your BEST

This spring, a small Boston publishing house that had recently connected to the Internet discovered something suspicious on its Unix mail file server: an account under the username "mp" that didn't seem to belong there.

Somebody had broken in.

The system logs showed three account accesses under the mp username during the previous month. The attacker had set up a special FTP account with *unrestricted superuser access.* Before the discovery, anybody on the Internet could have connected to the company's computer and accessed or erased any file on the system.

Less than a month before the publishing house breach, a high-tech consulting firm in Cambridge, Massachusetts, suffered an intrusion of its own. This attacker was more skillful, erasing evidence of the intrusion from the log files and modifying system utilities to mask his or her

ILLUSTRATION BY JOHN WEBER

Defense SYSTEM

YOUR DATA ISN'T SAFE. To protect your data from digital espionage, we explore the issues and cover the products you need to ensure security. **by Simson Garfinkel**

ongoing presence. The intruder planted software that captured passwords from potentially thousands of users—passwords that the intruder will likely use to break into still more systems.

Clearly, it's time to get serious. After years of being relatively lax, companies are beginning to take computer security seriously. "This nation is under IW (Information Warfare) attack today by a spectrum of adversaries ranging from the teenage hacker to sophisticated, wide-ranging illegal entries into telecommunications networks and computer systems," states a report the Department of Defense's Science Board Summer Study Task Force issued last summer.

Even if you don't buy into the idea of global information warfare, there's plenty of reason for concern about the security of your network. You don't have to be a genius or a computer-security guru to protect your corporate network. All you need is some common sense to understand the threats your organization faces and to determine the best measures you can take to protect your systems and data.

Most corporate sites already take advantage of basic security measures like user passwords and locked server rooms. But as networks expand to include links to the Internet, remote access via dial-in lines, and other digital connections, your risk increases correspondingly. Fortunately, there are ways to reduce the probability of invasion. A combination of commonsense precautions and the proper use of security hardware and software can nearly eliminate your system's vulnerabilities. In this article, we explore the security issues that affect corporate desktops and LANs, WANs (wide-area networks), and telecommunications systems, as well as products designed to prevent intrusions.

Simson Garfinkel is a freelance writer and security expert. His latest book is *PGP: Pretty Good Privacy*, from O'Reilly Associates.

The Skim

WITHIN THESE WALLS

The Primer

In LAN, security paranoia pays off

MOST COMPANIES wouldn't dream of giving a newly hired administrative assistant the keys to the CEO's private file cabinet. Yet many companies do the equivalent of this—and more—with their computers and local-area networks. The data on your computers is one of your company's most valuable assets. Everything is there: correspondence, customer lists, financial models, personnel information, and plans for future products.

Regular backups are the key to recovering from any kind of data loss. Keep backups under lock and key and record the date of each backup, the backup tape's number, and the tape's current location.

Render the tape useless to potential thieves by encrypting the data. The two kinds of cryptography are secret key and public key. Secret-key systems are like passwords: Type the key once to scramble your data. Typing your key a second time unscrambles the data.

Public-key cryptography uses one key for encrypting and another for decrypting. Public-key systems and e-mail work well together, because you can store a person's public key in a directory (like X.500). Anybody can use that public key to send that person encrypted mail. You can run most public-key algorithms in reverse to create unforgivable digital signatures that simply verify the sender.

Secret-key systems, such as Kerberos, store a copy of everybody's keys on a central server. If someone compromises the server, then you have to change everyone's keys. Public-key systems store only public keys, not secret keys. You can publish the public keys—the secret keys will still be secure.

The best encryption solution is software that automatically encrypts files at write time and decrypts them when you read them back from the hard disk. (Some backup programs let you encrypt files during writes to tape.)

Encryption is the *only* way to eliminate network eavesdropping. Any computer can intercept and read every packet of information transmitted over the LAN. If you back up your files over the network each night, an attacker with physical access to your LAN doesn't even have to break into your file server.

Don't employ user-typed passwords: Let the user type a pass phrase, then hash it with a hashing algorithm such as MD4 or MD5. Avoid systems that store a cryptographic key unencrypted on your hard disk: You'll get more security with smart cards that users

The Players

Scrambled data keeps all your secrets

Contemporary Cybernetics offers a DES-encryption option on many of its CY-series tape drives. The cryptography doesn't require any programming and doesn't slow down the backup and restore processes. Cybernetics literally burns the cryptographic key into a small plastic key that fits into a matching keyhole on the drive's front. We had to insert this physical key into the drive, turn it, and then remove it when we turned on our test system. The physical token prevents somebody from using a stolen drive to read stolen backup tapes. It worked so invisibly that we didn't even realize the encryption was happening.

Plenty of companies offer encryption software that integrates with Windows or DOS. The simplest of these programs let you create an encrypted partition on your hard disk that you must access through a special encrypting device driver. If this is all you need, then you should check out SecureDrive, a public domain disk-encryption program written by Edgar Swank. The program encrypts your data with DES, an algorithm that should be safe enough for most purposes through the next five years. We noticed a slight decrease in speed but got past it by keeping our data files on the encrypted drive and storing our applications on the C: drive. SecureDrive comes with the source code so you can verify the absence of hidden trapdoors into your system.

