
INFORMATION SECURITY
IS YOUR SYSTEM SAFE?

The Airport "Jester"

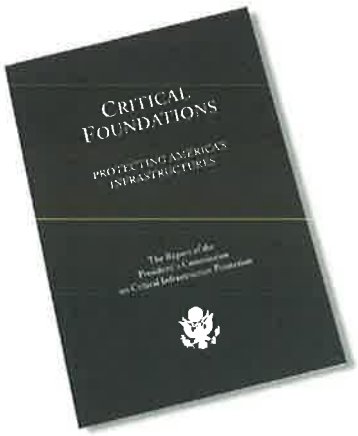
On March 10th, 1997, a teenage boy known as "Jester" used his home computer, a modem, and self-taught hacking skills to infiltrate the local telephone company's switching network at the airport in Worcester, Massachusetts. His subsequent mischief caused a system crash that knocked out telecommunications for six hours, disrupting communications to and from the airport control tower. Fortunately, no accidents resulted, and the airport quickly returned to normal activity.

During the ensuing investigation, airport officials discovered that the boy had little trouble infiltrating the switching system due to a lack of password-protection. The boy pled guilty to Federal hacking charges, the first ever levied against a juvenile.[1] The case highlighted the growing importance of computer network security and triggered a vigorous response from the Department of Justice. Prosecutors, determined to take a hard line on the case, vowed to pursue other hackers who disrupt important computer systems, especially those controlling the Nation's infrastructure. "These are not pranks. This is not like throwing spitballs at your teacher," U.S. Attorney David Stern said, "Hackers should know that they will be caught and they will be prosecuted." [2]

As Federal law enforcement officials pursue criminals like "Jester," they will be following a Presidential Decision Directive, known as PDD-63, that outlines a new mandate to protect the Nation's infrastructure. While the Constitution framed the Federal government's responsibility for national security as a matter of border defense, the ensuing 200 years have seen a great diversification in security concerns. The Federal government now monitors a host of threats that may adversely affect the Nation's economic well-being, its transportation system, and the personal safety of its citizens. For example, certain genetic sequences and pathogens, capable of forming the base of biological weapons, are now regulated by the Federal government as a matter of national security. To the evolving list of security concerns, the President recently added the Nation's computerized infrastructure – the computers, mainframes, and networks that control everything from traffic lights to defense systems. His concern is justified. Already, hackers have temporarily disabled over 100 U.S. defense systems, and executed thefts estimated at over $10 billion. Almost every single Fortune 500 company has suffered electronic intrusions. National security officials are most concerned about the potential of an "electronic Pearl Harbor," in which terrorists first disrupt utilities and emergency response systems, and then detonate a bomb or chemical agent. In February of 1998, the Department of Defense was besieged with hacker attacks as the result of an apparent hacker contest. One of the main offenders, an 18 year-old Israeli student known as "the Analyzer" claims to have gained entry into 400 U.S. government computer systems, including some at the Pentagon.

To minimize vulnerabilities and counter threats like the incident at the Worcester Airport, the Federal Aviation Administration (FAA) has initiated a variety of efforts to safeguard its air traffic control systems from unlawful entry. The FAA enlisted the Volpe Center to perform risk and vulnerability assessments on its network, and to develop security plans and procedures for these systems. The Center's Infrastructure Protection and Operations Division performs these assessments using a "systems approach" that evaluates data

[1] *ils.unc.edi/~allij/security/litreview.html*
[2] *www.wired.com/new/print_version/politics/story/1103.html*



sensitivity, potential threats, vulnerabilities, and existing countermeasures; these assessments generally produce recommendations identifying cost-effective safeguards. Illustrating this type of evaluation, the Division has performed a preliminary security assessment of over one hundred air traffic subsystems for the FAA's Air Traffic Services. The assessment provides guidelines for future in-depth analyses and security risk assessments of the top-ranked National Airspace System (NAS) subsystems. It has been used as one of the major inputs to the FAA's response to PDD-63.

Since producing this groundbreaking assessment, the Center has contributed to numerous information security projects throughout the Department of Transportation. By evaluating and designing information security systems, the Center assists agencies in protecting high priority systems from life-threatening shutdowns at the hands of "information terrorists."

The Problem

What is this new threat of "Cyber-Terrorism"?

As the power and versatility of computers have increased, information technology has become an integral part of the Nation's infrastructure. Traffic lights, train signals, power grids, and telephone networks are all, to varying degrees, controlled by computers. As the Federal government pursues advancements in rail travel and intelligent transportation systems, our physical infrastructure will increasingly rely on "virtual" information networks. This interconnection will facilitate more efficient transportation, but it also exposes the infrastructure to potentially dangerous vulnerabilities. The interconnection of computer networks makes it increasingly difficult to develop comprehensive security systems. Security experts must guard not just one single entry point, but must secure a multitude of interconnections.

In order to protect these connections, information security experts such as those at the Volpe Center evaluate four categories of vulnerabilities that may be exploited to infiltrate or disrupt a network. *Technical* vulnerabilities are a result of weaknesses in the hardware, software, and communication components of automated information systems. These weaknesses may include inadequate access controls, outdated virus detection programs, or unrestricted remote system access. *Operational* vulnerabilities are procedural weaknesses that may unintentionally facilitate or exacerbate security breaches. These deficiencies include lax security enforcement, a failure to detect unauthorized access, a lack of system backup, or nonexistent contingency plans. *Administrative* vulnerabilities are flaws in information security policies, such as insufficient security coordination between systems, or a lack of security policies altogether. These weaknesses often extend across all information systems within a particular organization. Insufficient security around the computer and network components causes physical vulnerabilities, represented by a lack of physical access controls or intrusion detection. Lax environmental controls such as inadequate or inappropriate fire suppression, or lack of backup power, are also included in the physical vulnerabilities category.

While information security specialists find and correct these vulnerabilities, legions of hackers scramble to beat them to the punch. The diversity of these cyber-criminals is astounding. They may range from the young, mischievous "Jester," to organized groups of terrorists or criminals intent on wreaking havoc. To complicate matters, these cyber-criminals all have different motivations for invading networks. Once they are inside, their intentions range from theft and espionage to protest and terrorism. The least threatening may be those who hack into systems as a means of testing their own abilities, although even interlopers such as "Jester" may inadvertently cause serious disruptions. Disgruntled employees may use

their knowledge of a corporate system to alter data or steal information. Foreign operatives may attempt to access various Federal information systems to extract information. There are even protest groups that write computer programs designed to shut down government Internet sites by bombarding them with electronic mail. For example, protesters of NATO's military actions against Serbian forces in Kosovo recently besieged the organization's website. Once they have gained access to the system, hackers are capable of causing extensive damage. They can reprogram access codes, interfere with system controls, and even create "back doors" that may provide a means for repeated infiltration.

Frighteningly, the techniques and methods used by many of these hackers are freely available and traded on the Internet. Now, those less computer-savvy can accomplish hacking feats that previously would have required extensive experience. Their collaboration is not only web-based. This summer will mark the seventh annual DefCon conference in Las Vegas, where hackers from the world over will congregate for a weekend to share ideas and strategies in person.

Failure to provide adequate security against these hackers may present an opportunity for disaster. In California, a hacker recently broke into the computer system that manages the Oroville Reservoir, a huge lake in the hills outside of the Sacramento Valley. Fortunately this interloper did not open the floodgates, an action that could have resulted in thousands of casualties and millions of dollars of damage.

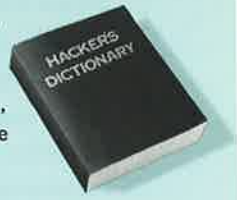
The diverse ownership and operation of the information infrastructure hinders comprehensive evaluation of the potential for such disasters. Many networks are owned by private entities, each of which uses a separate system with different weaknesses and capabilities. For example, the globalization of transportation and logistics, which is becoming the norm in the United States, will depend on both public and private networks. While individual transportation operators may practice good security, the security of the "system of systems" is only as good as the weakest link.

The diversity of systems and the demand for security has led to a growth in the number of information security specialists who develop networks designed to be impenetrable to would-be intruders. While the technology for this type of defense exists, it requires a vast array of specialized knowledge to institute it effectively.

the techniques and methods used by many of these hackers are freely available and traded on the Internet

A Hacker's Dictionary

Back Door – A hidden program, left behind by an intruder or disgruntled employee, which allows future access to a victim computer.



Bastion host – A server that is steeled for attack and can therefore be used outside the firewall. Subject to attack, bastion hosts are often sacrificial.

Logic Bomb – A program or code designed to cause a system crash.

Phreaking – Illegal manipulation of the telephone system.

Spoofing – Any procedure that involves impersonating another user or computer to gain unauthorized access to the target computer.

Sniffer – A program that surreptitiously captures message packets that cross a network. It can be used legitimately by an engineer to troubleshoot the network or illegitimately by a hacker looking to steal user ID's or passwords.

Time Bomb – Any program that waits for a specified time or event to disable a machine or otherwise cause that machine or system to fail.

Trojan horse – An application that secretly performs unauthorized tasks that endanger the system unknown to the user.

Denial of Service – A condition that results when a hacker maliciously renders a network server inoperable, thereby denying computer service to legitimate users.

Flooding – A tool that overflows the network connection queue, thereby causing denial of service.

Dedicated Federal Response

Numerous security breaches and the potential for serious incidents have brought information security to the urgent attention of the highest levels of the government. Acknowledging the American infrastructure's reliance on computer systems, President Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP), chaired by Gen. Robert Marsh (ret.), to "study the critical infrastructures that constitute the life support systems of the Nation, determine the vulnerabilities, and propose a strategy for protecting them into the future."

Leading the study of the transportation infrastructure were Dr. William Harris

and Mr. Thomas Falvey. The Volpe Center supported Commissioners Falvey and Harris throughout their evaluation of the Nation's transportation systems. The Center conducted a high-level assessment of the FAA's evolving National Airspace System; this assessment was instrumental to the Commission's findings. In October of 1997, the PCCIP submitted its final report entitled "Critical Foundations: Protecting America's Infrastructures." While the Commission discovered no immediate threat to national security, it was alarmed by the relaxed state of security measures guarding the Nation's infrastructure. In particular, the Commission found that transportation systems are a favorite target of terrorism internationally. It noted that the developing National Airspace System, which uses open systems with a multitude of communication networks, will be increasingly susceptible to cyber-attacks if adequate security measures are not taken. Because so many components of the information infrastructure are privately owned and operated, the report stressed the importance of cooperation between the private and public sectors. Specific recommendations included promoting industrial information exchange, reconfiguring laws salient to information security, and increasing government-sponsored research and development aimed at defending our computer-based infrastructure. The report's recommended "national organization structure" outlined responsibility and methods for achieving these recommendations.

> *"We already are seeing the first wave of deliberate cyber attacks, and the potential for harm is clear. We have to be ready for adversaries to launch attacks that could paralyze utilities and services across entire regions."*
>
> President Clinton

A major outcome of the report was the creation of the National Infrastructure Protection Center, a collaboration of the Federal Bureau of Investigation, the Department of Defense, the Central Intelligence Agency, the National Security Agency, the Department of Transportation, the Department of Energy, the Secret Service, and private sector experts. The Center seeks to assess information security risks to the national infrastructure and develop responses to these risks.

As a direct result of the Critical Foundations report, President Clinton issued Presidential Decision Directive-63 in May 1998, outlining a 180-day deadline for all cabinet-level agencies to develop plans for protecting critical information systems from disruption. In response to this directive, the Department of Transportation issued a plan directing each operating administration to develop remediation plans for their critical information systems. The FAA, with assistance from the Volpe Center, has developed a plan to ensure the security of the National Airspace System, mission support systems and aviation safety systems. Other Federal agencies have issued similar plans, and the effort to secure the Nation's information infrastructure will be funded by $1.46 billion in the FY 2000 budget.

In January of 1999, President Clinton again stressed the importance of information security. He emphasized that "cyber-terrorism" is no longer a distant threat. "We already are seeing the first wave of deliberate cyber attacks, and the potential for harm is clear. We have to be ready for adversaries to launch attacks that could paralyze utilities and services across entire regions."

Even before the President issued his Directive, the Volpe Center had played important roles in information security. Recently, the Center supported initiatives to ensure the security of both the modernized National Airspace System, as well as the many existing "legacy" systems and networks. In January 1998, the Volpe Center assembled inputs for the FAA for the development of a telecommunications security risk management plan. This work, prepared in support of the Office of NAS Operations identifies the security controls, processes, and procedures that are needed in order to implement an effective telecommunications security risk management program. This approach is currently being used by several FAA Lines of Business in conducting risk assessments.

For the PCCIP, the Center reviewed the potential vulnerabilities of the transportation infrastructure and produced a general report that addressed supervisory control and data acquisition (SCADA) systems for pipelines, and positive train separation systems for rail. These studies found that even closed systems, such as SCADA, may be vulnerable to an "insider attack" which could disrupt operations significantly.

The Center's past project experience combined with its researchers' familiarity with transportation systems cement the Volpe Center's position as a key resource in transportation system information security. Experts at the Center have detailed knowledge of both the physical components of transportation infrastructure and the "virtual" information systems that manage this infrastructure.

To keep researchers current, the Volpe Center constantly brings in industry experts to provide state-of-the-art training in information systems security. Last December, experts from the Management Information Security Training Institute presented a one-day seminar to Volpe Center researchers on the latest trends in information systems security. The seminar covered technical information on security topics, hacking trends, law enforcement responses, and new statutes and regulations requiring management to address information systems security, including the new Federal mandates in PDD-63.

The Center is also a multidisciplinary environment where communication across fields is a key component of advancements in transportation. The Volpe Center can act as an important facilitator of transportation and security industry groups such as the Information Systems Security Association and the High Technology Crime Investigation Association, bringing diverse parties together to share knowledge and strategies. For example, the Center hosted a conference entitled "Cyber Incidents: Bridging the Gap between Law Enforcement and Private Industry." This January 1999 forum featured private sector information security experts, law enforcement agencies, and Department of Transportation computer applications experts, all hoping to improve their methods to counter information invasion.

The Center also provides specific consulting and support services to agencies concerned with the security of their systems.

Volpe Center Information Security Managers and Experts:

Volpe's Director of the Office of Safety and Security
Robert C. Ricci

His responsibilities include the management of the Volpe Center's programs in support of the Federal Rail Administration in rail track systems research, structures and dynamics and the National Highway Traffic Safety Administration in crash-worthiness, biomechanics, and crash avoidance programs. He is also responsible for the Volpe Center's activities in the area of Information Security. For the past 29 years Mr. Ricci has worked at the Volpe Center in various managerial positions in computer simulation, engineering analyses, and computer technology. He started his career in spacecraft design at the NASA Electronics Research Center in Massachusetts, and in computer research, at RCA Labs in New Jersey. Mr. Ricci was an Alfred P. Sloan Fellow at MIT's Sloan School of Management.

Volpe's Director of Infrastructure Protection and Operations Division
Michael G. Dinning

Mike Dinning directs most of the Volpe Center's work in transportation systems security. The Center's projects include developing information security plans, policies, assessments and remediation designs for major transportation systems. Mike's division is also active in implementing physical security systems for critical government facilities. Mike has been at the Volpe Center for over 20 years, managing a wide variety of innovative technology programs. He works closely with industry to deploy the results of the Volpe Center's research, and is active in industry associations such as the Intelligent Transportation Society of America and the Smart Card Forum.

Volpe's Information Security Program Manager
Kevin Harnett

Kevin Harnett's 19-year career at the Center displays the breadth of his expertise. He has experience as a Computer Specialist and Program Manager in support of a wide range of strategic planning, system development, and system architecture projects for the FAA, Coast Guard, and DoD.

continued on page 17

The Center's "systems approach" leverages existing resources (experts and contractors) to solve new problems, while offering experienced, behind-the-scenes support to clients. This approach is a risk management procedure applied throughout the system's lifecycle, from the requirement analysis through development and operation. The Center examines both the virtual and physical risks involved with each step. At each step of analysis, implementation, and management, the Volpe Center draws knowledge from its experts in different fields and applies them, creating organization-wide security coordination on all projects. Historically, many security programs have been installed only after a computer system was designed. Where appropriate, the Volpe Center has encouraged clients to address security features during the initial planning and development phase, allowing a comprehensive integration of the security measures and the overall system.

The Center tailors this approach to the particular requirements of each system based on considerations of the system's "Information Valuation." (Assets applicable to the mission are assessed in terms of their "sensitivity" impact to the integrity, availability, and confidentiality of the information they process). The confidentiality of the system is a function of the consequences of disclosure of the system's contents. For example, confidential medical records and Social Security numbers are not made available to the general public. Meanwhile, the reliance of an organization on its system influences issues of integrity. A security system must consider the degree to which manipulation or deletion of data would harm the organization. For example, changing information used to calculate algorithms could be devastating to system users. Security systems must also address different levels of availability. Some types of information, such as tactical aircraft communications, are very "time critical," and must be made available to the authorized parties without delay. Other types of information, such as strategic weather information, require just as much confidentiality, but are not as sensitive to delays in access.

The Center's work goes beyond merely securing networks and now includes planning for computer emergencies that may be unavoidable. It is not enough to merely protect; agencies must now be prepared for infiltration and system failures. The FAA's Computer Security Incident Response Capability (CSIRC) is analogous to an emergency room, ready to combat attacks against the FAA's critical communications infrastructure. The Volpe Center is helping the FAA develop the plan and requirements for a CSIRC that will protect the infrastructure from intrusions and unauthorized activities, manage incidents that do occur, and provide disaster recovery. The Center is developing a training plan, incident reporting and management procedures, a program plan, and a concept of operations. These strategies are all focused on preparing for many different types of information security incidents and emergencies.

Information security is also a key issue in modes of transportation other than aviation. The development of Intelligent Transportation Systems (ITS) will result in increasing reliance of transportation systems on information technology. The Volpe Center is a key contributor to the planning and development of ITS systems and will be positioned to design the security measures for these systems. The Center has already assessed the potential vulnerabilities of evolving ITS systems and has recommended that a systems approach to security is needed for developing such services. Since ITS systems are developed and operated by a variety of public and private organizations, maintaining their security may prove as complex as securing the FAA's systems.

The Center remains active in physical security initiatives as well, working for such sponsors as the Department of State, Department of Defense, and the Treasury Department to assess and upgrade their facilities. These projects keep the Volpe Center up-to-date and well versed in current physical security trends and tools, enabling the Center to bring the best technologies and approaches to the transportation community.

Defending the Nest

Over the past thirty years, America has built into its surroundings interconnected computerized networks that promote increased safety, mobility, and efficiency. Unfortunately, our dependence on these networks leaves us vulnerable to the wolf-like hackers who seek to blow down the house. If they succeed, we may be left stranded, unable to protect ourselves, reach our destinations, and communicate with each other. While these hackers will continue to assault the Nation's infrastructure, stronger security measures will prevent any easy victories. As experts from diverse fields collaborate, the defense systems they develop will become increasingly resistant to attack.

The Security Arms Race

Like all security systems, information security has developed in response to attacks, and recently the attacks have become more sophisticated in an effort to bypass these security barriers.

1-Normal Routine:

Every computer on a network has its own address. Network communications are established between two computers when the first computer sends a request to a second computer and the second computer acknowledges the request by responding to the address provided by the first computer. This process is known as a handshake. Once the handshake takes place, the computers can communicate.

2-Security Action:

An early safeguard to control hacker attacks was to limit communications to specified computers with a filter, thereby shutting out the hacker.

3-Hacker Advance:

To counter the filter, hackers created the "spoofing" attack. By temporarily modifying their own network address to appear as though they were from the trusted address, they were able to fool or "spoof" the filter, allowing them access to the protected computer.

4-Security Action:

To protect internal computers from an external spoofing attack, as well as several other types of hacker attacks, a more sophisticated external network gateway was created: the firewall. The firewall prevents external computers from masquerading as internal "trusted" computers by disregarding external message packets that have "spoofed" an internal return address.

5-Hacker Advance:

In response to firewalls, hackers developed the "denial of service" attack. While most routers and firewalls can process a high number of reasonably sized incoming messages, they are limited in their ability to manage large pieces of information. By sending a grossly oversized packet of information, hackers can cause routers to overload and shut down, crashing the entire system.

6-Security Action:

Firewalls can be modified to filter out the hostile address. If the attack is onerous, the attacker can be traced and the attack reported to the hackers internet service provider for action.

continued from p. 15

This computer system and program management expertise facilitated his transition to Information System Security for the FAA. For the past 2 years, Kevin has been the Program Manager of the Volpe Center's Information Security Support to the FAA. His projects range from PDD-63 planning and risk assessments/vulnerability analyses, to Internet/network security, computer emergency response, security training, and security policy.

Volpe's Cyber Warrior
Charlie McCarthy

Charlie McCarthy exemplifies the new breed of "cyber warriors" being recruited by the Volpe Center. With decades of engineering experience in computer and communications security, and a recent background in law, Charlie provides the insight and perspective that the Volpe Center's sponsors demand for complex information security problems. Charlie joined the Volpe Center in 1997, after serving as Information Security Director for the Massachusetts Department of Revenue. Charlie's career also includes engineering experience with the FAA, Airway Facilities, overseas computer and communications security experience with the Central Intelligence Agency, and physical, technical, and information systems security experience with private sector organizations.

Volpe's Project Manager for Information Architecture Security
Daniel P. Sullivan

Dan Sullivan's experience with highly complex projects plays significantly into his role as project manager for the Office of Safety and Security. Managing the President's Commission on Critical Infrastructure Protection is one among many of the projects Dan has recently overseen. Others include the FAA's Information Security Project, and the Transportation Vulnerability Assessment. In addition to managing major research projects at the Volpe Center, Dan also serves as the interface for a classified contract being performed by the National Academy of Science. Prior to his work at the Volpe Center, Dan's career included positions in government sales and marketing for major corporations including Digital Equipment Corporation, as well as serving as senior economist for the U.S. Civil Aeronautics Board, the U.S. Federal Power Commission, and as Captain in the U.S. Marine Corps.