United States General Accounting Office

GAO

Testimony

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

For Hearing on
Wednesday,
June 5, 1996

INFORMATION SECURITY

Computer Hacker Information Available on the Internet

Statement for the Record of Jack L. Brock, Jr.,
Director, Defense Information and Financial Management Systems
and
Keith A. Rhodes, Technical Assistant Director,
Office of the Chief Scientist,
Accounting and Information Management Division

GAO/T-AIMD-96-108

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to again participate in the Subcommittee's continuing hearings on the security of our nation's information systems. As you know, on May 22, 1996, the first day of the Subcommittee's hearings, we testified and released our report[1] about the increasing risks computer hackers[2] pose to computer systems and information at the Department of Defense. Our purpose today is to reiterate the importance of computer security to Defense and other federal agencies, and to provide an introduction to hacker techniques and information available on the Internet.

Computer Attacks Are an Increasing Threat

The Department of Defense, like the rest of government and the private sector, relies on technology. The Department depends increasingly on computers linked together in a vast collection of networks, many of which are connected to the worldwide Internet.[3] The Internet provides tremendous benefits; it can streamline business operations and put a vast array of information at the fingertips of millions of users. Over the last several years, we have seen a rush to connect to the Internet, and today there are over 40 million users worldwide.

However, with these benefits come risks. Hackers have been exploiting security weaknesses of systems connected to the Internet for years. The number of people with access to the Internet, any one of which is a potential hacker, coupled with the rapid growth and reliance on interconnected computers, has made the cyberspace frontier a dangerous place. Hackers have more tools and techniques than ever before, and the number of attacks is growing every day. The need for secure information systems and networks has never been greater.

The Department of Defense's computer systems are being attacked every day. Although the exact number of attacks cannot be readily determined because only a small portion are actually detected and reported, Defense

[1]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

[2]The term hacker refers to unauthorized individuals who attempt to penetrate information systems; browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way.

[3]The Internet is a global network interconnecting thousands of dissimilar computer networks and millions of computers worldwide. Over the past 20 years, its role has evolved from relatively obscure use by scientists and researchers to a popular, user-friendly means of information exchange for millions of users.

Information Systems Agency (DISA) data suggest that Defense may have experienced as many as 250,000 attacks last year, and that the number of attacks is doubling each year. DISA information also shows that attacks are successful 65 percent of the time.

Not all attacks result in actual intrusions; 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. Many attacks, however, have been very serious, resulting in stolen and destroyed sensitive data and software. By installing backdoors, guessing passwords, or other techniques, hackers have surreptitiously gained illegal entry into sensitive Defense systems, many of which support critical functions, such as weapons systems research and development, supply, personnel, contract management, and finance. They have caused entire systems and networks to crash, denying computer service to authorized users and preventing Defense personnel from performing their duties. Although Defense has not computed the cost of these attacks, unofficial estimates place the cost at millions of dollars in lost productivity and damage to systems.

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 attackers can disrupt communications, steal sensitive information, and threaten our ability to execute military operations. The National Security Agency and other experts have acknowledged that potential adversaries are attempting to obtain sensitive information by hacking into military computer systems. They believe that over 120 countries either have or are developing information warfare capabilities. 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 need to steal sensitive data or shut down military computers is a $2,000 computer, a modem, and a connection to the Internet.

The Internet was spawned from ARPANET, a network designed by the Advanced Research Projects Agency in the 1960s to provide a means of electronically exchanging military research information. The main goals of ARPANET were to provide a network that would continue to function even if sections of the network were lost, to allow computers of many different types to communicate with each other, and to enable inexpensive, convenient addition or removal of nodes (Internet hookups). In the 1980s, ARPANET became the Internet. Because of this history, the

Department of Defense has been using the Internet longer and more widely than other government agencies. As a result, the Department, despite its problems, probably has one of the strongest computer security programs in government. Its experience suggests, however, that other agencies will increasingly be at risk of computer attacks as they expand their use of the Internet.

How Computer Systems Are Attacked

A variety of weaknesses can leave computer systems vulnerable to attack. For example, they are vulnerable when (1) inexperienced or untrained users accidentally violate good security practices by inadvertently publicizing their passwords, (2) weak passwords are chosen which can be easily guessed, or (3) identified system or network security weaknesses go uncorrected. Malicious threats can be intentionally designed to unleash computer viruses,[4] trigger future attacks, or install software programs that compromise or damage information and systems.