The trouble with SecureDrive is that if you forget your key, you're hosed. RSA Secure, from RSA Data Security, gets around this problem. RSA Secure has a unique feature called Emergency Access, which lets you store a copy of your password on a floppy disk, or you can use Secret Sharing to split your key among several trustees: You specify the number of trustees to create, and the number of trustees you will need to recover your information.

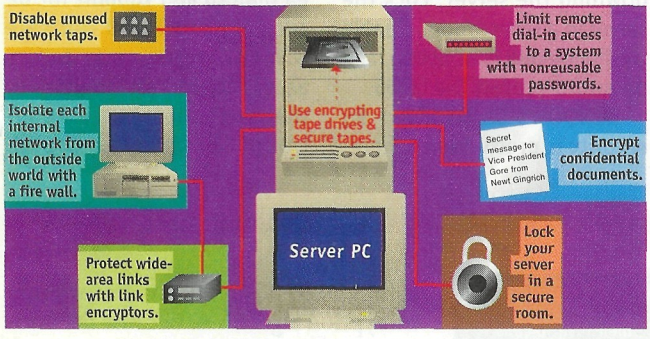
RSA Secure uses RSA's proprietary RC4 cypher with 80-bit keys. Cryptographers are beginning to look at this code, and it seems to be quite secure. This is a terrific product, one of the best we looked at. Its authors really thought about the day-to-day reality of using encryption. Instead of working at the device-driver level, RSA Secure integrates

can take with them.

SECURE NETWORKS Many firms think that physically securing their network will prevent intrusion. But because perfect physical security is nearly impossible, reinforce it on your NT or NetWare LAN with sound management techniques. Disable unused active network taps. Convince (or coerce) your users to encrypt sensitive files. And make sure your users don't run packet-sniffing programs. Good network-management software, such as Microsoft's SMS or Computer Associates' CA-Unicenter, can assist in tracking.

NT, WIN 95, AND NETWARE Microsoft designed Windows NT to provide users with C2-level security. C2 provides user authentication, resource isolation, and network activity auditing. NT's user-authentication scheme relies on user

>>>CONTINUES ON PAGE 84>>>



with the Windows File Manager and lets you encrypt or decrypt files on demand. We set up a list of AutoCrypt files or directories that automatically encrypted when we exited Windows and then decrypted when we started back up (once we supplied the appropriate key).

We tried Watchdog, a security kernel from Fischer International Systems that provides password-protected access to directories. We learned that unless we installed the operational encryption engine, it was easy to subvert the system by booting from a floppy disk. The installation program for the Windows version of Watchdog locked up our test PC, and we had to remove it manually. The lesson: Pilot cryptography schemes on a sacrificial PC first and do a complete backup before any installation.

You can dramatically limit network eavesdropping by not sending passwords

>>>CONTINUES ON PAGE 84>>>

Pretty Good Privacy? Yes.

Just Use PGP

Stop the controls. PGP remains today's best encryption solution.

Two years ago, Bruce Schneier published a groundbreaking book, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, which made it easy for programmers to add high-strength encryption algorithms to their programs. Since then, *Applied Cryptography* has sold tens of thousands of copies all over the world. But an interesting quirk of U.S. law prevents Schneier from sending floppy disks of the book out of the country: U.S. law classifies cryptographic programs as munitions that require special export permission from the Departments of State and Defense.

There's sound historic precedent for preventing the export of cryptography. During World War II, the Allies cracked Hitler's ultrasecret Enigma cipher. Historians credit this Allied code-breaking effort with shortening the war by as much as a year.

That was before computers. Today, a program called PGP, which stands for Pretty Good Privacy, can turn any PC into a cryptographic workhorse. After spending years analyzing PGP, some of the world's best cryptologic minds concluded that its codes are unbreakable—at least for now. And PGP is freely available on the Internet. Proponents of PGP live all over the world; they use it to protect their electronic mail from accidental interception, corporate espionage, and even the prying eyes of totalitarian regimes.

PGP packs a double punch for corporate users, combining encryption and authentication to secure the data it's protecting. There are two versions of PGP: the freeware version licensed for single-users only, available as a download; and a commercial product from ViaCrypt (PGP for WinCIM/CSNav) that's fully compatible with the free version. If you want to use PGP in a corporate or commercial setting, you'll need to buy the ViaCrypt product. ViaCrypt's version lets you encrypt and decrypt messages, and generate public and private keys of up to 1,024 bits.

You would think that with PGP's widespread distribution, the U.S. government would stop fighting it and admit defeat. You would be wrong. For more than a year, a federal prosecutor has been building a case against PGP's author, Phillip R. Zimmermann. Most likely, the government will charge Zimmermann with conspiring with unknown persons outside the United States to illegally export PGP in violation of U.S. munitions law—if the prosecutor decides to press the case.

