Deborah S. Ray
and Eric J. Ray
Editors

Network Security and Technical Communicators: Background, Risks, and Responsibilities

This column examines emerging technologies of interest to technical communicators to help them identify those that are worthy of further investigation. It is intended neither as an endorsement of any technology or product, nor as a recommendation to purchase. The opinions expressed by the column editors are their own and do not represent the views of the Society for Technical Communication. All URLs and site contents were verified at the time of writing.

When you leave your house, do you leave the door open? When you leave to go on vacation, do you leave doors and windows unlatched or unlocked? Is your company's or client's worksite generally open for anyone off the street to wander through? Have you ever allowed anyone unknown to you to borrow your car to go joyriding or to use your home as a base for illegal activities? How many strangers have you given the keys to your home, or access to your confidential information?

Clearly, the answers to these questions are no, no, no, no, and none. But, as technical communicators, we often expose our Internet-connected computers to the same risk and vulnerabilities for crackers—people who maliciously break into computers (called *cracking*)—to come along and access our files, explore our computers, screencap what we're working on, swipe files, plant files, reboot our computers, and do so without our even knowing we've been victimized. Without even realizing the consequences of what we're doing, we often leave our computers wide open, as much so as a house with unlocked doors and windows, and risk being directly attacked, burglarized, ransacked, vandalized, or used as the vehicle for an illicit joyride.

As we'll show you, computer cracking these days is surprisingly easy to do . . . and all too common. In fact, during the course of writing this article, we set up a program to warn of other computers probing or attempting to hack one of our Internet-connected computers. Within the first five hours, we logged three separate attempts to access the computer, and we have logged five to eight attempts per day since then. And remember, these are just cracking attempts on one computer, at our small company, located in the basement of our home.

Because technical communicators often work with and develop confidential and proprietary information, we need to understand how we may be targeted and take steps to minimize security risks. In this consciousness-raising article, we explain why technical communicators face security risks, explore the basics of Internet communications, explain how computers are cracked, explain what crackers can do on your computer, and offer tips and resources for protecting yourself against crackers.

WHY ARE TECHNICAL COMMUNICATORS AT RISK?

As technical communicators, we may imagine ourselves as facing little risk of being victimized by computer crackers; however, we do face unique risks just by the nature of the information we write and resources we use, as well as our work environments and habits. At a minimum, we are exposed to the same risks of cracking as other people, in other professions, in any number of unprotected at-home or at-office environments simply because we're using Internet-connected computers. Although computer cracking attacks are generally random and do not often target specific people, companies, or information, the risk does exist.

Consider, though, the types of information we deal with on a day-to-day basis. Many of us access proprietary company resources, documents, files, and data, and we often compose documents and other resources that are proprietary until released. For these reasons, we need

to pay special attention to security risks and take steps to minimize them.

Additionally, technical communicators face a unique risk of being hacked because of our work environments and habits. For example, rather than always working in one office in one location where security measures are in place, many of us occasionally or regularly work at secondary locations, such as satellite offices or home, where often no specific security measures exist. Whereas our computers at the office may be protected through firewalls and intrusion-detection monitors, our secondary work locations often do not have such protection. For example, we e-mail our files from work to home (or perhaps shuttle files home via diskette) and access those files using unprotected computers, and then often leave the files there for use at a later time. Doing so puts the files and the information they contain at risk by simply being on an unprotected Internet-connected computer. Compounding the risk is the fact that while working in these secondary locations, we often stay connected to the Internet for extended periods of time using Internet connectivity, such as cable modems, ISDN, or DSL—technologies that increase the likelihood of being hacked simply because the computer is online, available, and not specifically protected.

Additionally, many of us work collaboratively with others, a fact that can increase security risks too. For example, as we'll explain later in this article, receiving files from other people—either attached to e-mail messages or downloaded from FTP or Web sites—puts us at risk of receiving *Trojan Horses (*also called *Trojans).* These seemingly harmless executable programs are often undetected by anti-virus software, often look like nothing more than defective files that didn't actually run, or often provide fun or useful services; however, they can actually harm your computer and files or allow crackers access to your computer. Incidentally, it was Trojans that were used in the spate of Distributed Denial of Service attacks on high-profile Internet sites in early 2000.

