In Security, Ignorance Is Not Bliss

In the Age of the Internet, the more you know about security, the better off you are.

As many of us know, system security in today's interconnected world is rapidly becoming more challenging for the systems administrator. There are so many potential security holes that the average administrator could spend every day tracking down and plugging them. Telling users to log off when they are done and forcing them to change their passwords periodically is not enough. As more and more organizations communicate over local- and wide-area networks and the Internet, the number of potential security cracks increases exponentially.

Plugging all the holes may not be necessary for most organizations; however, awareness of the possible points of entry should be on the forefront of every system administrator's mind to keep their systems from being mugged by hackers. Here are the major areas of concern and some suggestions for what to do about them.

Viruses. These nasty bugs can come in from infected diskettes and tapes or through data transmitted over the Internet. When you travel by plane these days, you are asked whether you have accepted anything from strangers and have packed your bags yourself. There is a lesson here: If you didn't create the diskette yourself, run it through one of the commercially available virus scanning software packages before loading it on your computer, and periodically perform a virus scan on all the company computers to be on the safe side.

Internal Networks. Internal networks typically consist of many systems communicating over the network with a variety of different versions of networking protocols, even if the entire network is based on TCP/IP. For example, if you assign a port or ports to service specific incoming requests like Rlogin or Telnet, a system can come into the network over one of those preassigned ports and be granted carte blanche access to the servers on the network. Using trusted ports is a good start, but only Unix systems support trusted ports. Non-Unix systems running the TCP/IP protocol stack without an embedded trusted port protocol can act as a gateway into the network, even on trusted ports. Once in, an intruder can spoof the network and gain access to other Unix systems.

Trusted hosts also can be accidents waiting to happen. They do not require a password to grant access. By either removing the /etc/hosts.equiv file completely or eliminating systems that don't really need trusted permission—requiring a password—you can reduce the possibility of an intruder gaining access to your network. Additionally, though the .rhosts file in the user's home directory makes it easier for the user, it is a potential major security hole. Plug it permanently by removing and prohibiting the creation of .rhosts files. Your users may complain because they will have to take a couple of more steps to gain access, but the safety will be worth the inconvenience.

The Internet. There are so many potential security holes on systems connected to the Internet that cheese makers in Wisconsin are working on a new variety called Internet Swiss; it has more holes than low-fat Jarlsberg. The problems involve anonymous FTP and how you connect to the Internet. Secure your anonymous FTP login first and foremost. This is easier than you think, and the majority of the necessary changes can be accomplished with the standard Unix security and access control commands: chmod, chown and chgrp.

For anonymous FTP users, make sure that whatever files you want them to access are in a subdirectory under FTP's home directory (/u/ftp or /usr/ftp). If one doesn't exist, create the appropriate directory (and FTP user) for your operating system version and modify the /etc/passwd file to reflect the changes, if necessary. Make sure the directory is owned by FTP and unwritable by all users. Give FTP users access only to the commands you want by copying them to a bin subdirectory under FTP's home directory, rather than adding the directories like /bin or /etc to their command search path. Make the directory owned by root and unwritable so FTP users can't add or modify entries.

Create an etc subdirectory in the FTP user's home directory that is owned by

By Glenn K. Schulke

the FTP user and unwritable by anyone, and put in copies of the /etc/group and /etc/passwd files containing only the entries required for the FTP user. Make sure that FTP's .profile, .cshrc or .kshrc search path contains this new search path and will not look at the regular /bin or /etc directories. Create another subdirectory in FTP's home directory, such as pub or xfr, where files will be placed for transfer in and out, and make the directory owned by FTP and writable by all. This is the only place where anonymous FTP users will be able to transfer files in and out. With the other changes made above, your anonymous FTP account should be reasonably secure.

The Internet is in the public domain, so common sense says don't put anything out there that you don't want people to have access to. As we saw in an earlier version of Netscape's Navigator, those who thought their data encryption scheme was secure were wrong.

Sendmail. It seems that as time passes, we tend to forget lessons the past has taught us. Remember, for example, the infamous Internet worm launched by Robert Morris in 1988. By design, sendmail runs as a superuser process. Knowing this, Morris issued a sendmail debugging command that allowed him through sendmail to issue any command desired. If you have an older version of Unix and are running sendmail, you have a potential time bomb on your hands. Update to a newer version or check out some of the other mailers such as smail or smap.

The X Window System. As the xhost utility allows other machines to connect and grant access, a common mistake (made to save time and hassle to the user) is to enter the xhost + command, thereby effectively disabling all access protection. All that hackers have to do is open a new window, and they're off and running.

Awareness of the possible points of entry should be on the forefront of every system administrator's mind to keep their systems from being mugged by hackers.

There are some good free tools for detecting problems with your network. The Security Analysis Tool for Auditing Networks (SATAN) and Tripwire are two readily available security analysis tools that can be useful in debugging security problems. Some of the areas probed include FTP and TFTP problems: whether your sendmail program is out of date; whether there are entries in your /etc/hosts.equiv that could cause your system to be trusted to all; and NFS configuration and other security issues. Add to these detecting break-ins quickly, so you can deploy damage control before it's too late.

You'll have to stay one step ahead of the wily hacker. The proliferation of the Internet has created many security holes, and with the sheer numbers and the amount of information available, both hackers and security specialists are having a tough time keeping up. When it comes to security, the more you know, the better the job you can do to keep your systems secure and your company's data integrity intact. IT

Glenn K. Schulke *is president of Open Technologies, Inc., a systems integrator specializing in software integration services, located in Tempe, AZ. He can be reached at gschulke@aol.com.*

COMPANIES MENTIONED IN THIS ISSUE

FEATURES

Sink or Swim with CTI: p. 26
Aspect Telecommunications
AT&T
Northern Telecom
Rolm

Wallflowers of the Web: p. 30
Adobe Systems
ANT Internet
BBN
Free Range Media
Symantec
U.S. Interactive

COLUMNS

Behind the News: p. 16
Allied Computer Group
Dickens Data Systems
Hewlett-Packard
IBM
Market Sales Co.
Pyramid Technology
Sun Microsystems
Symix
Western Micro
Workstation Technologies

Home Page: p. 40
Pointcast

High Technology and the Law: p. 46
CompuServe