Can the government make its charges stick? Maybe, maybe not. But it doesn't matter. By forcing Zimmermann to spend thousands of dollars in legal fees, the prosecutor has created an effective deterrent against anyone who would dare to follow in his footsteps.—**Simson Garfinkel**

Within These Walls

The Primer

Jargon

key The word, phrase, or string of bits a person uses to encrypt or decrypt your document. With a good encryption system, losing your key has roughly the same effect as skewering your hard disk with a screwdriver.

secret-key cryptography A cryptography system that uses the same key to encrypt and decrypt your messages. Think of the key as a codebook: If somebody steals it, they can understand all of your encrypted messages.

public-key cryptography A more advanced form of cryptography that uses one key to encrypt your message and another to decrypt it. Public-key algorithms are slower than secure-key algorithms. As a result, their main use is to exchange keys people then use to decode secret-key encrypted messages.

DSS The U.S. government's Digital Signature Standard. Based on public keys and secret keys, DSS can sign and verify documents but not encrypt them.

>>>CONTINUED FROM PAGE 83>>>

accounts and the concept of user groups. Users who belong to more than one group (with differing rights) are subject to the lesser rights. NT lets you set a threshold for incorrect log-on attempts (followed by server lockout) and supports single log on to one or many computers throughout a logical network domain. Force NT users to change passwords at regular intervals.

You'll get the best results when you combine NT Server with NTFS (NT File System) rather than FAT (file allocation table) because NTFS lets you define access rights down to the file level, specifying users with access to the files and each user's access level. If you use FAT with NT Server, you can control file access only through shared network directories—users who boot with a DOS disk can bypass this system.

Don't allow your NT system to boot into DOS, as a hacker can get to everything just by downing the server. Lock the server in a secure room, disable the floppy-disk boot option, and password-protect the CMOS.

WINDOWS 95 Windows 95 security is pretty basic (share- and user-level) and doesn't come close to NT security. Share-level lets users password-protect resources, while user-level assigns privileges to user IDs and restricts access to particular files. Windows 95 user-level security relies on pass-through validation that an NT or NetWare server provides. And the Windows 95 security subsystem applies only to network access.

NETWARE NetWare, like NT, is capable of C2-level security support. NetWare also includes object-level security in NDS (NetWare Directory Services). Microsoft and Novell plan to add support for B2 security to NT and NetWare 4.1. B2 forces mandatory access control (as opposed to the discretionary access control of C2 systems). ■■■

The Players

>>>CONTINUED FROM PAGE 83>>>

over LANs. CyberSAFE has developed a network security environment called Challenger, which is based on Kerberos, a security system that authenticates user identity at log on. Kerberos doesn't use public-key cryptography, so you'll have to maintain a secure server for holding the plain-text copies of everybody's key. Challenger gives you a single sign-on, so users don't have to remember multiple passwords for different computers. Challenger works with Windows, DOS, Macintosh, and seven different Unix platforms. (CyberSAFE has beta clients available for MVS, NetWare, Windows NT, and OS/2.) The program demands a physically secure server because it stores plain-text passwords for every user and every network service. On the plus side, CyberSAFE integrates with Security Dynamics' SecurID card. But Challenger won't encrypt files shared over your LAN using NetWare or NFS; you must individually encrypt important files.

The SmartDisk Security Corp. makes a cryptographic token (the SmartDisk) that looks like a 3.5-inch floppy disk and gives you a secure place to put your cryptographic keys. The card works with SafeBoot, a system that encrypts the contents of your hard disk and uses the key stored in the SmartDisk to decrypt the information. Unfortunately, instead of using DES, SSC uses a proprietary encryption algorithm. Because the algorithm is exportable, it can't be very good. Too bad—it's good hardware in search of better software. ■■■

C2 Security at a Glance

Discretionary access control
Users define rights to files they've created.

Identification and authentication
System uses unique IDs and security profiles for authentication and auditing.

Object-reuse protection
Keeps users from getting to data left from previous writes or other uses.

Auditing
Associates a user's identity with all security-related actions.

C2-secure systems have four requirements: discretionary access control, identification and authentication, object-reuse protection, and auditing. B2 security adds mandatory access control.

CyberSAFE Challenger Pilot, $9,950. CyberSAFE Corp., 2443 152nd Ave. NE, Redmond, WA 98052; 206-883-8721; fax, 206-883-6951. *reader service card 031*

CY 85055, starting at $5,000. Contemporary Cybernetics Group, 11846 Rock Landing, Rock Landing Corp. Ctr., Newport News, VA 23606; 804-873-9000; fax, 804-873-8836. *reader service card 029*

RSA Secure, $129, RSA Data Security, 100 Marine Pkwy., Suite 500, Redwood City, CA 94065-1031; 415-595-8782; fax, 415-595-1873; info@rsa.com. *reader service card 030*

SecureDrive, ftp://ftp.csua.berkely.edu/pub/cypherpunks/filesystems.

