United States General Accounting Office

GAO

Testimony

Before the Permanent Subcommittee on Investigations,
Committee on Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at
9:30 a.m.
Wednesday
May 22, 1996

INFORMATION SECURITY

Computer Attacks at Department of Defense Pose Increasing Risks

Statement of Jack L. Brock, Jr., Director
Defense Information and Financial Management Systems
Accounting and Information Management Division

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to participate in the Subcommittee's hearings on the security of our nation's information systems. The Ranking Minority Member and other Subcommittee members have expressed serious concerns about unauthorized access to sensitive information in computer systems at the Department of Defense and directed that we review information security at the Department. These concerns are well-founded. Defense has already experienced what it estimates to be hundreds of thousands of computer attacks originating from network connections, some of which have caused considerable damage. As you will learn from our testimony, these so-called hacker intrusions not only cost Defense tens of millions of dollars, but pose a serious threat to our national security.

Computer Security Is Difficult but Necessary

Defense, like the rest of the government and the private sector, is relying on technology to make itself more efficient. The Department is depending more and more on high-performance computers linked together in a vast collection of networks, many of which are themselves connected to the worldwide Internet. Hackers have been exploiting security weaknesses of systems connected to the Internet for years, they have more tools and techniques than ever before, and the number of attacks is growing every day. These attacks, coupled with the rapid growth and reliance on interconnected computers, have turned cyberspace into a veritable electronic frontier. The need to secure information systems has never been greater, but the task is complex and often difficult to understand.

Information systems security is complicated not only by rapid growth in computer use and computer crime, but also by the complexity of computer networks. Most large organizations today like Defense have a conglomeration of mainframes, PCs, routers, servers, software, applications, and external connections. In addition, since absolute protection is not feasible, developing effective information systems security involves an often complicated set of trade-offs. Organizations have to consider the (1) type and sensitivity of the information to be protected, (2) vulnerabilities of the computers and networks, (3) various threats, including hackers, thieves, disgruntled employees, competitors, and in Defense's case, foreign adversaries and spies, (4) countermeasures available to combat the problem, and (5) costs.

In managing security risks, organizations must decide how great the risk is to their systems and information, what they are going to do to defend themselves, and what risks they are willing to accept. In most cases, a prudent approach involves selecting an appropriate level of protection and then ensuring that any security breaches that do occur can be effectively detected and countered. This generally means that controls be established in a number of areas, including, but not limited to:

- a comprehensive security program with top management commitment, sufficient resources, and clearly assigned roles and responsibilities for those responsible for the program's implementation;
- clear, consistent, and up-to-date information security policies and procedures;
- vulnerability assessments to identify security weaknesses;
- awareness training to ensure that computer users understand the security risks associated with networked computers;
- assurance that systems administrators and information security officials have sufficient time and training to do their jobs properly;
- cost-effective use of technical and automated security solutions; and
- a robust incident response capability to detect and react to attacks and to aggressively track and prosecute attackers.

Defense Systems Are Under Attack

The Department of Defense's computer systems are being attacked every day. Although Defense does not know exactly how often hackers try to break into its computers, the Defense Information Systems Agency (DISA) estimates that as many as 250,000 attacks may have occurred last year. According to DISA, the number of attacks has been increasing each year for the past few years, and that trend is expected to continue. Equally worrisome are DISA's internal test results; in assessing vulnerabilities, DISA attacks and successfully penetrates Defense systems 65 percent of the time. Not all hacker attacks result in actual intrusions into computer systems; some are attempts to obtain information on systems in preparation for future attacks, while others are made by the curious or those who wish to challenge the Department's computer defenses. For example, Air Force officials at Wright-Patterson Air Force Base told us that, on average, they receive 3,000 to 4,000 attempts to access information each month from countries all around the world.

Many attacks, however, have been very serious. Hackers have stolen and destroyed sensitive data and software. They have installed "backdoors" into computer systems which allow them to surreptitiously regain entry

into sensitive Defense systems. They have "crashed" entire systems and networks, denying computer service to authorized users and preventing Defense personnel from performing their duties. These are the attacks that warrant the most concern and highlight the need for greater information systems security at Defense. To further demonstrate the seriousness of some these attacks, I would like to briefly discuss the 1994 hacker attacks the Subcommittee asked us to specifically examine on the Air Force's Rome Laboratory in Rome, New York. This incident demonstrates how easy it is for hackers to gain access to our nation's most important and advanced research.

