Washington Post" that a bank or financial institution has been the victim of an attack or an attempted attack. The FSISAC provides a means for sharing information – and for distributing threat information obtained from government sources – without fear of attribution or publicity. Nothing contained in the FS/ISAC rules or regulations alters the obligations of banks or other financial institutions to report criminal activities to regulators or law enforcement agencies. Nothing contained in the ISAC regulations precludes or discourages reporting of incidents, except that information learned exclusively from the information provided in the ISAC database remains confidential unless disclosed by the source of that information.

The FS/ISAC represents a form of public-private cooperation that can be a model for the future. The Treasury Department and the SEC support but do not run the FS/ISAC – it is a separate entity with its own governing board made up of representatives of various financial institutions. The government may use the FS/ISAC as a means for disseminating information TO members of the financial services industry, but relies on traditional reporting requirements for obtaining information FROM the industry. It works to facilitate inter-corporate information sharing to help protect one of the critical infrastructures.

It is contemplated that the FS/ISAC model can be and will be utilized as a template for voluntary industry cooperation and information sharing in other industries. Only through voluntary cooperation can this model work. A similar vehicle for voluntary cooperation has existed in the telecommunications industry for many years. This entity, known as NSTAC – the National Secure Telecommunications Advisory Commission – that includes in its members, Science Applications International Corporation, Global Integrity's parent company, facilitates voluntary information sharing in the telecommunications industry. Mandatory reporting to government agencies of

security incidents or vulnerabilities will prove counter productive, as some will choose to report every "ping" or bad password use, and some will report only the most serious attacks.

In addition, the Banking Industry Technology Secretariat (BITS), which represents a consortium of financial institutions, has contracted with Global Integrity to test all manner of products which may be used in financial institutions to ensure that they meet a uniform set of security related criteria. It is presumed that such testing will assure a minimum level of security, and may establish a baseline against which companies may be measured.

Role of the Government

There are certain roles and functions that are and can be the province of the government. These include setting minimum standards for security and interoperability, conducting and supporting fundamental research on new security technologies -- particularly in the area of biometrics and smart card technologies -- promoting awareness of issues relating to information protection, ensuring greater international cooperation between law enforcement and other agencies, and bringing down barriers which inhibit such cooperation.

Setting of Standards

The government can and should set standards in cooperation with both Internet companies like Cisco, IBM and others, and telecommunications and software companies for security. These standards should both afford a reasonable degree of security and be attainable in a cost effective manner. Such standards should empower users to secure themselves, but should not be used as a "command and control" mechanism to force new regulatory burdens on users. In essence, the goal should be to standardize for interoperability AND security, and not to mandate a particular technology.

A. Research and Development

Computers and computer networks are inherently complicated. Moreover, it is always easier to tear down a building than it is to design and build it. The government has a legitimate role in funding and supporting basic and applied research in the area of information security. Let us not forget that the Internet itself was the outgrowth of basic research initiatives by the Department of Defense Advance Research Projects Agency. Such research funding should be across disciplines – not limited to computer sciences. Security depends not only on hardware and software, but also on policies, practices, and personnel. We need not only to understand the vulnerabilities of the infrastructure, but also to understand who exploits them and why.

B. Education and Training

Education and training is an essential component of information protection. No passwords, or poor passwords are the most common and cost efficient way to obtain unauthorized access to a computer or computer system. Users, administrators and other must be educated about the appropriate use and threats to computer systems. The bulk of this training should be done by companies educating

their employees about the need to be vigilant, and the government educating its employees and contractors about the need for security precautions.

In addition to user education, the government has a role in promoting the development of undergraduate and graduate level programs in information security. Global Integrity has established a mentoring program in this area with several universities, including Purdue University, and I have taught classes in information security at the George Washington University and a distance-learning program at James Madison University. The dearth of trained professionals, inside and outside of government may cause the private sector to unfortunately reach out – from sheer desperation or a misguided trust – to untrained individuals at best, or computer hackers themselves. Basic levels of competence, possibly including independent non-governmental certification programs will assist in ensuring that there is a cadre of trained information security professionals.