SmartDisk, $200, SmartDisk Security Corp., 4073 Mercantile Ave., Naples, FL 33942; 813-263-3475; fax, 813-643-6357; sdscinfo@netcom.com. *reader service card 032*

Watchdog for Windows 1.01, $100. Fischer Intl. Systems Corp., 4073 Merchantile Ave., Naples, FL 33942; 800-237-4510; fax, 813-643-3772. *reader service card 075*

The Skinny

Best defense: Common sense

The best way to protect your corporate LAN is to secure it against insiders, employees who have physical access to your systems and who know your procedures. Protect against insiders, and you'll defend your organization against four out of every five corporate data losses. And securing your network against insiders defends it from most outside attacks. Give users the privileges they need to do their work, but nothing more.

Every user with write privileges and e-mail is a potential virus-distribution mechanism. Load an antivirus program on the network and on each user's PC. Eliminating e-mail isn't a sensible response to the threat of a virus attack.

A powerful encryption system can do a better job protecting your data than a bank vault with a 24-hour guard. Don't trust proprietary encryption systems: Most of them aren't any good. Insist on DES, RC4, or IDEA. And don't trust an encryption key that's smaller than 56 bits. If a company says that revealing its cryptographic algorithm would jeopardize your data, then you know not to trust its products. The best cryptographic algorithms don't depend on any more security than the secrecy of the key. Don't believe companies that claim their secrecy adds an additional layer of security: If they used a strong encryption system, that extra layer would serve no purpose.

Back up your laptop data and applications before each trip; it's faster to reload from a backup tape than from a pile of floppy disks. Install a program that automatically encrypts files on the hard disk to cut the chance of proprietary data falling into the wrong hands.

Synchronize your security program with the level of protection your data demands. Decide which files need the greatest protection and assign access rights accordingly. Users won't take your security measures seriously if those measures don't make sense. Data typically grows less sensitive over time, so institute a policy of periodic data review. As information ages, reevaluate its sensitivity and reassign access rights accordingly. ■■■

The Critical Distinctions

Best-Kept Secrets

Go For Public Keys

Public keys are the safest way to secure your data today.

Stanford researchers Whitfield Diffie and Martin Hellman invented public-key cryptography in 1977. Under this system, each user has two keys: a private key, known only to its owner, and a public key, known to all users. You use your private key to encrypt a message, and the recipient uses your public key to decrypt it. Someone who knows your public key can use it to encrypt a message he or she sends to you. Only your private key can decrypt messages encrypted with your public key.

The Diffie-Hellman system allows two parties to exchange information over a communications link with absolute secrecy, even if a third party is monitoring the link. Many communications device manufacturers—such as AT&T, with its Clipper phone, the Surety 3600s—build this algorithm into their devices. But Diffie-Hellman requires active participation (as in a phone conversation) on both sides of the communications link. For that reason, it's not useful for encrypting documents or electronic mail.

RSA All the Way If you want to send and receive encrypted mail, then you'll probably find yourself using the RSA algorithm. RSA Data Security, the company that RSA's three inventors formed, widely licenses the algorithm (and augments it with development tools).

You first need to create a pair of cryptographic keys: a secret key and a public key. The public key encrypts messages; the secret key decrypts them. RSA keys can be any length: the longer they are, the more secure. Most serious RSA users employ keys that are at least 1,024 bits long. Experts say that messages encrypted with these keys should be safe for at least 30 years.

Although RSA Data Security has developed a set of standards for public-key cryptography, most programs that use RSA still have incompatible keys and data file formats. As a result, you can't take your RSA key from Lotus Notes and use it with PGP, for example.

Nevertheless, because PGP is freely available for noncommercial use, its file formats are quickly becoming international standards for exchanging cryptographic keys and files. With PGP, you can create your own public key, then distribute it freely. Don't worry about your public key falling into the wrong hands: No matter who gets it, he or she won't be able to use it to decipher your incoming mail.

On the other hand, be sure you keep your private key to yourself!—**Simson Garfinkel**

FAR AND WIDE

The Primer

Internet-to-WAN plans? Fire wall required

ADDING A CONNECTION to the Internet broadens your network's scope even further, letting you communicate with more than 20 million users. Although typical WANs use essentially the same hardware and software as the Internet uses, the two networks have radically different security profiles.

Within your own corporate WAN, the main security goal should be protecting your links from outsiders. A pair of link encryptors will encrypt your data as it leaves one location and unencrypt it when it arrives at its destination.

Link encryption scrambles data at transmission time, then unencrypts and reencrypts it at every network node, such as routers or servers. The process is invisible to users. Link encryption does leave unencrypted data exposed within each network node, however. Select a different encryption key for each pair of nodes, so if an attacker compromises a single node, the rest of the system remains secure. Link encryption also encrypts header and routing information along with the data in each packet.

End-to-end encryption scrambles a message when it leaves the source and decrypts the data when the destination node receives it. End-to-end encryption never exposes unencrypted data, but may transmit header and routing information in an unencrypted form.

FIRE WALLS AND THE INTERNET Open yourself to the Internet, and you'll want tools that let you share data and use Internet services without creating vulnerability. A fire wall allows you to limit the kinds of services and data that flow between your internal network and the outside world. A fire wall is a secure computer that checks, routes, and labels all data traffic into and out of the organization.

Simple fire walls work with routers that use packet filtering. You specify which network services can cross from your internal network to the Internet and which ones can't. E-mail moves through TCP/IP port 25, but because bugs in the standard Unix mail program have been a common source of network attacks, prudent organizations block connections to port 25 on all other internal computers.

Your fire wall should completely block connections on UDP (User Datagram Protocol) port 2049 (which NFS uses) to prevent outsiders from mounting network disks and reading proprietary corporate files. Other good candidates for blocking are UDP port 69 (TFTP), 111 (RPC), TCP ports 79 (Finger), 109 and 110 (POP), and 540 (UUCP). If you don't know what a service is for, block it.

Got a hacker in Missouri who is trying to break into your machines? Once you know the IP address of his computer, program your fire wall to block all packets to or from his subnet.

The most sophisticated fire walls block all packets between your inside net and the outside world. These fire walls use programs called proxies that forward the services you've autho-

>>>CONTINUES ON PAGE 90>>>

The Players

Public-key encryption: It's the only choice

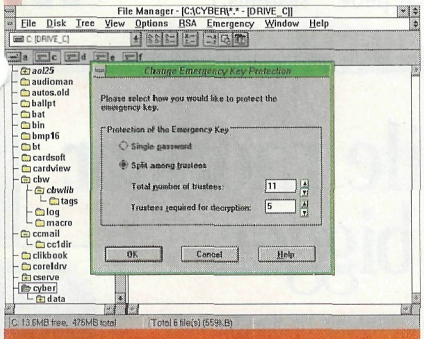
The undisputed leader in the field of link encryptors is Cylink. Cylink was the very first company to license the Diffie-Hellman public-key encryption algorithm, which exchanges a 56-bit DES key. Today, Cylink has a complete line of link encryption devices. Cylink's LSA Data Encryptor is a portable device the size of a hardback book that encrypts modems up to V.34 speeds. It comes in a tamperproof box, so you don't have to worry about industrial spies breaking it open and inserting a small radio transmitter while you're in the bathroom. At the other end of the spectrum are Cylink's 4200 Series devices, which can encrypt a T1 line. The company also has an AirLink microwave system for bridging LANs up to 30 miles apart. We had one minor complaint with the LSA system: It initially took 15 seconds to sync up because the system first sent the public key, then an encrypted session key, and finally, a digitally signed ID certificate. Subsequent connections were faster.

According to the Computer Security Institute, viruses and outsiders together account for less than 7% of all corporate data losses. Above are the real causes of corporate security problems.

The Players

Recently, Cylink began using the U.S. government's Digital Signature Standard (DSS) for authentication. With DSS, each user has a private key for signing electronic documents and a public key for verifying them. Users distribute the keys in X.509 certificates and then sign them with other keys. After establishing the encrypted link, Cylink's routers use DSS to sign the 512-bit Diffie-Hellman session key. This effectively eliminates man-in-the-middle attacks.

Adding a pair of encrypting routers or bridges will let your organization use the Internet as an alternative to a large-scale WAN without compromising your security. Semaphore Communications Corp. makes a set of bridges that provides centralized management over encrypted links; it uses a combination of RSA and DES for more secure encryption. The system consists of two components: the WG-3013 Network Encryption Unit-Workgroup (an AUI Drop Cable, a data key, and three batteries) and an IEEE 802.3 network interface (Ethernet).



RSA Secure lets you encrypt files and directories either manually or automatically at start-up and shutdown. You can create one emergency access key or several keys a user must recombine to access the encrypted data.

These multiprotocol bridges handle both IPX and AppleTalk in addition to IP. The WAN software includes secure frame relay, X.25, and ATM. But remember, these bridges are no substitute for a fire wall. In fact, by design, they turn off encryption when you're communicating with an insecure network.

Want to build your own fire wall? Then be sure to get a copy of the fire wall bible, *Firewalls and Internet Security: Repelling the Wily Hacker*, by William R. Cheswick and Steven M. Bellovin. Based on Cheswick and Bellovin's experiences building the fire wall at AT&T Bell Labs, this book is big on detail, but it assumes you have access to your fire wall software source code.

After you read the Cheswick and Bellovin tome, FTP to FTP.TIS.COM and pick up a free copy of the Trusted Information Systems' fire wall toolkit. You'll find it in the pub/fire walls directory. The toolkit relies on proxies, which run on a computer that bridges both internal and external fire walls. The proxies sit between the network client on the desktop and the server on the Internet and mediate all communications. If you're looking for a low-end NetWare product that does this trick, check out Instant Internet, which filters out all external TCP/IP traffic. It supports IPX/SPX and NetBIOS, so IS administrators don't have to invest in TCP/IP to gain Internet access from their NetWare LANs.

If you're not ready to build your own fire wall, Trusted Information Systems sells one—with its own hardware and a software service contract. TIS offers the software (Gauntlet 3.0), including source code, so you can examine the system and verify it does what you want. This package requires a C compiler and a dedicated machine to install it on. If you're a corporate user, choose Gauntlet over the downloadable free toolkit we discussed above.

We found Gauntlet more than adequate for most corporate users. Gauntlet 3.0 features completely transparent (no programming required) proxies, fire-wall-to-fire-wall encryption, and user permissions—and it detects and rejects IP spoofing attacks. Gauntlet software sells for $15,000. The company also sells a SunOS software-only version for $11,500, for customers who want to provide their own hardware.

Once you get your network secured, you can use a new program called SATAN, which you can download from the *Windows Sources* Web page, to simulate an attack on your own machines. Try using SATAN from both inside and

>>>CONTINUES ON PAGE 92>>>

The Primer

>>>CONTINUED FROM PAGE 88>>>

rized through the barrier. You'll need client software on your internal network that understands how to use these proxies. Both NCSA Mosaic and Netscape Navigator, among others, have the smarts for this.

You can save money by doing away with your own corporate WAN and using the Internet exclusively. And you can even do this securely with an encrypting router, which automatically encrypts packets you send between your sites but ignores information bound elsewhere.

Be wary of fire walls or authentication systems that base their security solely on IP addresses. Computer criminals use a technique called IP spoofing that lets them send IP packets with forged information. This is the trick that allowed Kevin Mitnick to break into several computers earlier this year and steal thousands of credit card numbers.

Finally, if you do connect with the Internet, be sure that attackers can't create security holes with your network's remote management system. IPng, the new version of IP, will use some form of public-key cryptography to tighten up security (existing SNMP management schemes have very little). IPng promises to deliver improved management and data security facilities. (In the future, you'll be able to use the IPng protocol to do many of the things that people now do with SNMP-based systems.) ■■■

Jargon

DES (Data Encryption Standard) A widely used encryption standard, DES uses a 56-bit key and provides reasonable security, as long as you aren't encrypting transactions worth millions of dollars.

RC2, RC4 Dr. Ron Rivest wrote these two encryption algorithms, each of which uses a variable-length key that can be as long as 1,024 bits. The U.S. State Department allows the export of programs with RC2 or RC4 with key lengths of 40 or fewer bits, so you know that this method isn't very secure. RC2 is a block cipher; RC4 is a stream cipher.

IDEA (International Data Encryption Algorithm) IDEA uses a 128-bit key and appears to be quite secure; PGP uses this bulk encryption algorithm.

IPng (IP Next Generation) The Internet Engineering Task Force (IETF) developed this enhanced Internet Protocol, which improves data security and increases Internet addresses from 32 bits to 128 bits.

The Players

>>>CONTINUED FROM PAGE 89>>>
outside your fire wall. You can also monitor your internal network for packets from the outside that are using forbidden internal services. You can program most LAN analyzer programs, such as FTP Software's LANWatch 4.0, to alert you when such packets show up. We ran LANWatch from a Web browser, attacked a machine on our internal network, and didn't find any security holes. Dan Farmer (SATAN's father) tried the same thing; he didn't get in either.

Finally, set up the freeware program Tripwire on all your internal machines. The first time you run it, Tripwire creates an MD5 checksum for most of the security-critical files on a Unix host (either your fire wall or Internet server). The next time you run it, Tripwire identifies modified files. If you're the unwitting host (read: victim) of a hacker, any altered files will stand out like sore thumbs. Of course, you'll need a C compiler, and the current version's programming requirements lean heavily toward the skill sets of Unix gurus. An NT version is reportedly in the works.

Novix for NetWare 2.2 lets NetWare LAN administrators connect to the Internet without investing in TCP/IP. Novix provides fire wall support, which blocks TCP/IP traffic at the gateway system while letting PC users access host computers running TCP/IP. The system supports SMTP, telnet, FTP, and other applications. Novix clients share a single IP address. Novix integrates NetWare security, including access rights, and lets IS directors use TCP/IP for NetWare LAN to NetWare LAN connectivity.

Fire walls that scan for viruses don't work because much data travels compressed. A rule to remember: If you are going to compress it, then you probably shouldn't encrypt it. Compression depends on patterns in the data, and an encryption algorithm tries to avoid creating patterns. These two data-management technologies thus work at cross-purposes. Compressed data is the easiest data to decrypt because the compression patterns are easy to spot. ■■■

Firewalls and Internet Security: Repelling the Wily Hacker, by William R. Cheswick and Steven M. Bellovin, $26.95, Addison-Wesley, 1 Jacob Way, Reading, MA 01867; 800-447-2226; fax, 617-944-9338. *reader service card 023*

Gauntlet 3.0, $25,000. Trusted Information Systems, Inc., 3060 Washington Rd., Glenwood, MD 21738; 301-854-6889; fax, 301-854-5363. *reader service card 025*

Instant Internet, $3,495. Performance Technologies, 7800 Interstate 10 W., San Antonio, TX 78230; 800-784-4638; fax, 210-979-2002. *reader service card 024*

LANWatch 4.0, $1,200. FTP Software, Inc.,100 Brickstone Sq., 5th fl., Andover, MA 01810; 800-282-4387; fax, 508-794-4488. *reader service card 027*

LSA Data Encryptor, $295. Cylink Corp., 910 Hermosa Ct., Sunnyvale, CA 94086; 800-533-3958; fax, 408-735-6643. *reader service card 021*

Novix for NetWare 2.2, 5 users, $1,425. Firefox, Inc., 2841 Junction Ave., Suite 103, San Jose, CA 95134-1921; 800-230-6090; fax, 408-321-8311. *reader service card 034*

SATAN, freeware. http//www.zd.com/~wsources.