All these factors—working in nonsecure secondary locations on unprotected computers, being online for extended periods of time with nonsecure connections, and sharing files with others—put technical communicators at particular risk of being victims of computer cracking.

HOW DO CRACKERS FIND AND ACCESS OUR COMPUTERS?

You might be wondering, though, how crackers can actually break into your computer. To understand how crackers can find their way into your computer, you need to understand network structure, as well as how networks and computers connect. In the following sections, we'll explain Internet communication basics and demonstrate how crackers can find, access, and exploit your computer over the Internet.

Understanding Internet communication basics

The Internet and most intranets are essentially just networks of computers that have identifiable addresses, are physically connected, and have common communications protocols in place. Let's start with the Internet-connected computer on your desk.

The computer sitting on your desk has its own unique address that identifies it to other computers, much the same way that a house number identifies a house to people looking to find it. The address—a 32-bit Internet Protocol (or *IP*) address—is usually represented as four sets of numbers from one through 255, such as 192.60.22.1 or 10.23.43.12. These numbers, often called *dotted quads*, identify two pieces of information: the network the computer is on (the first three sections of quad), and the individual computer (the last section).

You're probably more familiar with IP addresses as locations you access on the Internet, such as www.stc.org. Such addresses are just a more readable and human-friendly format of the dotted quads that are linked to a specific number. For example, the address www.stc.org (a form that is more comprehensible to most humans) translates to the IP number 206.103.63.198 (a form that is easily readable to other computers). In many cases, each computer will have one IP number; however, when a computer has multiple names or network interfaces, it might have multiple IP numbers, such as 10.12.43.10 through 10.12.43.15. So, with its IP number(s) established, the computer now has an address that's available and identifiable to other computers on the network.

For your computer to communicate with other computers, though, specific network communications components need to be in place. Figure 1 shows a simplified diagram of the pieces that make network communications possible, called the *OSI (Open Systems Interconnection)* model. Reading this model from the bottom up, you can see how each communications layer builds on another.

As you can see in Figure 1, the OSI Model shows the components and devices that make up the physical connection, software that makes the network work, software and devices that transport data through the network, and software that you, the computer user, interact with. These layers provide the foundation for computers to communicate with each other using common devices, software, formatting, information transport, compatibility, interfaces, and functionality that can occur

Name	Function
Application Layer	Supports functions like e-mail and file transfer, and other applications
Presentation Layer	Provides control over screens (appearance) of communicated information
Session Layer	Provides capability for individual network devices to interact with other devices
Transport Layer	Provides control over the end-to-end communications carried over the network, including error checking and formatting the received data. On the Internet, this control is achieved with TCP (Transmission Control Protocol).
Network Layer	Routes or directs communications from one network device to another. On the Internet, this routing is achieved with IP (Internet Protocol).
Logical Link Layer	Includes device drivers and other software used to make the computer communicate with the network adapter cards
Physical Layer	Includes network adapter cards, cables, and physical connections

Figure 1. The OSI Model illustrates the components and devices that enable computers to communicate with each other.

between computers on the network.

You'll notice in the shaded Transport and Network layers that *TCP/IP* (*Transmission Control Protocol/Internet Protocol*) is what provides the common communications basis between the physical network components and the software and devices that you interact with. As the bridge between the two, TCP/IP makes installing and running network applications easy because you don't have to address configurations of individual computers. Instead, all the components share the same communications foundation. Using these common components, then, TCP/IP-aware applications (such as Web servers, mail servers, AOL's Instant Messenger, ICQ, and similar programs) can communicate with any kind of device running on practically any kind of physical network, including traditional cables (such as the local area network in your office), fiberoptic lines (such as long-distance Internet connections), and wireless connections (including, among other examples, the Palm VII handheld computers).

Understanding how TCP/IP affects computer security

Although TCP/IP does not directly create or contain security holes, it does provide an environment for problems to occur. As Figure 2 shows, TCP/IP supports a number of *ports*, which you might think of as available slots where applications (servers, specifically, like Web or mail servers) are installed and run within your computer. When running, these applications actively listen for incoming connections, essentially leaving the port open to incoming information that is routed to it. And, because each of these listening ports is open, each is a potential entry point into your computer. So rather than crackers having a single entry point into your computer, they actually have the potential to have as many entry points as your computer has running server programs. Because most applications these days are TCP/IP aware or have TCP/IP-aware components that listen for incoming connections (such as AOL's Instant Messenger or the Personal Web Server installed with most versions of FrontPage), the number of entry points—the number of possible cracking opportunities—on your computer can be high.

What's perhaps more significant, though, is how relatively easy it is for crackers to find and access these ports. While writing this article, we downloaded a freeware Windows-based port scanning program, called SuperScan, and scanned the IP numbers of the computers on our own network, as shown in Figure 3. Within just five minutes or so, SuperScan reported back how many computers we have running on our network, their IP addresses, and enough information that a cracker could reasonably guess which operating systems are installed.

Although these results may seem harmless, crackers can use such information to determine how to crack into your computer and determine what can be done once it has been cracked. For example, with operating system information gleaned from the port scan results, we then searched the Internet for operating system-specific cracking information and easily and quickly found scripts, programs, and step-by-step instructions that could walk a cracking novice through an attack. Using the scripts, programs, and instructions, we were able to crack computers on our own network and execute a number of harmful commands, such as ones that partially crashed the computers, increased CPU usage (making the computer so busy that it was unusable), decoded password files, ran

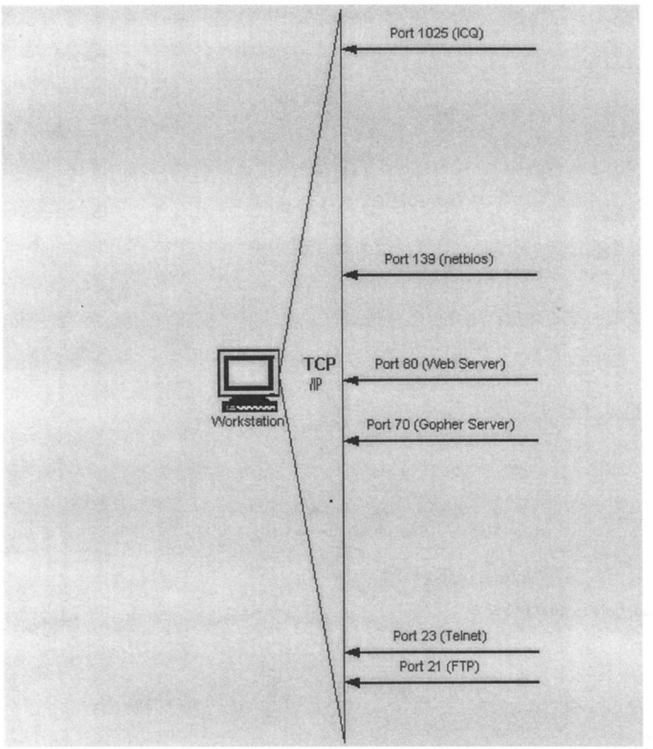

Figure 2. The TCP/IP stack supports a number of ports, which listen for incoming connections.

programs to read arbitrary files on the hard drive, and ran programs to execute arbitrary commands.

What's more, we were also able to plant Trojans on our computers. As we described earlier in this article, these programs are intended to do harm but are disguised as files you might open or use. For this example, we found a Trojan on the Internet that is designed to install itself on the computer and listen on a specific port, thereby providing an opening to a cracker. We downloaded the .zip file, unzipped it, followed the instructions, and then e-mailed it to a test account on our network. After receiving the e-mailed message with the .zip file attached, we double-clicked the attachment, saw an hourglass for a second or so, and then seemingly nothing happened. But with the double-click of this Trojan, a program was installed on the computer, with no obvious cues or clues to us that anything was installed. With our mail program, we had to double-click on the attachment for the Trojan to be installed; however, using other programs that automatically open attachments with the e-mail message (such as Microsoft Outlook), these Trojans could be automatically installed just by opening the e-mail message. After the program is installed and running, crackers from throughout the Internet can readily access and manipulate your computer, as shown in Figure 4.

These are just a few simple examples of what crackers can do once they gain access to your computer. With these and other more sophisticated and customized cracking programs available, computer cracking is a growing risk. In the few days that we spent testing our computers' security, we encountered several dozen attempted cracks. And we'd always thought our computers were fairly secure.

WHAT CAN YOU DO TO PROTECT YOURSELF AND YOUR DATA?

Protecting yourself against hackers is, in many ways, similar to protecting yourself against burglars, muggers, or other dangers: The first step is to simply make it easier for the cracker to move on to another target than to attack you. Of course, the complexity of computers, networks, and the Internet make this more complicated than just installing deadbolts and staying away from dark alleys; however, the same principles of being aware and taking precautions apply. The following tips and resources will help you keep your computer and projects secure.

Take precautions

- Use a firewall. A firewall can find and block port-scanning activities as well as prevent Trojans from communicating outside of your network. The firewall could be a 486-class computer running Linux, a dedicated firewall appliance from a good computer store, or any number of other hardware or software solutions. Even if you have only a single computer connected to the Internet, you should strongly consider a firewall as part of your overall security approach.
- Use anti-virus software regularly, scan all new or incoming files immediately, and keep your anti-virus software up to date.
- Know and trust the source of software that is sent to you or that you download. Look for

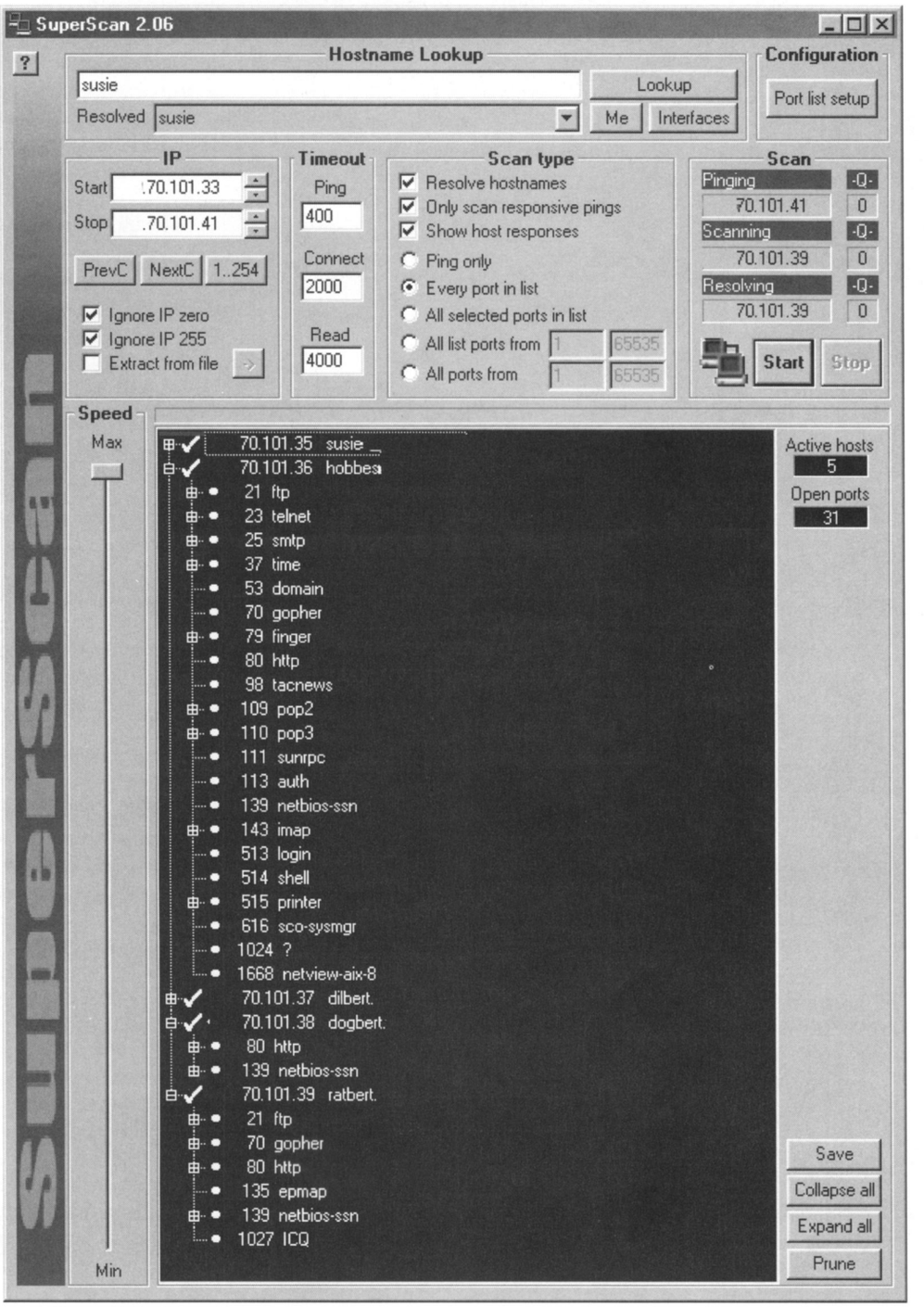

Figure 3. Available for free on the Internet, SuperScan provides a variety of ways to narrow port scans and target computers more precisely.

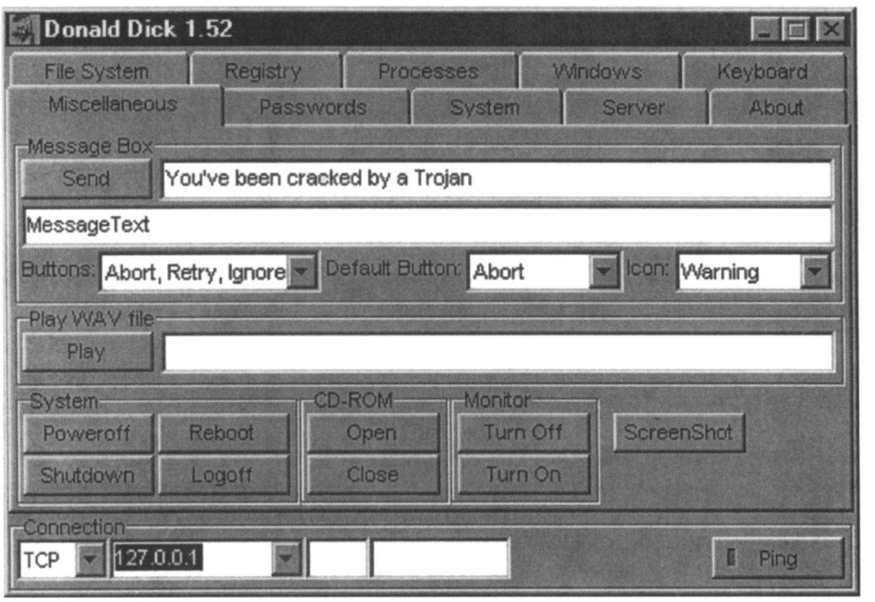

Figure 4. This Trojan program provides crackers with a dialog box of capabilities that act like a remote control to our computer.

cryptographically signed messages that verify the source of the information, or follow up with a phone call to the sender.