C. Technical Support

Many information security attacks are beyond the technical capabilities of any individual company, and no individual company should be required to bear the burden of fixing what are essentially societal problems. The government, in cooperation with private industry, can provide meaningful databases and technical support to assist.

D. Promoting New Security Technologies

A lesson should be learned from the recent debates over encryption. After almost ten years of debate, the government has finally liberalized the regulations concerning the use and export of commercial encryption software to the point where most companies now feel free to create and use such software to protect confidentiality, integrity and availability of information. However, the efforts to restrict the export of such software – while motivated by a legitimate desire to protect national security and promote the ability of law enforcement and intelligence agencies to lawfully intercept communications -- proved to be counterproductive, and had the unfortunate effect of making individual communications less secure. At present, the default for most companies and government agencies is to send electronic communications in an unencrypted and therefore insecure manner. For true information protection, the default should be seamless effective encryption.

E. Protecting the Government's Own Infrastructure

The government should also spend the resources necessary to protect and defend its own infrastructure – civilian and military. Most of the current administration's efforts reflected in its budget requests are geared toward this goal. For example, on February 15, 2000 the White House issued a press release indicating a proposal, reflected in the budget previously submitted for a 15% increase in the FY 2000 request for spending on critical infrastructure to reflect a total budget for such operations of $2.0 billion. The administration proposes spending $606 million for research and development. These expenditures are geared principally toward protecting the government's infrastructure, training those charged with protecting government systems, and establishing an early warning system to detect attempted penetration into the government's own computers.

What the Government SHOULD NOT do.

The government should not seize the publicity surrounding these incidents to take upon itself new powers of regulation or impose new burdens upon those operating on the web. Any such regulations would likely be ineffective, counter productive, and would impose a disproportionate compliance burden on U.S. companies.

The government must respect the fundamental rights of privacy – including a respect for the right of anononimity where appropriate. For political and social discourse to flourish on the web – in America and abroad -- governments must agree not to unduly burden the privacy rights of the electronic community.

The government should not use the legitimate threats to computer systems as a justification for increased monitoring or surveillance of its citizens or others. While much of the traffic on the Internet is "public" in the sense that the IP traffic is transmitted over insecure routers and servers, the government should not create a database of "normal" traffic patterns or surveille otherwise innocent Internet traffic.

Most importantly, the government should not rush to pass new laws or new regulations unless and until it is demonstrated that current legal regimes are both inadequate to solve the problems, and are not preserving other fundamental rights or liberties. We should not sacrifice liberty at the altar of security.

I thank the Committee for the opportunity to present my views, and welcome any questions the Committee may have.

Mark D. Rasch, Esq.
Vice President
Global Integrity Corporation
12100 Sunset Hills Road
Reston, Virginia 20190
(703) 375-2416 tel
(703) 375-2497 fax
Mark.Rasch@GlobalIntegrity.com
www.GlobalIntegrity.com

Mr. HORN. Thank you very much.

Our next witness and the last one on this panel is Mr. James Adams, chief executive officer of iDEFENSE.

Mr. ADAMS. Chairman Horn and members of the committee, I want to thank you very much for inviting me here today. Few revolutions are accomplished without bloodshed. Already as we plunge headlong into the knowledge age, we are beginning to receive the initial casualty reports from the front lines of the technology revolution.

From the headlines, you would think that the recent denial-of-service attacks were the beginning of the end of cyber world as we know it. Nothing could be further from the truth. These were mere in-breaks on the audio-V commerce. Consider instead that some 30 countries have aggressive, offensive information warfare programs. All of them have America firmly in their sights.

Consider too that if you buy a piece of hardware or software from several countries, among them, some of our allies, there is real concern that you will be buying doctored equipment. It will syphon copies of all material that passes across that hardware or software back to the country of manufacture.

The hacker today is not just the stereo-typical computer geek with a grudge against the world. The serious hacker today is much more likely to be in the employ of government, big business, or organized crime. Consider the band of Russian hackers who, over the past 2 years, have syphoned off an enormous amount of research and development secrets from United States corporate and government entities in an operation code named Moonlight Mays television.