Tripwire, freeware. ftp://coast.cs.purdue.edu/pub/COAST/Tripwire.

WG-3013 Network Encryption Unit-Workgroup, $3,995. Semaphore Communications Corp., 2040 Martin Ave., Santa Clara, CA 95050; 408-980-7750; fax, 408-980-7760. *reader service card 022*

The Skinny

Develop an attack strategy, then *use it*

You can boost productivity and cut costs with the Internet, but unless you develop a strategy for dealing with attacks, security holes can cost you more than you'll save.

The safest way to use the Internet is to avoid connecting it to your company's internal network. Instead, set up special PCs for Internet mail, file transfer, and Net surfing. Put the machines in special rooms and don't allow anybody to take floppy disks in or out; that's what the National Security Agency (NSA) does.

If you don't need to be as secure as the U.S. government, accept the fact that you're taking on risk. Reduce that risk as much as possible by creating strong barriers between your company's network and the outside. You can program most routers to create simple fire walls with packet filtering. Program your fire walls to let employees connect to the outside world but prevent outsiders from getting in by creating rules that examine the TCP/IPO ACK bit.

Don't, however, rely solely on a packet filter: Build a full fire wall with an impassable host PC. Monitor that host for break-ins and try to break into it yourself. If you're on the Internet, expect an attack; it's inevitable.

The best security is both transparent to your users and impossible to turn off. But if you make things too difficult, users might try to end run your fire wall by buying an Internet SLIP or PPP account from an outside vendor. That can spell disaster for a fire wall, because many SLIP implementations will happily route packets from the Internet to your LAN. Educate your users, but monitor your network for packets that you can't explain. ■■■

ON THE WIRE

The Primer

Talking? Someone's probably listening

OPENING YOUR COMPANY'S voice and data networks for external wireless and wireline access creates two potential problems. The first is that people will eavesdrop on your users, learning confidential details about your business and potentially discovering the passwords and access codes employees use to connect to your network. The greater risk is that an attacker will move beyond mere eavesdropping and use those codes to access systems, steal more-confidential material, and even maliciously delete files, change documents, or plant viruses in your computers.

Conventional phone lines are subject to both passive and active taps. Passive taps are those in which an intruder monitors conversations and electronic transmissions. Active taps are more serious, because the intruder actually modifies the information, changes its routing, or compromises its authenticity. Secure phones can help eliminate these problems, because they use encryption to render conversations unintelligible to anyone listening in.

Strong encryption will protect your communications while they are in transit. And strong authentication systems will prevent outsiders from masquerading as your employees—even if intruders manage to learn the necessary telephone numbers and passwords. A message-authentication system guarantees that the data you receive is the same as the original.

Cellular telephones and modems have created new vulnerabilities, because anyone with a scanner can tap into your signal. Just ask Prince Charles.

SCRAMBLE IT The only way to protect yourself against eavesdropping is to use encryption. That's partially why the Clinton administration wants you to use its Clipper chip, which employs an extremely secure 80-bit secret-key encryption algorithm. The Clipper is already beginning to show up in a variety of products, but there's a catch: Each chip has

>>>CONTINUES ON PAGE 96>>>

The Players

Block intruders at every entry point

SafeComm Link for Windows, from Cylink, provides a software-only implementation of Cylink's link encryptor. Cylink's products authenticate your identity to the system by using the government's Digital Signature Standard (DSS) and X.509 certificates when you log on.

We feel that this version is more than adequate for most business needs. SafeComm's great in an environment where you run Windows laptops, because it's compatible with CrossTalk, ProComm, and cc:Mail Mobile.

Axent Technologies' SecurExchange works with most popular Windows mail packages, including MS Mail and cc:Mail. It uses RSA public and private keys to encrypt mail and identifies the user with certificates that include the user's public key. Once SecurExchange had notarized our certificate, we used it to open all our user accounts. After finishing this process, we could exchange mail with other users who had valid public-key certificates.

AT&T's SecretAgent attaches a digital signature to network files that renders them unreadable unless the recipient has the right key. Users encrypt files with public keys, but they can initiate the actual encryption and decryption processes only with their private keys.

Try PGP, a popular program for encrypting electronic mail. PGP uses RSA to exchange keys and IDEA to encrypt the messages themselves.

ViaCrypt has a version of PGP that works directly with CompuServe's WinCIM. This version lets you automatically encrypt e-mail messages as you send them to CompuServe and decrypt them on receipt. This is a welcome change from the shareware version, in which you have to manually activate PGP after you create a message. ViaCrypt also sells a version of PGP that works with the National iPower Data Security Card.

>>>CONTINUES ON PAGE 96>>>

The AT&T Surety 3600s. This phone uses a Clipper chip for encryption. That chip protects your calls from wiretaps by everyone but the government. It actually improved the sound quality of our noisy long-distance call.