Rome Laboratory

Rome Laboratory is the Air Force's premier command and control research facility—it works on very sensitive research projects such as artificial intelligence and radar guidance. In March and April 1994, a British hacker known as "Datastream Cowboy" and another hacker called "Kuji" (hackers commonly use nicknames or "handles" to conceal their real identities) attacked Rome Laboratory's computer systems over 150 times. To make tracing their attacks more difficult, the hackers weaved their way through international phone switches to a computer modem in Manhattan. The two hackers used fairly common hacker techniques, including loading "Trojan horses" and "sniffer" programs, to break into the lab's systems. Trojan horses are programs that when called by authorized users perform useful functions, but that also perform unauthorized functions, often usurping the privileges of the user. They may also add "backdoors" into a system which hackers can exploit. Sniffer programs surreptitiously collect information passing through networks, including user identifications and passwords. The hackers took control of the lab's network, ultimately taking all 33 subnetworks off-line for several days.

The attacks were initially suspected by a systems administrator at the lab who noticed an unauthorized file on her system. After determining that their systems were under attack, Rome Laboratory officials notified the Air Force Information Warfare Center and the Air Force Office of Special Investigations. Working together, these Air Force officials regained control of the lab's network and systems. They also monitored the hackers by establishing an "electronic fishbowl" in which they limited the intruders' access to one isolated subnetwork.

During the attacks, the hackers stole sensitive air tasking order research data. Air tasking orders are the messages military commanders send during wartime to pilots; the orders provide information on air battle

tactics, such as where the enemy is located and what targets are to be attacked. The hackers also launched other attacks from the lab's computer systems, gaining access to systems at NASA's Goddard Space Flight Center, Wright-Patterson Air Force Base, and Defense contractors around the country.

Datastream Cowboy was caught in Great Britain by Scotland Yard authorities, due in large part to the Air Force's monitoring and investigative efforts. Legal proceedings are still pending against the hacker for illegally using and stealing British telephone service; no charges have been brought against him for breaking into U.S. military computer systems. Kuji was never caught. Consequently, no one knows what happened to the data stolen from Rome Lab.

Damage From the Attacks

In general, Defense does not assess the damage from the computer attacks because it can be expensive, time-consuming and technically difficult. But in the Rome case, Air Force Information Warfare Center staff estimated that the attacks on the Rome Lab cost the government over half a million dollars. This included costs for time spent to take the lab's systems off the networks, verify the integrity of the systems, install security "patches," and restore computer service. It also included costs for the Office of Special Investigations and Warfare Center personnel deployed to the lab.

But the estimate did not include the value of the research data that was compromised by the hackers. Information in general is very difficult to value and appraise. In addition, the value of sensitive Defense data may be very different to an adversary than to the military, and may vary a great deal, depending on the adversary. Rome Lab officials told us, however, that if their air tasking order research project had been damaged beyond repair, it would have cost about $4 million and 3 years to reconstruct it. In addition, the Air Force could not determine whether any of the attacks were a threat to national security. It is quite possible that at least one of the hackers may have been working for a foreign country interested in obtaining military research data or learning what the Air Force is working on. While this is only one example of the thousands of attacks Defense experiences each year, it demonstrates the damage caused and the costs incurred to verify sensitive data and patch systems.

National Security Concerns

Even more critical than the cost and disruption caused by these attacks is the potential threat to national security. Many Defense and computer

systems experts believe that computer attacks are capable of disrupting communications, stealing sensitive information, and threatening our ability to execute military operations. The National Security Agency and others have acknowledged that potential adversaries are attempting to obtain such sensitive information by hacking into military computer systems. Countries today do not have to be military superpowers with large standing armies, fleets of battleships, or squadrons of fighters to gain a competitive edge. Instead, all they really need to steal sensitive data or shut down military computers is a $2,000 computer and modem and a connection to the Internet.