Attackers use a variety of methods to exploit numerous computer system vulnerabilities. Examples, include (1) sendmail - a common type of attack in which the attacker installs malicious code in an electronic mail message that adds a password into the system's password file thereby giving the attacker total system privileges, (2) password cracking - a technique in which attackers try to guess or steal passwords to obtain access to computer systems, and (3) packet sniffing - a technique in which attackers surreptitiously insert a software program that captures the passwords and user identifications contained in the first 128 key strokes of a connection.

Once they have gained access, hackers use the computer systems as though they were legitimate users. They use a variety of techniques to cover their tracks and avoid detection. Hackers can steal information, both from the systems compromised as well as systems connected to them.

Hacker Information Available on the Internet

Computer attacks have also become easier to carry out due to the proliferation of readily available hacker information, tools, and techniques on the Internet. Behind this proliferation are informal hacker groups, such as 2600, the Legion of Doom, and Phrack, Inc., which openly share information on things such as how to break into computer systems and how to obtain free telephone service. The information posted on the

[4]A virus is a code fragment that reproduces by inserting copies of itself to other programs. In may damage data directly, or it may degrade system performance by taking over system resources which are then not available to authorized users.

electronic bulletin boards at the web sites[5] such groups sponsor allows virtually any of the more than 40 million Internet users who wants to be a hacker to become one.

The potential hacker can learn about these groups from any computer with an Internet connection by using any one of a number of search programs available to Internet users. These programs, or search "engines," which include lycos, alta vista, yahoo, web crawler, excite, magellan, all can be used as a starting point to help a potential hacker pinpoint web sites containing information for conducting computer attacks. For example, we tried a simple single-word and dual-word query using the alta vista program. Using the word "hacking", we got more than 20,000 responses showing Internet sites or files where information on hacking is available. Similarly, using the words "password cracking", we got an additional 20,000 responses. The two examples below are typical of the responses we came across.

- alt.2600/#hack FAQ at www.(site).edu/alt2600/FAQ.html
- alt.2600 Survival Guide at www.(site).edu/alt2600/survive.html

These two responses are from alt.2600, the file name of a web site on the Internet that supports the readers of 2600 Magazine, a hacker quarterly. The purpose of the alt.2600 survival guide is to provide information on the hacker news group, as well as information on how to avoid being caught by the people and organizations under attack. To get to the web site containing the files, one need only click on the file name. In this case, we were sent to a web site called the Internet Underground. The Internet Underground site provides a typical disclaimer

"This WWW (world-wide web) page is provided for informational sake to those like me who are interested in computer and telephone security. In no way do I encourage you to do anything illegal (emphasis added). Far from it. Think of this as a guide of what not to do."

This disclaimer is like openly providing the recipe for baking a cake, but telling you not to bake it. Despite this disclaimer, people will use the information to hack into computer systems.

At this Internet Underground site, one can examine the frequently asked questions, or take a look at the survival guide itself. The survival guide

[5]The worldwide web (www), started by Tim Berners-Lee while at the European Laboratory for Particle Physics, is a "distributed hypermedia system." In practice, the web is a vast collection of interconnected information, spanning the world. A web site is any computer on the Internet running a World-Wide Web server process. A particular web site is identified by the hostname part of the uniform resource locator.

begins, “Welcome to alt.2600, the Internet news group for readers of 2600 Magazine. On alt.2600 we discuss telephone (phreaking), computer (hacking), and related topics. . . . alt.2600 readers pride themselves on being hackers. A hacker seeks out information by every available means (emphasis added).”

If you proceed further into this site, you can locate additional information files. For example, “info philes” (spelled with a “ph” because the file mostly contains information on how to break into a telephone system) contains information on how to build devices known as boxes that allow you to break into cable/video boxes, pay telephones, or telephone circuits. For example, one home page[6] we visited containing information on these devices was John’s Boxing Page. Again we came across a disclaimer that read “. . . my intention is not to defraud or encourage people to defraud the phone company. . .” and then proceeded to describe how to build 26 different kinds of boxes. One of the files linked to this home page gave the following directions for building a red box.