I would like to focus on this nexus between the public and private sectors, and on the government's efforts to respond to the growing threat. A couple of illustrations to begin; 20 years ago, some 70 percent of all technology development was funded by the public sector. Today, that figure is under 5 percent. In other words, in the course of one generation, every government agency should have changed how it does business.

Has that happened? No. Looking ahead for that same 20-year period, we will see the following. The ordinary computer that you have on your desk will have the computing capacity of the human brain. At the same time, research offers the possibility of our ability to manufacture perfectly the human body. So, in the course of a generation, our view of life, death, family, society, and culture, the bed rocks of our way of life down this century will have changed forever.

Is government or the private sector thinking and planning for such fundamental change? No. One further point; the pace of the revolution is accelerating rapidly. Yet, the pace of change within government seems to be exactly the same today as it was 10 years ago. How has the government responded so far? Well, there has been the usual President's Commission and then the Principal's Working Group, then the bureaucratic compromise that nobody really wanted, and then the national plan which arrived 7 months late and was not a plan at all, but an invitation to further discussion.

[Chart shown.]

Mr. ADAMS. These two charts that I brought today illustrate the current chaos. What you see is a totally disorganized organization chart. One that, if it were in the private sector, would be a sign of eminent bankruptcy. You see no clear leadership. You see duplication of efforts; the waste of billions of dollars of taxpayers' money, and the struggle by stovepipe agencies to retain power, influence, and money.

In other words, there is no coherent strategy and the tactics are not about winning a war, but about preserving turf. There are, of course, some notable exceptions to this. You have heard from one of them today, John Tritak. What is needed today is an outside entity with real power to implement drastic change in the way government approaches technology and the underlying security of its systems.

What is needed most is a personal entity that would draw on skill sets in many areas that will overlap those of the CIO, CFO, or CSO, and most of the other officers or entities in any organization. Let us give this new person the title of chief of business assurance. He or she would be in charge of the Office of Business Assurance. Business assurance is more than security, more than technology, and more than a combination of the two.

It is an understanding of the whole environment and what that means for a business or a public sector operation. The CBA's task would be to continuously gather and synthesize infrastructure-related trends and events to intelligently evaluate the technological context within which the organization operates, to identify and assess potential threats, and then to suggest defense action.

Viewed from the positive side, to assess the technological revolutions' opportunities and propose effective offensive strategies. The Office of Business Assurance must be a totally independent organization with real teeth and real power within government. There is much in common between government and industry when it comes to the challenges and the opportunities that the technology revolution poses.

Both sectors face a common threat. Both sectors share common goals. Both employ technologies that are, in essence, identical. Both must work together to protect each other. I will leave you with this thought. You will employee total transformations of the way business and government is conducted internally and externally going forward. We have heard a great deal in recent months about the potential of a digital divide that is developing between the computer-haves and the computer-have-nots.

I believe there is another digital divide that is growing between the American Government and its citizens. If this committee's efforts do not move forward in changing this culture inertia, there is real danger that the digital divide that exist between the government and the private sector will only widen. We cannot afford a situation where the governed feel that their government is out of touch and increasingly irrelevant to their lives.

Thank you.

[The prepared statement of Mr. Adams follows:]

TESTIMONY OF JAMES ADAMS
CHIEF EXECUTIVE OFFICER
INFRASTRUCTURE DEFENSE, INC.

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY

COMMITTEE ON GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

MARCH 9, 2000

iDEFENSE
The Power of Intelligence

James Adams, CEO of iDEFENSE
Subcommittee on Government Management, Information, and Technology
March 9, 2000

Introduction

Chairman Horn, members of the committee, I want to thank you for inviting me today. I consider it an honor to share with you my perspective on the increasingly vital issue of developing a real solution to securing our computer, network and Internet systems.

At the outset, I want to commend Chairman Horn, and the committee, for its outstanding efforts to prod the government to develop a timely response to the Y2K issue. It was not lost on many in the private sector that it took a serious dose of public humiliation -- dished out in large measure by the Chairman -- to move the vast, inert bureaucracy to respond to a potentially lethal electronic threat.

