United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, United States Senate

For Release
on Delivery
Expected at
1:00 p.m. EST
Wednesday,
November 20, 1991

COMPUTER SECURITY

Hackers Penetrate DOD Computer Systems

Statement of
Jack L. Brock, Jr., Director
Government Information and Financial Management
Information Management and Technology Division

Mr. Chairman and Members of the Subcommittee:

I am pleased to participate in the Subcommittee's hearings on computer security. At your request, our work focused on hacker intrusions into Department of Defense (DOD) unclassified, sensitive computer systems during Operation Desert Storm/Shield. My testimony today is based on our review of intrusions by a group of Dutch hackers into Army, Navy, and Air Force computer systems. In particular, we conducted a detailed review of the hacker intrusions and system administration responsibilities at three DOD sites. While our focus was on unclassified, sensitive systems, some of the systems penetrated by this group of hackers did not contain sensitive information.

The government faces increased levels of risk for information security because of greater network use and computer literacy, and greater dependency on information technology overall. For years hackers have been exploiting security weaknesses of systems attached to the Internet--an unclassified network composed of over 5,000 smaller networks nationwide and overseas and used primarily by government and academic researchers. Their techniques have been publicized in hacker bulletin boards and magazines, and even in a bestseller, The Cuckoo's Egg written by Clifford Stoll. Hackers, however, continue to successfully exploit these security weaknesses and undermine the integrity and confidentiality of sensitive government information.

Between April 1990 and May 1991, computer systems at 34 DOD sites attached to the Internet were successfully penetrated by foreign hackers. The hackers exploited well-known security weaknesses--many of which were exploited in the past by other hacker groups. These weaknesses persist because of inadequate attention to computer security, such as password management, and the lack of technical expertise on the part of some system administrators--persons responsible for the technical management of the system.

DUTCH HACKERS PENETRATE DOD COMPUTER SYSTEMS

Between April 1990 and May 1991, computer hackers from the Netherlands penetrated 34 DOD sites. DOD officials, however, are still unable to determine the full scope of the problem because security measures for identifying intrusions are frequently lacking. At many of the sites, the hackers had access to unclassified, sensitive information on such topics as (1) military personnel--personnel performance reports, travel information, and personnel reductions; (2) logistics--descriptions of the type and quantity of equipment being moved; and (3) weapons systems development data.

Although such information is unclassified, it can be highly sensitive, particularly during times of international conflict. For example, information from at least one system, which was successfully penetrated at several sites, directly supported

Operation Desert Storm/Shield. In addition, according to one DOD official, personnel information can be used to target employees who may be willing to sell classified information. Further, some DOD and government officials have expressed concern that the aggregation of unclassified, sensitive information could result in the compromise of classified information.

Hackers Exploit Well-Known Security Weaknesses

The hackers generally gained access to the DOD computer systems by travelling through several networks and computer systems. Using commercial long-distance services, such as Tymnet, the hackers weaved their way on the Internet through university, government, and commercial systems, often using these sites as platforms to enter military sites.

The hackers then exploited various security weaknesses to gain access into military sites. The most common weaknesses included (1) accounts with easily guessed passwords or no passwords, (2) well-known security holes in computer operating systems, and (3) vendor-supplied accounts--privileged accounts with well-known passwords or no passwords at all that are used for system operation and maintenance. Once the hackers had access to a computer at a given site, access to other computers at that site was relatively easy because the computers were often configured to trust one another.

At several sites the hackers exploited a Trivial File Transfer Protocol[1] (TFTP). Some versions of this program had a well-known security hole that allowed users on the Internet to access a file containing encrypted passwords without logging into the system. Once the hackers accessed the password file, they (1) probed for accounts with no passwords or accounts where the username and password were identical, or (2) downloaded the password file to another computer and ran a password cracking program--a program that matches words found in the dictionary against the encrypted password file. Finally, the hackers entered the system, using an authorized account and password, and were granted the same privileges as the authorized user.

At two of the sites we visited the hackers were able to enter the systems because vendor-supplied accounts were left on the system with a well-known password or with no password at all. Operating systems and software are often delivered to users with certain accounts necessary for system operation. When delivered, these accounts--some of which include system administrator privileges that allow them to do anything on the system without restriction--

---

[1]TFTP is a file transfer program that permits the copying of files without logging in.

are often unprotected or are protected with known passwords, and are therefore vulnerable until the password is changed.