Defense officials and information systems security experts believe that over 120 foreign countries are developing information warfare techniques. These techniques allow our enemies to seize control of or harm sensitive Defense information systems or public networks which Defense relies upon for communications. Terrorists or other adversaries now have the ability to launch untraceable attacks from anywhere in the world. They could infect critical systems, including weapons and command and control systems, with sophisticated computer viruses, potentially causing them to malfunction. They could also prevent our military forces from communicating and disrupt our supply and logistics lines by attacking key Defense systems.

Several studies document this looming problem. An October 1994 report entitled Information Architecture for the Battlefield prepared by the Defense Science Board underscores that a structured information systems attack could be prepared and exercised by a foreign country or terrorist group under the guise of unstructured hacker-like activity and, thus, could "cripple U.S. operational readiness and military effectiveness." The Board added that "the threat . . . goes well beyond the Department. Every aspect of modern life is tied to a computer system at some point, and most of these systems are relatively unprotected." Given our dependence on these systems, information warfare has the potential to be an inexpensive but highly effective tactic which many countries now plan to use as part of their overall security strategy.

Defense Faces Challenges in Securing Its Systems

Many factors combine to make information systems security a huge challenge for Defense: the vast size of its information infrastructure, its reliance on computer systems and increasing amounts of sensitive information, rapid growth in Internet use, and increasing skill levels among hackers coupled with technological advances in their tools and

methods of attack. Defense has taken steps to strengthen its information systems security, but it has not established a comprehensive and effective security program that gives sufficient priority to protecting its information systems.

Some elements of a good security program are in place. Most notably, Defense has implemented a formal information warfare program. DISA is in charge of the program and has developed and begun implementing a plan for protecting against, detecting, and reacting to information systems attacks. DISA established its Global Defensive Information Warfare Control Center and its Automated Systems Security Incident Support Team (ASSIST) in Arlington, Virginia. Both the center and ASSIST provide centrally coordinated, around-the-clock response to attacks and assistance to the entire Department. Each of the military services has established computer emergency response capabilities, as well. The Air Force is widely recognized as the leader among the services for having developed considerable experience and technical resources to defend its information systems.

However, many of Defense's policies relating to computer systems attacks are outdated and inconsistent. They do not set any standards or require actions for what we and many others believe are important security activities, such as periodic vulnerability assessments, internal reporting of attacks, correction of known vulnerabilities, and damage assessments. In addition, many of the Department's system and network administrators are not adequately trained and do not have enough time to do their jobs properly. Computer users throughout the Department are often unaware of fundamental security practices, such as using sound passwords and protecting them. Further, Defense's efforts to develop automated programs and use other technology to help counter information systems attacks need to be much more aggressive and implemented on a departmentwide basis, rather than in the few current locations.

In our report being released today, Information Security: Computer Attacks at the Department of Defense Pose Increasing Risks (GAO/AIMD-96-84), we are recommending that Defense take a number of actions to address these weaknesses and improve its information security posture. To ensure it has an effective security program, we recommend that the Department establish up-to-date policies for preventing, detecting, and responding to attacks on its systems; increase awareness among all computer users of the risks of computer systems connected to the Internet; and ensure that information security officials and systems

administrators receive enough time and training to do their jobs properly. Further, we recommend that Defense assess its incident response capability to determine its sufficiency in light of the growing threat, and implement more proactive and aggressive measures to detect systems attacks. The fact that these important elements are missing indicates that Defense has not adequately prioritized the need to protect its information resources. Top management at Defense needs to ensure that sufficient resources are devoted to information security and that corrective measures are successfully implemented.

Continued Oversight Needed

We have testified and reported on information systems weaknesses for several years now. In November 1991, I testified before the Subcommittee on Government Information and Regulation on a group of Dutch hackers breaking into Defense systems.[1] Some of the issues and problems we discussed here today existed then; some have worsened, and new challenges arise daily as technology continues to advance. Without increased attention by Defense top management and continued oversight by the Congress, security weaknesses will continue. Hackers and our adversaries will keep compromising sensitive Defense systems.

That completes my testimony. I'll be happy to answer any questions you or Members of the Subcommittee may have.

[1]Computer Security: Hackers Penetrate DOD Computer Systems (GAO/T-IMTEC-92-5, November 20, 1991).

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON  RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested