THE SAFETY NET

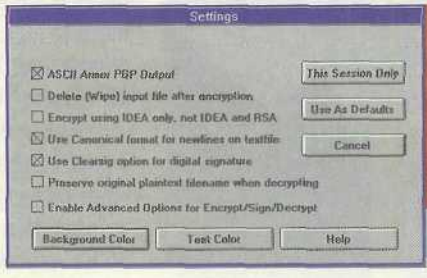
The Primer

Add security before you open for business

LAST year, Internet users got a wake-up call. Hackers had broken onto the net's busiest networks and installed *packet sniffers*. These programs picked up every Ethernet packet on the local-area network of key Internet routers. They then recorded the first two dozen characters (usually passwords and user names) that went over each telnet and FTP connection. No one knows how long the sniffers were running—weeks, perhaps, or months. The only reason anyone discovered these programs is that they stored the stolen account information in a file on the same computer that was running the packet sniffer: Eventually, the files filled the computer's hard disk and crashed the system.

KNOW YOUR ENEMY Today, the Net is still vulnerable, because it's still largely unguarded. Networks transmit unencrypted data. And practically anyone in the U.S., Europe, and Japan who wants an Internet account can get one. These two factors are fueling more and more security breaches. Some hackers break into systems to look around. Others take over modem connections and run up huge bills placing long-distance phone calls or intercept and alter e-mail messages.

Indeed, the very act of sending an e-mail message involves copying that message. Once the message arrives at the receiving machine, it waits in the /usr/spool/mail directory (in the case of a Unix system) or on the hard disk of the server running the post office (in the case of NT), where any intruder who obtains superuser (root) privileges can read it.



ViaCrypt's commercial version of PGP manages public and secret keys. In the settings dialog, you can select IDEA or RSA encryption.

Many system administrators react to such security breaches by pulling the plugs on their organizations' Internet connections. But there are less drastic alternatives.

AN OUNCE OF SECURITY A simple (but Draconian) way to counter password sniffers is to disable services requiring authentication, so you never have to type your password over the Net. Turn off access by telnet. Do not allow any use of FTP except anonymous FTP. Your users will still be able to use the Internet for e-mail, newsgroups, Mosaic, Gopher, and other services that don't require authentication.

A better approach is a *one-time password*. With this system, you use each password only once, so it doesn't matter if somebody else captures a password. Another kind of one-time system is *challenge/response*. With these systems, you carry a special-purpose calculator. When you try to log on, the computer prints a number. You type this number into the calculator and press a special button. The calculator performs a mathematical function unique for each user and then prints the result, which you send back to the computer. Again, someone tapping the conversation can't impersonate you, because they don't have the calculator.

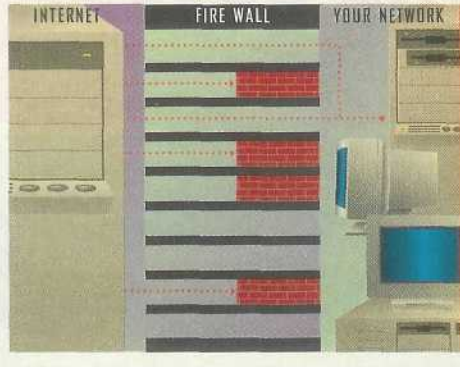
SCRAMBLED MEGS A third approach is encryption, which scrambles data you send over the Internet so it's meaningless to any listeners. Hardware or software can handle encryption.

Encryption can also solve another security problem: the interception of electronic mail messages. By using *public key encryption*, you can encrypt an electronic mail message so only the intended recipient can read it. Some messages (encrypted with the sender's private key) can be read by anyone possessing the public key, an approach that works well for broadcast messages. Most public key systems also provide a feature, *digital signatures*, that you can use to sign messages so recipients know the messages are authentic.

Stanford professors Whitfield Diffie and Martin Hellman invented public key cryptography in the 1970s. Most public key systems today employ the RSA algorithm, named for its inventors: Ronald Rivest, Adi Shamir, and Leonard Adleman.

With RSA, each person who wishes to exchange electronic mail creates two encryption keys, a *public key* and a *private key*. The public key encrypts messages; the private key decrypts them. To make your public key, the RSA encryption program randomly generates two large prime numbers hundreds of digits long. The program then bases the public key on a number it derives from the product of the two prime numbers; it bases the private key on the prime numbers themselves. This method works because it is easy to multiply two large numbers together, but it's difficult to take a large composite number and determine its factors.

PRETTY GOOD PRIVACY One of the most popular programs to implement RSA encryption is PGP, short for Pretty Good Privacy. To send an encrypted message with PGP, you create the message with a word processor



A fire wall is a router that acts as a packet filter. By changing values in the router table, you can filter packets based on such criteria as the time of day and the address.

Jargon

authentication A technique, such as using digital signatures, to verify the identity of users, hosts, and programs that try to gain network access.

fire wall A fire wall is software typically run on a dedicated server that blocks transmission of certain classes of traffic to secure internal LANs from the outside world.

public key Public-key encryption is a security technique that uses a public key and a private key. The public key, used to encrypt data, is published; the private key, which decodes messages, remains secret and is allotted individually. RSA is a popular encryption algorithm. To create a public key, the RSA encryption program randomly generates two prime numbers hundreds of digits long. It then bases the public key on a number derived from the product of the two prime numbers.

and save it in a file. You then encrypt the message with PGP's "-ea" (encrypt ASCII) options. PGP creates a file that appears to contain garbage. This is the file you send to your correspondents. When your correspondents receive the file, they process it with PGP, which decrypts the file and produces the original, intelligible version.

Although the principles of public key encryption have been around nearly two decades, it is not available in most e-mail programs. That's partly because the lack of standards for encrypting messages has prevented widespread adoption of the technology. Also, the RSA algorithm is patented: To use RSA, software developers need to negotiate a license from RSA Data Security. Another reason few mainstream e-mail packages incorporate RSA encryption is that it's difficult to manage and distribute keys. One notable exception is Lotus Notes, which uses RSA encryption to encrypt e-mail as well as communication between Notes servers.

One final note: Encrypting data that goes over a fire wall (see below) foils such passive attempts to compromise security as eavesdropping. However, it does little to deter active attempts in which hackers intercept and alter messages.

JUMPING OVER FIRE WALLS Just as a physical fire wall prevents the spread of fire from one part of a building to another, a network fire wall is a software barrier that blocks the flow of information from one part of a network to another. Network administrators can configure fire walls, deciding which type of messages to block and which to let pass. For example, a fire wall might allow computers on the Internet to send messages only to a particular, specified computer on your company's local-area network.

You can program most routers to do simple packet filtering, the most basic fire wall. Unfortunately, vendors deliver routers with all filtering turned off. You must decide which Internet services you wish to offer, then program your router to block packets for everything else. At the very least, be sure to disallow UDP packets destined for the port 2049 that the network file system (NFS) on computers running Linux uses. If you are connecting to the Internet with a SLIP or PPP connection with a computer running Unix or Linux, edit your configuration files (especially /etc/inetd.conf) to disable the services you don't want to offer.

If you aren't up to installing a fire wall, consider a *TCP wrapper*. A wrapper is a program that intercepts network connections to your computer, records the connection's origin, then completes the connection to the appropriate network server. Your administrator can set up a table that blocks access to particular services from a given host or network. ■■■

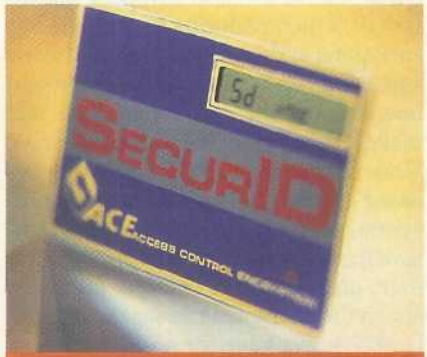
The Players

Security choice depends on your budget and expertise

You can program most routers to do simple packet filters. To build a more sophisticated fire wall, consider Trusted Information Systems' fire wall kit. The kit contains several *network proxies*, programs that run on the bastion host that forwards information from your internal hosts across the fire wall and on to the Internet. These programs log every transaction. Configuration files also let you block particular services or hosts. This is a sophisticated system, and you need to be well versed in Unix to get it to work. The less adventurous can buy a commercial version of the system, Gauntlet, for $15,000.

A Real Card To offer your users secure remote access by modem or over the Internet, consider SecurID, which uses credit card–size smart cards. Each smart card displays a number that changes each minute according to a predefined algorithm. When you try to log

>>>CONTINUES ON PAGE 140>>>



For safe remote Internet access, SecurID smart cards work with either Security Dynamic's ACE/Server software or one of three Access Control Modules (ACMs).

JEFFREY KREI

Which 17" monitor is the best value?

Typical "value priced" monitor

VisionMaster 8617A

Same size. Similar price. But "value priced" monitors just don't measure up to VisionMaster.

What does value really mean? In 17" monitors, what big-name manufacturers try to pass off as their "value line" usually comes up rather small.

3 YEAR WARRANTY

Because while value-line monitors often have an attractive price, their features aren't much to look at. Higher dot pitches, lower refresh rates and lower warranties can make a 17" "value" monitor a big compromise.

Not so with VisionMaster. The 8617A has a price comparable to the value lines, with high-end monitor features. Like an incredibly fast 80 Hz vertical refresh @ 1280 x 1024 resolution for crystal-clear, flicker-free images. Three color temperature controls and Colorific® color matching software. A base three-year and optional VisionCare warranty which ensures 48-hour delivery of a replacement monitor.

VisionCare

MPR II low-radiation certification. And VESA DPMS EnergyStar compliance.

So compare the 17" VisionMaster 8617A with "value" 17" monitors. Once you take a closer look, you'll find that value without performance is no value at all.

No monitor beats the 17" VisionMaster*

	VISIONMASTER MF-8617A	NEC XE17	VIEWSONIC 17G	MAG DX17F
SCREEN SIZE	17"	17"	17"	17"
DOT PITCH	0.26	0.28	0.28	0.26
MAX RESOLUTION	1600 x 1200	1280 x 1024	1280 x 1024	1280x 1024
MAX. REFRESH @ 1280 x 1024	80Hz	60Hz	60Hz	60Hz
COLOR MATCHING	YES	YES	YES	NO
POWER SAVING	YES	YES	YES	YES
WARRANTY PARTS/LABOR	3YRS/3YRS	3YRS/3YRS	3YRS/1YR	3YRS/3YRS
MSRP PRICE	$799	$1,060	$945	$729

For more information or the reseller nearest you, call today at 1-800-298-4335.

VISIONMASTER™

iiyama

iiyama North America
650 Louis Drive, Warminster, PA 18974
In Canada, call A. Crawford Assoc., 905-890-2010.
Outside the U.S., call 215-957-6543.
Fax 215-957-6551.

* Prices effective 12/1/94.

The Skinny

>>>CONTINUED FROM PAGE 140>>>

a job solely for do-it-yourselfers. Computers should assume you want security when you power on and automatically set up such methods as fire walls and one-time passwords.

In the meantime, you've got to ask yourself two key questions: What information do you need to store on the computer connected to the Internet? And what would happen if somone broke into that computer and copied or trashed all its files? Remember, if an Internet gateway lets users access Internet services from their desktops, then every computer in your organization is on the Net. People in Vermont logging on to a computer in San Francisco could have their passwords stolen, simply because the data passed through a computer in Cambridge, Massachusetts, on a LAN someone had compromised.

SECURE STRATEGIES If you want to publish Internet information about your company, put a computer on the Internet but don't connect the computer to your internal LAN. If you want your users to exchange e-mail on the Information Highway, invest in a good fire wall. And don't let users log on to your computers from the Net unless you set up a one-time password system. Finally, if you have two offices that need to exchange mail over the Internet, encryption is essential. Otherwise, outsiders could be collecting and tabulating your data, and you'd never know until it was too late. ■■■

TECHNOLOGY	PROS	CONS
DIGITAL SIGNATURE	Authenticates sender and message content.	Doesn't scramble messages.
MESSAGE DIGEST	Appends a one-way authentication code to ensure messages aren't altered en route.	Doesn't scramble messages and doesn't authenticate the sender.
PUBLIC-KEY ENCRYPTION	By relying on one public and one private key, you can distribute the public key without compromising secrecy.	RSA, the prevailing standard, takes longer to encrypt than DES.
SYMMETRIC KEY ENCRYPTION	DES, the prevailing standard, works faster than RSA.	Both recipient and sender share one private key.

Protect Your LAN

Building Fire Walls

Leaving your LAN unsecured is like leaving the office door unlocked.

An ounce of electronic prevention is worth a pound of cure. If your company's going to connect to the Internet, prevention takes the form of *fire walls*, electronic filters that secure internal networks from interlopers surfing the Net.

Fight Fire with Fire Walls The simplest fire wall is a *packet filter* you set up to prevent outsiders from accessing particular computers on your Internet network. These filters can prevent such services as remote log-on from gaining entry. You specify a filter in a table, which you edit on your system and then download to the router. The filter contains rules that specify the types of packets that can and can't pass through the fire wall. You can block packets based on the sender's address, the destination, the protocol, or the packet's port. For example, you might specify that any packet for TCP port 25 (SMTP) can pass. Or you might have your fire wall block all packets for UDP port 2049 (Sun's Network File System).

Electronic Sentinels More-sophisticated fire walls use a *bastion host*, a dedicated computer that handles all communication with the outside world. A bastion host usually runs a stripped-down version of Unix. It contains the few programs it needs to send information from one side of the fire wall to the other but lacks programs, such as a C-language compiler, that might be useful to a hacker. The fewer programs running on a bastion host, the less chance of an unidentified point of entry for interlopers.

Bastion hosts can connect to both the external and internal networks, thus performing the function of a mail and news gateway. They also work with packet filters you set up, so TCP/IP connections from the outside world can connect only to the bastion host, but computers on your inside network can initiate external connections. Particularly security-conscious sites should keep the bastion host on its own network and move information between networks with floppy disks and tapes.

Fire walls are not the be-all, end-all answer to security. While they let you focus security efforts on particular computers, fire walls are difficult to configure, and mistakes can leave an entire network vulnerable. But fire walls do let you block connections to services or hosts that are less secure and, in doing so, provide a comfortable degree of security.—**Simson Garfinkel**

STRAIGHT TALK

TALK IS CHEAP on the speech-recognition frontier. But getting the technology to work for you takes a supercharged PC and the patience to...talk...like...this.

by Don Labriola

Talking to a computer generally earns you puzzled stares rather than the respect of coworkers. But entering data, dictating memos, and navigating your favorite applications by voice poses an attractive alternative to the keyboard and mouse—an alternative that's rapidly becoming a reality as automated speech-recognition (ASR) systems make their way to our desktops.

All ASR systems operate similarly. You speak into a microphone; by the Nyquist Limit (a theorem that states that to accurately capture an analog signal you need a sampling rate of twice the frequency), a sample rate of 8 kHz to 10 kHz should be ample for capturing the 4,000 unique, significant frequencies that comprise speech. Once the ASR system has digitized your words, its software applies a reverse Fourier transform to the digitized data, mapping the frequencies in the digitized speech to discrete ranges, or vectors. These vectors represent phonemes, the basic sounds—such as "uh" or "ee"—that make up words.

The software then compares these phonemes against a set of prototypes. Variations in speech—such as inflection, pitch, and speed—cause deviations from the prototypes, so most systems also apply a Hidden Markov Model (HMM) to more accurately guess the identity of a given phoneme. In essence, to estimate the probability of a phoneme match, the HMM combines its guess about the present phoneme with the probability that this phoneme follows the preceding one in normal speech .

This Year's Model Products differ in their approaches to the first part of the process—how they implement noise cancellation techniques, for example—but most of the diversity in products occurs at the language modeling level. The language model determines whether a product falls into one of two broad categories. Large-vocabulary systems use N-gram modeling, a technique analogous to HMM in which N represents the number of words a system looks at (usually two or three) to guess the probability of a word match. These systems can usually recognize from 10,000 to 35,000 words. They most often function as dictation systems for doctors and attorneys.

Small Is Beautiful Small-vocabulary systems, on the other hand, understand only a few hundred words at a time. They may use N-gram models but more likely will use finite-state grammars. With a limited set of words to choose from and a constrained set of relationships among these words, these systems are often just right for command-and-control (C&C) applications.

With few exceptions, most of today's desktop ASR products handle only discrete speech input. Not surprisingly, this diminishes the enthusiasm of many potential converts. Our experience with Verbex's Listen 2.0 for Windows, a small-vocabulary C&C program, and two large-vocabulary products, Kurzweil Applied Intelligence's Voice 1.0 for Windows and Dragon Systems' DragonDictate, indicates that ASR technology will take at least a few years to catch up with both the public's expectations and its needs. (IBM's VoiceType Dictation for Windows and Philips' Speech Processor 6200 were not ready to test for this story.)

Don Labriola, of Solution Technologies, Ltd., writes and speaks frequently on telephony technology.

ILLUSTRATION BY [illegible] WEBER