Today, this committee is rightfully tackling a broader, and potentially much more threatening issue than Y2K, that of the overall computer security of the public and private sector. We are currently in the midst of a revolution, the Information Revolution, which calls for dramatic and bold steps in the area of securing cyberspace. The issue of computer security is vital to the health of the nation and this committee is taking a lead role in raising the right issues at the right time.

In fact, it is in the context of creating a comprehensive, proactive defense of our critical infrastructure that my company, iDEFENSE, was founded in 1998. iDEFENSE provides intelligence-driven products -- daily reports, consulting and certification – that allow clients to mitigate or avoid computer network, Internet and information asset attacks before they occur. As an example, iDEFENSE began warning its clients about the possibility of Distributed Denial of Service attacks back in October and November of last year.

The Revolution is Here

Few revolutions are accomplished without bloodshed. Already, as we plunge headlong and terribly ill-prepared into the Knowledge Age, we are beginning to receive the initial casualty reports from the front lines of the technology revolution and to witness first-hand the cyberthreats that, if allowed to fully mature, could cause horrendous damage to society.

The ongoing campaign of Denial of Service attacks include some of the household names of e-commerce — Microsoft, Yahoo, eBay, Amazon.com, CNN, ZDNet, and E*Trade. Comparative newcomer Buy.com was attacked on the day of its Initial Public Offering, and other smaller firms such as Datek Online Holdings Corp. experienced problems, which are probably related to the attacks. Targeted sites receive hits on their servers of up to one Gigabyte of data per second, and are unavailable to the general public for anywhere from 30 minutes to several hours.

From the headlines, you would think that these attacks suggested the end of the cyberworld as we know it. Nothing could be further from the truth. These were mere pinpricks on the body of e-commerce. Consider instead that some 30 countries have aggressive offensive Information Warfare programs and all of them have America firmly in their sights. Consider, to, that if you buy a piece of hardware or software from several countries, among them some of our allies, there is real concern that you will be buying doctored equipment that will siphon copies of all material that passes across that hardware or software back to the country of manufacture.

The hacker today isn't just the stereotypical computer geek with a grudge against the world because he can't get a date. And not every hack that is successfully pulled off is as sophomoric

as, say, a recent incident when the self-styled Masters of Downloading hacked into the official U.S. Senate Web site and replaced its front page with a message proclaiming "Screw You Guys."

The hacker today is much more likely to be in the employ of a government, of big business or organized crime. And the hackers of tomorrow will be all of that and the disenfranchised of the 21st century who will resort to the virtual space to commit acts of terrorism far more effective than anything we've seen from the Armalite or the Semtex bomb in the 20th century.

Consider the band of Russian hackers who, over the past two years, have siphoned off an enormous amount of research and development secrets from U.S. corporate and government entities in an operation codenamed Moonlight Maze by American intelligence. The value of this stolen information is in the tens of millions—perhaps hundreds of millions—of dollars; there's really no way to tell. The information was shipped over the Internet to Moscow for sale to the highest bidder.

Fortunately, this threat was detected by a U.S. government agency. Unfortunately, that information was not passed on to the private institutions that it might have helped. Among government and industry alike, an understanding of the critical infrastructure's threat environment is barely in its infancy.

All of these attacks, mistakes, and plain acts of God need to be studied very carefully. Because they define the threat front that is driving right through our very fragile economic, governmental, and corporate armor.

These are the kind of problems we—jointly, the public and private sectors—face in the technology revolution. So the big question is, who is going to solve these problems? The government? Private industry? Or the two working together? Or are the problems going to be solved at all?

Government Response?

How has government responded so far? Well, there has been the usual President's Commission, and then the Principal's Working Group, then the bureaucratic compromise that nobody really wanted and then the National Plan which arrived seven months late and wasn't a plan at all but an invitation to have more discussions. Meanwhile, the government in all its stateliness continues to move forward as if the Revolution is not happening. Seven months ago, my company won a major contract with a government agency to deliver urgently needed intelligence. The money was allocated, the paperwork done. Yet it remains mired in the bureaucratic hell from which apparently it cannot be extricated. Meanwhile that same government agency is under cyber attack each and every day. This is not a revolution. This is business as usual.

Another government agency is trying to revolutionize its procurement processes to keep up with the pace of the revolution. They are proudly talking about reducing procurement times down to under two years. In other words, by the time new equipment is in place, the revolution has already moved on eight Internet years. In my company, if I can't have a revolutionary new system in place within 90 days, I don't want it.

What this means to me is that the threat is growing rapidly, that a largely inert government has so far been unable to meet the challenge and that more must be done. And this does matter because there is more at stake here than simply whether a new computer works or does not,

whether a web site is hacked or not. At stake is the relationship between the governed and their government in a democracy. High stakes indeed.

Chief of Business Assurance

To fix the problems that afflict our body politic and our body corporate will require far more than Band-Aids. We're not talking casts and splints or even organ transplants. What we're talking about is leaving the old body and moving into a new one. We are talking—I am talking—about beginning to make changes in our cultural, political, and economic processes and institutions of such magnitude that they will dwarf even those that accompanied the industrial revolution.

What is needed is an outside entity – with real power – to implement drastic change in the way government approaches technology and the underlying security of its systems. Currently, jurisdictional wrangling, procurement problems and a slew of other issues are seriously hampering government's ability to stay current with the rapid pace of the Information Revolution.

What is needed most is a person or an entity that will draw on skill sets in many areas will overlap that of the CIO, CFO, CSO, and most of the other officers or entities. Let's give this new person the title of Chief of Business Assurance. Or perhaps the Office of Business Assurance to relate it directly to the federal government.

This new acronym should be the response to the current need. In some ways it is mirrored by the debate that started at the beginning of the Information Revolution that led to the appointment of Chief Information Officers in many companies and within government. But Business Assurance is more than security, more than technology, and more than a combination of the two. It is an understanding of the whole environment and what that means for a business or a public sector operation.

The OBA's task would be to continuously gather and synthesize infrastructure-related trends and events, to intelligently evaluate the technological context within which the organization operates, to identify and assess potential threats, and then to suggest defense action. Or, viewed from the positive side, to assess the technological revolution's opportunities and propose effective offensive strategies.

The Office of Business Assurance must be a totally independent organization, with real teeth and power within government. Those organizations that have the foresight to create and properly staff this position will be immeasurably better equipped to handle the tidal wave of change that is just now beginning to break over our government, industry, economy, and culture.

There is much in common between government and industry when it comes to the challenges—and the opportunities—that the technology revolution poses. Both sectors face a common threat that ranges from vandal hackers and hard-core criminals to foreign agents and natural disasters. Both sectors share common goals for the well being of America and her people. Both employ technologies that are in essence identical. And both must work together to protect each other.

My company, Infrastructure Defense, pioneers an approach to infrastructure protection that is aimed chiefly at the private sector. Many of the principles, however—value-chain analysis, for example, and threat analysis—are directly transferable to government organizations. The two sectors are not that far apart.

With common problems and common goals, there are opportunities for common solutions. One of the most important, I believe—one that is too new to have been embraced by either the private or public sector—is the need for every organization to incorporate a risk-mitigation

process. A second priority is to build a comprehensive information sharing system across all sectors on cyberthreats and countermeasures. We cannot afford to allow important information to grow stagnant within particular public or private entities. The rapid pace of technological

change necessitates a correspondingly robust response mechanism. I urge this Committee to champion this important issue as the federal response to the growing cyberthreat is constructed.

Conclusion

I leave you with this thought. You will see total transformations of the way business and government is conducted, internally and externally. A failure to change to meet these new challenges is to risk the destruction that all revolutions bring in their wake. Proactive action is the route to survival.

We have heard a great deal in recent months about the potential of a digital divide that is developing between the computer haves and the computer have nots. I believe there is another digital divide that is growing between the American government and its citizens. If this Committee's efforts do not move forward in changing the culture of inertia, there is real danger that the "digital divide" that exists between the government and the private sector will only widen. We cannot afford a situation where the governed feel that their government is out of touch and increasingly irrelevant to their lives.

Again, thank you for the honor of appearing before the Committee today.

Mr. HORN. Thank you. All three of you have made some really excellent suggestions. Let me start some of this query. Let me note that, Mr. Rasch, you were very active before you took your current job. You were a trial attorney with the Fraud Section of the Criminal Division of the U.S. Department of Justice. You left the Department in 1991. You were the sole attorney in the Computer Crime Unit. That was on a part-time basis.

The Computer Crime and Intellectual Property Section of the Department of Justice today consist of 18 attorneys. The Internet consisted of perhaps 60,000 computers. Then you have made some very thoughtful things. Let me pursue this. I turned to Mr. Ryan, the counsel to the subcommittee, when you were testifying. I said, let us draft a bill that would make this simply illegal.

Now, how does the Justice Department, what does it use to be able to get after hackers now? What laws? Do you need new legislation which would ban them and get those out of here?

Mr. Rasch, the principal statute that exist to prosecute Federal computer crimes is 18 U.S.C. Section 1030, which is the Federal computer crimes statute. That focuses on activities. For example, intentionally accessing a computer without authorization or disrupting authorized access to a computer. So, for example, the recent attacks and the denial-of-service attacks squarely come within the ambit of that statute and are being aggressively investigated and could be prosecuted under that.

Mr. HORN. Is there any first amendment concerns on this?

Mr. RASCH. Probably not. This is action and not speech. Although just as burning down a building may be an expression, it is certainly is not a protected expression. There are some first amendment concerns in the area of encryption and some legislation. There is some case law on the question of whether or not software itself acts as a form of expression. That relates to these type of hacker tools.

The dissemination of hacker tools themselves; whether or not that type of dissemination is criminal. There are really two separate statutes that could be used there. One is the Digital Millennium Copyright Act which passed last year, which is right now being used in a civil lawsuit against the people who attempted to reverse-engineer the DVD codes to allow them to pirate software and things like that.

So far, it has withstood a challenge on Constitutional grounds. The second one would be 18 U.S.C. Section 1029 which makes it illegal to disseminate what are called access devices, which could be such things as passwords and things like that.

Mr. HORN. Any comments on those?

Mr. ADAMS. I think you raise an interesting, Chairman. I would just make this in addition to what Mark was saying. There has been a great deal of focus on law enforcement. Of course, law enforcement has a prominent role to play in this. The speed of the revolution is such that, that is very much after the fact, obviously. An event has occurred. We failed and therefore we have to do something about it.

By the time somebody is caught and prosecuted, the revolution has moved several steps forward. So, we need to think about what does the prevention look like in the globally virtual environment in

which we find ourselves. Then if that fails, of course you need something to follow that up. The first step has to be a much more comprehensive approach to prevention, warning, intentions, good intelligence, and so on.

Mr. HORN. At this point, I am going to turn the Chair over to the vice chairwoman, Mrs. Biggert, the gentle woman from Illinois. I, unfortunately, have other commitments that I have got to do. I want Mr. Turner and Mrs. Biggert to get all of the questions out that they can. So, thank you particularly for functioning and coming here.

Mrs. BIGGERT [presiding]. Mr. Turner, you are recognized for questions.

Mr. TURNER. Mr. Adams, you were showing us your two charts here, which I guess were designed to display the multitude of efforts within various Federal agencies to deal with information system security. Rather than look at that as a failed effort, I guess it shows that every agency is struggling to try to keep up with the problem.

There are obviously some things that we ought to do to consolidate the effort. This battle is so dependent upon technical expertise. One of the battlefields where we should be fighting on is to figure out how to train people to work for the good guys. There are probably people within these Federal agencies that are noted to be outstanding technical experts that do good work in trying to find solutions and trying to make the systems secure.

Are we going to be constantly behind the curve in terms of what government does? I think it is probably difficult to attract the best and the brightest to the public sector. I am sure that Global Integrity and others of the world are going to be reaching out and trying to pay the salaries necessary to attract the people who could really create the defensive mechanisms you need.

Mr. ADAMS. I think those are very good points. We clearly face a very difficult dilemma. The government is at the front line here, as is the private sector. The private sector, my largest number of recruits come from government agencies. The private sector is hiring the best and the brightest and moving forward very quickly. Clearly, there needs to be a relationship between the public and private sector. Look, for example, at what the CIA is doing to try and keep itself up to speed with the pace of technology change.

It is doing that by establishing essentially a venture capital arm that is the interface between the public and private sector. So, you have that on the one hand; different ways of doing it. On the other hand, something that the Federal Government can do dramatically different is push education into the system, so that what we are doing is seeding the next generation and the generation after that to keep itself up to speed.

The Federal Government is going to be an enabler. It is not going to be able to mandate very much. This revolution is occurring outside of its orbit. So, it can do a lot of things to influence it. It needs to, I think, do that more creatively so that it is seeding the population. We have tremendous shortages of skills at the moment in the whole area of computers, and computer security, information security, and so on.

So, how to tackle that more creatively and aggressively is going to be a very important issue which is partly where it all comes back to leadership. You need to have a more creative and push-through process than we have at the moment.

Mr. TURNER. If you were to have a free hand at creating an entity that would do that, what would it look like?

Mr. ADAMS. Well, I think what the lesson we have learned in this revolution from the private sector is that if you take an old economy company and you try and transition it to the new economy, this will largely fail. What you have to do is do the Apple Computer model. You setup a new building, different people, and put a pirate flag on the roof. They developed a culture and they forced something else into the system, which is why this idea of a Business Assurance, some sort of entity that sits outside of the Federal Government that is able to communicate effectively with the private sector and with the public sector and force through change.

What those charts illustrate is, as you rightly say, lots of people try to fix it. These are people of good will, by and large. They are unable to move collectively aggressively enough. They are falling further and further behind in the revolution, which is this disconnect. It is very dangerous in a democracy. So, if you can have a way of driving through change, something with real power, the Koskinen model, but with muscle, not just please will you all sit around the table.

If you do not do this, you will be held accountable for failure. That is something where there is an opportunity perhaps because it is the private sector that has the expertise and the energy. That is going to continue to be the case. That is just going to be a fact of life. So, much better to try and figure out a way to bridge that gulf, rather than say, well, we can actually fix it all ourselves. It is all about a partnership between the private and the public sector, making that work and then driving it into the public sector.

That is the trick for you all to try and come up with a way of creating something very muscular that will force change, rather than saying, well, let us get around to it in another couple of years. Too late.

Mr. TURNER. Although we obviously have to let the CIA do their own thing, would that kind of model work for the rest of government?

Mr. ADAMS. I think it is too early to say at the agency. Clearly, what we know is that they are bringing some interesting technology back into the system. The problem comes then is this is a voluntary exercise. We found this really cool stuff. We think you should use it. Can the culture be forced to change? The CIA is a very inert bureaucracy like a lot of government agencies. Will that drive it through?

I think it is an interesting model in creating the place for dialog, but it is a difficult challenge. For example, there is a government agency that is currently revising its ways of procuring things, trying to keep on the front of technology. It feels that it is making a big step forward by doing changes in 2 years; design and implementation in a couple of years. My company is not into design and implementation in 90 days. I cannot afford to do it because I am losing market share.

So, how do you change that culture to a place which is much more reflective of what is happening in the private sector? It is a very difficult challenge. It has to, I think, have somebody. You are talking about very big picture stuff here; billions, and billions, and billions of dollars, where you have a single entity that says you do this my way or it is not going to happen; so forcing it.

This is very counter-culture to the way governments traditionally work. One of the great strengths of democracy and the great strength of government entities is that they slowly evolve. They move forward to match a pace. Well, in a revolution that is very hard because you cannot afford to evolve in the same way. You have to either become a revolutionary or you get swept away. We have seen examples of that throughout history.

That is why this is both a dangerous and a very challenging time; dangerous because it can threaten the institutions that provide stability, but a tremendous opportunity for America as the leading Nation in the world to move with the revolution, embrace it, and drive it forward. The government and the private sector have to come together somehow to make that so.

Mr. TURNER. Thank you.

Mrs. BIGGERT. Thank you. Mr. Gerretson and probably Mr. Rasch, how vulnerable are home computer users? You mentioned that the whole Internet is only as secure as the most vulnerable link. Then after that, if after they surf the web and turn off their modems, are there still risks to the system?