PHOTOGRAPH BY DARIA AMATO

The Players

>>>CONTINUED FROM PAGE 96>>>

these products regularly.

AT&T's Surety 3600s telephone-security device connects between your telephone's base and handset and contains a bidirectional 4,800-Kbps modem, which allows duplex conversations. The 3600's best feature is its quality: It sounds almost as good as being there. In our tests, the 3600 actually improved the sound quality by eliminating background noise.

If you want secure authentication only, consider Security Dynamic's SecurID card. Choose the version with the keypad: It encrypts first, then sends your password. Security Dynamics will probably have incorporated SecurExchange 2.0 support for Windows NT Remote Access Server into its SecurID hardware key.

Digital Pathways also makes a handheld SecureNetKey. The Key is actually a card with a small keypad. You type in your PIN, as well as the host computer's challenge code, and the SecureNetKey displays your response. We typed the wrong PIN five times in a row, and the SecureNetKey locked us out for good. Digital Pathways also offers a software-only version that runs on a PC, useful if you don't need the extra security of the card. ■■■

AquaFone 1.0, $129. Cogon Electronics, 310 Broadview Ave., Suite 202, Warrenton, VA 22186; 800-418-1482; fax, 703-347-9768. *reader service card 016*

AT&T SecretAgent 3.0, $149.95. AT&T Secure Communications Systems, I-85 and Mt. Hope Church Rd., P.O. Box 20048, Greensboro, NC 27420; 800-203-5583; fax, 910-279-5140. *reader service card 012*

Lotus Notes 3.3, 50 or more, $275. Lotus Development Corp., 55 Cambridge Pkwy., Cambridge, MA 02142-1295; 800-343-5414; fax, 617-693-3512. *reader service card 014*

Nautilus, freeware. ftp://ftp.csua.berkeley.edu/pub/cypherpunks/nautilus.

PGP 2.62, freeware. ftp://net-dist.mit.edu/pub/PGP/pgp262dc.zip.

PGP 2.7, $125. ViaCrypt, Inc., 9033 N. 24th Ave., Suite 7, Phoenix, AZ 85021-2847; 602-944-0773; fax, 602-943-2601. *reader service card 013*

SafeComm Link, $395. Cylink Corp., 910 Hermosa Ct., Sunnyvale, CA 94086-4103; 800-533-3958; fax, 408-735-6643. *reader service card 010*

SecureNetKey, $60 per user. Digital Pathways, Inc., 201 Ravendale Dr., Mountain View, CA 94043; 800-344-7284; fax, 415-961-7487. *reader service card 020*

SecurExchange 2.0, 10 users, $495. Axent Technologies, 20 Traff Sq., Nashua, NH 03063; 603-886-1570; fax, 603-886-1782. *reader service card 011*

SecurID, $34 per card; SecurID for client and server software, $1,950. Security Dynamics, Inc., 1 Alewife Ctr., Cambridge, MA 02140; 617-547-7820; fax, 617-354-8836. *reader service card 019*

Surety 3600s, with the Clipper chip and five handset modules, $1,295. AT&T Secure Communications Systems, I-85 and Mt. Hope Church Rd., P.O. Box 20048, Greensboro, NC 27420; 800-203-5583; fax, 910-279-5140. *reader service card 018*

WanderLink 1.0, single user, $295; 10 users, $1,695. Funk Software, Inc., 222 Third St., Cambridge, MA 02142; 800-828-4146; fax, 617-547-1031. *reader service card 015*

The Skinny

Encrypt and authenticate the lot, or pay

Classic computer security dogma recognizes three ways a person can authenticate themselves to a computer: through something that the user knows (such as a password), something that the user has (such as a smart card), or something unique to the user (such as a fingerprint). But these days, most companies rely on only the first two strategies.

For years, companies have protected their equipment with simple passwords and dialback modems. Unfortunately, passwords are easy to steal or learn. Dialback modems, meanwhile, are useless for a highly mobile workforce. In addition, an intruder can fool a dialback modem, so we recommend installing separate dial-in and dial-out lines and modems. Even if an intruder spoofs the dialback modem into seeing a properly connected line by holding the line open, the modem won't connect the intruder, because it can't dial out on that line.

That leaves smart cards, software-based challenge-response systems, and nonreusable passwords as the only reliably secure ways for companies to protect their servers while still allowing dial-in, wireless, and Internet access. With these systems, a wiretap doesn't matter, because the same code will never work twice. Remember, most secure, nonreusable password strategies require users to know some element in addition to the one-time password. Ultimately, user awareness, coupled with a strict security policy and rigid safeguards, offers the best strategy for protecting communications.

Ideally, the computer industry will adopt uniform standards to secure and authenticate communications for telephone, wireless, and other forms of remote access. Unfortunately, the U.S. government's export restrictions on cryptography are blocking these efforts, because companies are loathe to adopt a secure standard that's legal for use only inside the United States.

On the other hand, the government's export restrictions have created an easy metric to rate the strength of cryptographic products. If a product is okay to export, it probably isn't very secure. ■■■