Keep yourself informed

- Monitor vendor sites, including the manufacturers of your operating system, Web browser, and e-mail programs, and immediately install any patches or upgrades that are available.
- Delay upgrades to closed-source programs (for example, anything from Microsoft or other traditional software vendors) as long as possible so that security holes are found and patched before you install the program and possibly make yourself vulnerable.
- Upgrade open-source programs (for example, Linux and similar community-development projects) as quickly as possible. Security holes in open source programs are often quickly found and fixed, so new versions tend to be more beneficial than dangerous.
- Monitor anti-virus sites, CIAC (Computer Incident Advisory Capability), and CERT (which originally stood for Computer Emergency Response Team) for announcements of problems or security issues that affect your operating system or software.
- Monitor hacker/cracker sites for information about exploits that affect your operating system or software.

Think like a cracker

- Find, download, and use network security products, including port scanners, intrusion detection software, and published exploits against your own operating system and software.
- Educate yourself about network security and the way that computers and the Internet work.

CONCLUSION

Although the Internet allows technical communicators to communicate and share information more effectively than ever before, it does introduce security risks. Technical communicators face a unique risk of becoming victims of computer crackers, not only because of the proprietary information we often use and create, but also because of the work environments and habits that tend not to have established security precautions.

As we described here, TCP/IP makes Internet information resources and work environment flexibility possible, but it simultaneously undermines the security of your computer and facilitates illegal computer cracking. Each TCP/IP port with a program that listens for incoming information (like Web servers or ICQ programs do) provides an entry point into your computer where crackers can explore and open files, find out what you're doing, and install Trojans, among many possibilities. Using the tips and resources provided here, however, you can minimize security risks by taking precautions, being informed, and thinking like a cracker.

FOR FURTHER READING

http://www.ciac.org/
Monitor the CIAC (Computer Incident Advisory Capability) site for authoritative information, warnings, and updates about security issues.

http://www.cert.org/
Monitor CERT (Computer Emergency Response Team) site, provided by Carnegie-Mellon University, which offers authoritative information about security issues.

http://www.nai.com/
Visit the NAI (Network Associates, Inc.) home page for virus, Trojan, and related security information.

http://www.norton.com/
Visit the Norton Anti-virus site for more security information.

http://www.AntiOnline.com/
Visit AntiOnline for a wide range of security and hacking information, including the Fight Back section, which is written in a very helpful Q&A format.

http://www.HappyHacker.org/
Visit the Happy Hacker site for information about how security precautions can be bypassed.

http://www.insecure.org/
Visit this site for a range of hacking information, as well as the Linux/Unix port scanning program nmap.

http://members.home.com/rkeir/software.html
Find SuperScan, a freeware Windows-based port scanner.

http://www.warforge.com/
Visit the War Forge site for additional computer cracking information.

http://www.networkice.com/
Visit this site for BlackICE, a popular intrusion detection system for Windows, as well as for very good advice and information about security.

ERIC J. RAY AND DEBORAH S. RAY are owners of RayComm, Inc., a technical communication consulting firm that specializes in practical applications of leading Internet and computing technologies. Together they have co-authored more than 10 computer books and previously wrote two syndicated computing columns, carried in daily newspapers throughout North America.

Deborah has been a technical communicator for nearly 7 years and has taught technical writing courses at two universities. In addition to writing about computer and Internet-related topics, she has also written, designed, and illustrated numerous engineering documents. She founded and currently maintains The Official TECHWR-L Web site, the Web site supporting the 5000-subscriber Internet discussion forum and the technical communication community worldwide.

Eric is a senior technical writer at Sun Microsystems. He has been a technical communicator for more than eight years, has done extensive consulting for clients such as Compaq Computer Corporation, MCI/WorldCom, and Sun Microsystems, and has served as technical consultant on numerous books, articles, and Web sites. He founded and currently maintains TECHWR-L, the oldest and largest Internet discussion forum for technical communication topics.