Mr. GERRETSON. I will take the first shot at that. The first answer is if you are on a dial-up modem, you are vulnerable while you are connected. Cable modems and DSL are widely becoming available now. They are always on. I run a private network at my house. I have a firewall. Every night I have probably six to eight of what I call drive by shootings where somebody comes and just tries out my system to see if they can get a hold of it.

The answer is they are very vulnerable. There is very little protection on them because it sits on there. Without that firewall, I probably would have been one of what they call the zombie machines attacking Yahoo and would have never known it. As the cable modems and the DSLs get more and more ubiquitously available, it is a huge problem.

Mr. RASCH. I would mirror that. We did a study at Global where we left a cable modem on at a home PC and simply tested it to see how many times, without a firewall deliberately, to test to see how many times it was attempted to be attacked. We found that in 1 month, almost 6,000 attempted attacks on a home PC.

What was interesting about that study, however, was the fact that these attacks were coming from Eastern Europe, from Africa, from Asia, as well as from the United States. So, these are coordinated concerted attacks on any computer that they can find on the Internet. That would include home PCs in the always-on mode; particularly, those on DSL connections or cable models.

Mrs. BIGGERT. So, in theory, these really then could lead you into, let us say, a Federal agency through those computers?

Mr. RASCH. Absolutely.

Mr. GERRETSON. That is right.

Mrs. BIGGERT. OK. Then we talked in the first hearing about this chart with the yellow bubbles at the top and sides representing the executive branch, and then those organizations that also have a stake-hold in the Federal computer security.

[The information referred to follows:]

Computer Security Management Key Players
All Executive Branch Agencies
National Institute of Standards and Technology (Commerce Dept.)
Chief Information Officers (CIO) Council
Critical Infrastructure Assurance Office (Commerce Dept.)
National Infrastructure Protection Center (Justice Dept.)
National Security Council
Office of Management and Budget
Department of Defense
General Services Administration
National Security Agency
Congress
Carnegie Mellon
Private Sector
State and Local Governments
Trade Associations
WHO IS COORDINATING COMPUTER SECURITY EFFORTS?

Mrs. BIGGERT. So, to me, it looks very similar to your chart, Mr. Adams. The problem is that we have kind of a blank in the middle. So, would you all agree that we need an outside coordinator to be in control of this to coordinate all of our efforts?

Mr. GERRETSON. Well, ma'am, I would say that my first question when I saw this chart and I was talking to Mr. Ryan about this is, who is coordinating the coordinators? It seems to be somewhat disorganized. I would like to make one little statement about that. The one advantage that the Federal Government has is that they know they are screwed up. We do a lot of commercial work.

If you get outside of the IA Groups, they do not even know they are in trouble. So, yes, you are lagging behind, in some cases, but, at least you know you are lagging behind. That is kind of contrary in view, but there are advantages to what you are doing. This is a problem.

Mr. RASCH. What I see as the problem is a definition of function. What we really need somebody to do is to say, not so much just coordinate the efforts, but say, alright, testing. That is NIST. For developing new technologies, that is somebody else. Basically, not so much coordinating, but defining who has what roles. One of the things that happened with the development of the Computer Emergency Response Team at Carnegie Mellon, the CERT Team, it was a wonderful idea, and remains a wonderful idea, and works very well.

Now, we have dozens, and dozens, and dozens of computer emergency response teams. The problem with that is it is like living in a town that has 20 different 911 numbers. So, you run into a problem of who are you going to call. So, you need to really define the functions first and then decide who is going to coordinate between and among those functions.

Mrs. BIGGERT. This has been very interesting. Obviously, you have heard the bells. We have another vote. So, I think that we will have to adjourn at this time. We will be having several more hearings. I know that we will be pursuing this more in-depth. I agree with you that we are behind and we need to look at this problem. I think that this has been a great start for this committee. So, I really appreciate you all participating and look forward to asking more questions of you, I am sure, in the future when we get into this.

So, without more, this committee hearing is adjourned.

[Whereupon, at 12:05 p.m., the subcommittee was adjourned.]

○