securing your NeXT computer on a WAN

by Lee Tucker

The security of a local area network (LAN) or single NeXT computer becomes more complicated when either is attached to a wide area network (WAN). With the recent increase in availability of application software packages that support various types of wide area networking, it's important to understand how to secure your machines from outside attack. Computers that grant external access require special attention. The purpose of this article is to help you understand the basic steps you need to take to secure a computer granting external access. For a more complete discussion of security issues for wide area networking, see the references listed at the end of the article.

figure 1. accessing a wide area network (see page 37 in the hard copy support bulletin)

There are two basic ways in which your computer can access WANs. The first type of access allows users to log in through a dialup modem with an account name and user password. The access that is then granted is through a UNIX shell (typically /bin/sh or /bin/csh). A variant on this method is called UUCP or UNIX to UNIX copy. Instead of a user logging into your machine, a remote machine logs in and holds a conversation using UUCP protocols with a special shell called uucico.

The second way you can access a WAN is through TCP/IP protocols. For a good overview of some packages used to implement this type of access, see the article in this issue, ªdialing up for network service,º which discusses SLIP and PPP. When using this type of access, you need to take more complex measures to secure your machine.

When you access a WAN, the WAN is also, in some sense, accessing your computer. To protect your machine from unwanted intrusions from the outside, you need the type of security discussed in this article. If all you ever do is call out on your modem and use bulletin boards or other on-line services, these measures aren't necessary.

The following is a basic step-by-step list of security measures. Please take the time to review these measures,

understand them, and implement them as you see fit. It's always best to consider security before attaching a dialup modem or external network to your computer. Trying to repair a computer after security has been breached is difficult, time consuming, and expensive.

step one: reviewing passwords

The single most important thing you can do for your security when you set up a dialup modem or TCP/IP link is to review the security of passwords on the computer where the modem or network is attached. The biggest failure in any UNIX security system is an account with no password, or with a password that is easy to guess. A cracker who knows the number for your modem and the name of an account without a password has access to your computer as that user.

Chapter 16 of the Network and System Administration manual gives a simple method for reviewing passwords. All domains to which the machine is bound must be checked. Start with the local domain and work upward. If you find an account without a password, you should either help the user set a password for the account or set it yourself.

You can set any account's password with the passwd command or with UserManager. You can set the password for the account foo by typing passwd foo at a shell prompt. If the computer prompts for the old password, you must enter it first. Enter the new password twice as prompted by the passwd command. UserManager can also be used to disable accounts or set their passwords.

With either a TCP/IP or a dialup modem, users on the computer granting access should change their passwords on a regular basis. One of the best ways to keep unwanted individuals from guessing a password is to keep it a moving target.

step two: securing NetInfo domains

If you're going to attach an external TCP/IP network, you need to secure read access to your NetInfo domains. This is important for two reasons. First, some data stored in NetInfo, such as user account names and encrypted passwords, can be used to break into your network directly. Second, other data, such as lists of

machines or shared file systems, can be used to gather information about how your network is configured so that more sophisticated attacks can be planned and executed. Chapter 16 of Network and System Administration gives the precise procedure for securing your NetInfo domains.

You might think that encrypted passwords or a list of hosts is fairly innocuous data. However, new variants on the UNIX method for encrypting passwords can allow crackers with sufficient computing power to encrypt enough passwords to attempt to guess their way in. This power gives them a reasonable chance of breaking at least one password on any given computer. They accomplish this by encrypting password after password until they get a match for the encrypted value stored in your NetInfo database. Then they use the unencrypted match to gain access to a shell on your machine. Once inside your computer, they have a foothold to further compromise your security. This is why password security is always step one in any UNIX security implementation.

step three: selecting services

Carefully consider which of the services your machine provides you wish to grant to the outside world. Do you want people to be able to log into your machine remotely, transfer files, or exchange mail or news? Once you've decided, it's important to disable all the other services you do not wish to share. Doing this helps prevent outsiders from using those unused services to compromise your security.

When you attach an external TCP/IP network, most services can be disabled simply by changing a line in the file /etc/inetd.conf. This file contains a list of on-demand services that your computer will grant when another computer attempts to connect to one of them. The inetd.conf file looks something like this:

```
# @(#)inetd.conf 1.1 87/08/12 3.2/4.3NFSSRC
#
# Internet server configuration database
#
ftp             stream          tcp     nowait  root    /usr/etc/ftpd           ftpd
telnet          stream          tcp     nowait  root    /usr/etc/telnetd        telnetd
shell           stream          tcp     nowait  root    /usr/etc/rshd           rshd
login           stream          tcp     nowait  root    /usr/etc/rlogind        rlogind
```

To disable rlogin, for instance, you should edit the file as root using Edit. Place a # in front of the line that reads:

```
login    stream    tcp    nowait    root    /usr/etc/rlogind    rlogind
```

so that it becomes:

```
#login    stream    tcp    nowait    root    /usr/etc/rlogind    rlogind
```

You should do this for most of the services in the file. You may wish to continue ftp and telnet.
For a UUCP-style connection, a different set of files is used to determine what services a remote computer can access. Configuration of these files is covered in Chapter 14 of Network and System Administration.

step four: monitoring and restricting access

After you've connected a TCP/IP network or dialup modem, you should begin to monitor your machine more carefully. It's often possible to spot intrusions onto your system by watching who is logging in, when, and for how long. Chapter 16 of Network and System Administration recommends some specific commands you can use to monitor this type of access.

Furthermore, any computer attached to an external network or a dial-up modem should never be trusted by other computers on your LAN. You should set up your .rhosts, and hosts.equiv appropriately. For specific information on how to configure these files, see the respective UNIX manual pages. If you trust the computer granting the access, when its security is compromised, the whole LAN is compromised.

step five (and beyond): further restricting access

In larger and more complex networks, there comes a time when the security measures just discussed are no longer sufficient. Most people using SLIP/PPP/UUCP connections are doing so to connect a single isolated computer or very small network into a much larger network. For most crackers, breaking into such a small operation isn't worth their time. However, if you're a growing business using these products, you should be careful. One day your network will become ªworth the effort.º

Concepts such as firewall systems and packet filtering come into play at this point. Firewalls are systems that stand between you and the WAN. Typically they have very few accounts, with very difficult passwords. They forward only those service requests that you have designated as appropriate. They're easy to watch for intrusion and to shut down to block all WAN access. With more sophisticated implementations of SLIP/PPP or with dedicated routing hardware, it's possible to further restrict TCP/IP access to your network. Information flow can be restricted to just the services you want to use and then directed solely to the correct target machines.

If you plan to connect a large LAN to a WAN, make sure you read the references at the end of this article. They contain much valuable insight in dealing with larger LANs and security. Experience is a very harsh teacher for security lessons, so it pays to learn from other people's experiences.

references

Garfinkel, Simson, and Gene Spafford. *Practical Unix Security.* O'Reilly and Associates, Inc., 1991.

Network and System Administration manual, Chapters 14, ªUsing UUCP,º and 16, ªSecurity.º NeXT Computer, Inc., 1990.

Russell, Deborah, and G. T. Gangemi, Sr. *Computer Security Basics*. O'Reilly and Associates, Inc., 1991.

Stoll, Clifford. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday, 1989.