1. Buy Radio Shack part number 43-146.
2. Unscrew all of the screws.
3. Desolder the crystal which says 3579 on it.
4. Replace it with a 6.5536 MHz crystal.
5. Replace the cover.
6. You now have a red box.

Although this information is claimed to be outdated and no longer valid, a red box is typically used to generate a digital or tonal signal that emulates the sound of coins being dropped into a public telephone, thus allowing hackers to make telephone calls for free.

There are many other hacker publications on the Internet. For example, Phrack is a very popular phone cracking association. When you go to this web site, you find several directories; one being the Phrack Magazine Underground Archives. The maintainers of the archives have collected a variety of documents from various phreaking, cracking, and hacking sources. These publications include information on hacker conferences and how to break into computer and telephone systems. It also contains links to other web sites. Following is just a partial list of groups in the archives.

[6]A home page is typically the top-level introduction to an individual’s or institution’s Internet site. It often includes a uniform resource locator, a draft standard for specifying an object on the Internet, such as a file or newsgroup, e.g. http://www.ncsa.uiuc.edu/. All other pages on a server are usually accessible by following links from the home page.

- 40 Hex Magazine
- Activist Times, Inc.
- The BIOC Files
- Chalisti
- Freakers Bureau Inc.
- Freedom
- The Legion of Doom
- Misc. Underground Files
- National Security Anarchists
- The New Fone Express
- PHUN Magazine
- United Phreakers Inc.
- The Art of Technology Digest
- Anarchy 'N' Explosives
- The Cult of the Dead Cow
- Chaos Digest
- Digital Free Press
- Informatik
- Legions of Lucifer
- N.A.R.C. Newsletter
- Network Information Access
- Phantasy Magazine
- Pirate Magazine
- Vindicator Publications

For example, some of these groups openly share information on how to go from one's home into a public telephone switch without paying for it, and then go from there into another telephone switch (possibly in another country), and then from there to the desired destination. This use of multiple telephone switches makes it more difficult for the authorities to trace the hacker.

Also available on the Internet are user-friendly hacker tools. For example, SATAN (Security Administrator Tool for Analyzing Networks) is one such tool that was designed to identify computer system and network security weaknesses, but which is also being used by hackers to break into systems. Similarly, a tool called rootkit is available on the Internet. Rootkit is actually a series of "trojan horses." A trojan horse is a software program that replaces and mimics an existing function, but also performs unauthorized functions, often usurping the privileges of authorized users. For example, a hacker can install rootkit on a targeted system in a remote location. The program would be invisible to the authorized system

administrator, but would enable the hacker to obtain a list of the files on that system, monitor disk usage, and see what processes are running.

We also found hacker tools at an Internet bulletin board called the Computer Underground Digest. It contains nearly 70 directories, each containing information on how to undertake acts of destruction and mayhem such as how to break into systems and how to create and plant viruses. For example, the directory called 40hex/ publishes Spotlight on Viruses which actually includes some of the source code[7] for viruses that one can use to disrupt somebody else's computer system. Some of the virus information in 40hex/ includes

- Virus Spotlight, The Tiny virus
- Sub-Zero virus
- Leprosy-B
- USA Virus News
- The Sunday Virus
- The Typo COM Virus
- How to modify viruses to avoid SCAN
- Simple encryption techniques
- 1992 virus
- The Bob Ross Virus
- The Terror Virus

In conclusion, these bulletin boards and sites clearly show that any marginally computer literate individual can use the Internet itself to quickly obtain basic information on the tools and techniques needed to become a computer hacker. They also demonstrate that the Subcommittee's concerns about unauthorized access to sensitive information in computer systems are well-founded. The Department of Defense has already experienced thousands of computer attacks originating from network connections, many of which have resulted in considerable disruption and damage. Other government agencies and the private sector will undoubtedly be at increasing risk of attack as their reliance on the Internet increases, as the number of worldwide Internet users multiplies, and as information on hacker tools and techniques becomes even more readily available.

[7]Source code is the software program written in human readable form by the programmer, as opposed to object code which is derived from source code and is machine executable.

Mr. Chairman, that completes our statement. We will be happy to answer any questions you or Members of the Subcommittee may have.

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