Hackers Established
Methods For Reentry

The majority of the hackers' activities appeared to be aimed at gaining access to DOD computer systems and then establishing methods for later entry. In many of the intrusions, the hackers modified the system to obtain system administrator privileges and to create new privileged accounts. For example, at some sites where the hacker entered the system using a vendor-supplied password, the hackers ran a program that elevated the privileges of the account and then erased evidence of the intrusion by removing the program. The hackers then created new privileged accounts with passwords known only to them and that blended in with the sites' naming conventions, making detection more difficult.

While there was little evidence that the hackers destroyed information, in several instances the hackers modified and copied military information. In a few cases, the hackers stored this information at major U.S. universities. They modified system logs to avoid detection and to remove traces of their activities. The hackers also frequently browsed directories and read electronic messages. In a few cases, they searched these messages for such key words as military, nuclear, weapons, missile, Desert Shield, and Desert Storm.

Agencies' Response
to the Incidents

In most cases, system administrators did not identify the intrusion, but were instead notified of the intrusion by university, contractor, or DOD officials. Once the system administrators were notified, they usually secured their system--such as changing the password of a vendor-supplied account. In a few cases, however, the sites left the vulnerability open temporarily in an effort to determine the intruder's identity. At one site we visited where this was done, the intruders' access to sensitive information was contained, and coordinated with law enforcement agencies.

Only one of the three military services had written procedures for incident handling prior to the intrusions. Since the intrusions, however, the other two services have established written procedures. Despite the lack of procedures, at two of the sites we visited security personnel prepared an incident report after they were notified about the intrusion. In addition, one site we visited established computer hacker reporting procedures for their organization. They also included security tips, such as changing

default passwords, using randomly-selected passwords, and maintaining audit trails.

HACKER INTRUSIONS HIGHLIGHT INADEQUATE ATTENTION TO COMPUTER SECURITY

The security weaknesses that permitted the intrusions and prevented their timely discovery highlight DOD's inadequate attention to computer security. Poor password management, failure to maintain and review audit trails, and inadequate computer security training all contributed to the intrusions.

DOD directives and military service regulations and instructions require both adequate computer security training for those responsible for systems, and audit trails--records of system activities--that are reviewed periodically and detailed enough to determine the cause or magnitude of compromise. In addition, the military services require password management procedures. The intrusions, however, indicate that these requirements were not always followed.

Poor password management--easily-guessed passwords and vendor-supplied accounts whose password had not been changed--was the most commonly exploited weakness contributing to the intrusions, including those at each of the sites we visited. At one site we visited the hacker exploited a vendor-supplied account, left on the system without a password, that in turn provided system administrator privileges.

In addition, officials also noted that failure to maintain or periodically review audit trails was a key reason why most system administrators were unable to detect the intrusions or determine how long their system had been compromised. For example, few of the 34 sites whose systems were penetrated were able to identify or verify the intrusions.

Several officials stated that system administration duties are generally part-time duties and that administrators frequently have little computer security background or training. At one site, for example, the system administrator had little knowledge of computers and system administrator responsibilities. In addition, with the exception of a brief overview of computer security as part of the introductory training for the system, the system administrator had not received any computer security training. Moreover, after the intrusion occurred, the newly appointed system administrator did not receive any additional computer security training and did not know the proper security reporting chain.

The security weaknesses that I have described here today have been and continue to be exploited by various hacker groups. Two years ago we issued a report, Computer Security: Virus Highlights Need

for Improved Internet Management, (GAO/IMTEC-89-57), highlighting some of the same weaknesses--poor password management and system administrators who lacked the technical expertise to deal with security problems--that we discussed here today. In addition, numerous Computer Emergency Response Team (CERT) security advisories, available to anyone on the Internet, have addressed these weaknesses. Yet, despite these warnings, these security weaknesses continue to exist. Without the proper resources and attention, these weaknesses will continue to exist and be exploited, thus undermining the integrity and confidentiality of government information.

This concludes my remarks. I will now answer any questions you or members of the Subcommittee may have concerning these issues.

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. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20877

Orders may also be placed by calling (202) 275-6241.

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

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100