part i

General Security Principles

2

What, Me Worry?

Before we dive into the general principles you need to know about online security, we think it's best to start by answering a couple of questions that you may have.

The first is, "Do I really need to worry about Internet security?" In these days of intense media hype, it's easy to look at the never-ending parade of stories about hacked Web sites, denial-of-service attacks, and viruses and to wonder how much to believe. What's real, and what's made up? The second, related question is, "Why would anyone want to attack *my* machine?"

The answers to these two questions are simply, "Yes, you really do need to worry about online security" and "People want to attack your machine simply because it's there." We realize, of course, that you might not want to take our word for these answers. So consider some statistics.

More People on the Net More Often

Although the Internet has existed, in one form or another, since the 1960s, it was not until 1995 or so that it really started growing. Statistics on the total number of Internet users are, as you might expect, hard to come by, but the number of Internet hosts is much easier to ascertain.

An Internet host is a specific computer directly connected to the Internet, with its own specific Internet address (as opposed to one assigned from a pool).

The number of Internet hosts can be determined through what is pretty much a computer-driven census. Between 1995 and early 2001, this number grew from 5 million to more than 100 million. That's a growth rate of nearly 20 times in six years, or more than 50 percent a year (**Figure 2.1**).

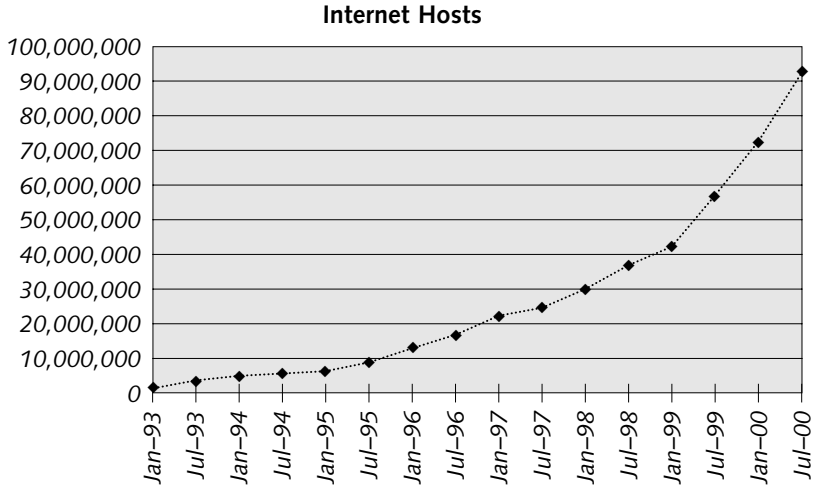

Figure 2.1 A look at the number of Internet hosts per year.

If you're interested in a more people-centric figure, the 100 million hosts in early 2001 translate to about 300 to 400 million users. And the trend is expected to continue. One study estimates that more than 600 million users will be online by the end of 2002 and more than 1 billion by 2005.

In addition to this rapid increase in the number of users, folks are staying online for longer periods of time. There are several

reasons for this, including that there's more to see and do on the Web than there was before. According to AOL, for instance, the average amount of time a user stayed on its system went up about 5 times between 1996 and 2000.

The main reason, however, why people are staying online longer—and certainly the one that's most relevant to security—is that many of today's high-speed connections allow users to remain on 24 hours a day, if they want. Nielsen/NetRatings estimates that the number of users on such high-speed connections in the United States more than doubled in 2000, to more than 11 million. We'll talk more about the many additional security ramifications of permanent high-speed connections later in this chapter, but they're causing the Net to be used a whole lot more by a whole lot more users.

More People Doing More Important Things

Just as more of us are online more often, the Net is becoming a more important part of our day-to-day lives. Many of us rely on e-mail as an essential form of communication. Some of us need the Net to do our jobs, either for an organization or for ourselves. Many businesses, such as Yahoo! and Amazon.com, could not even exist without the Net. So whereas in the 1990s, the Net was a requirement more for hobbyists and specialists, in the 21st century, the Net is essential for the rest of us as well. It's pretty much like water or electricity—we just can't do without it.

With the Internet, we have a utility that we have come to rely on and that is accessible by millions (soon to be billions) of people. The Net is not only accessible but also affectable. And for every million additional people on the Net, you know that so-many-thousand new hackers will try to affect things. Businesses and large organization have to come to recognize these facts, and most are taking protective measures, if somewhat belatedly. But the same realization has not yet trickled down to the rest of us.

We hope that these statistics, along with the rest of this book, will help convince you that all of us need to do whatever we can to make our online experience a safer one—and that in general, doing so is pretty easy.

More and More Attacks

When few of us were on the Net, few hackers were as well. And those hackers who were online didn't have much to hack. They generally went after machines running the Unix operating system, because Unix machines were more prevalent on the Net in the early days and were quite hackable.

To digress for a moment, most of you have probably heard the term "hacker." Although sometimes "hacker" just means "anybody who's good with a computer," it recently has specifically come to refer to someone whose computer skills are used to cause problems for others, usually over the Internet. That's how we're going to use the term in this book.

Even as the Internet began to grow from 1995 to 1998, the rate of hacker attacks remained relatively low. But recently, things have changed dramatically and the number of attacks has increased at a rate even greater than the number of users on the Net. It's not clear exactly what changed. Maybe the number of machines on the Net reached some sort of critical mass that made hacking worthwhile in the eyes of the hackers. Maybe the media glorified hacking to such an extent that it became "fashionable," especially for young people. Regardless, hacking is definitely on the rise. One good measure of this increase is the number of official security incidents reported by the CERT Coordination Center. The CERT (which at one time was short for Computer Emergency Response Team) Coordination Center is the major reporting center for Internet security problems.

As you can see in **Figure 2.2,** sometime around 1998, the incident rate starting increasing significantly, and it's been growing faster than the Internet ever since.

Exactly what an "incident" is and whether it's directly relevant to the rest of us are certainly valid questions. So here's a statistic that we believe will hit much closer to home (so to speak):

In a study performed by Open Door Networks on a typical Macintosh connected through the popular @Home cable network, during a 30-day period in early 2001, an average of eight unique unauthorized access attempts were detected per day.

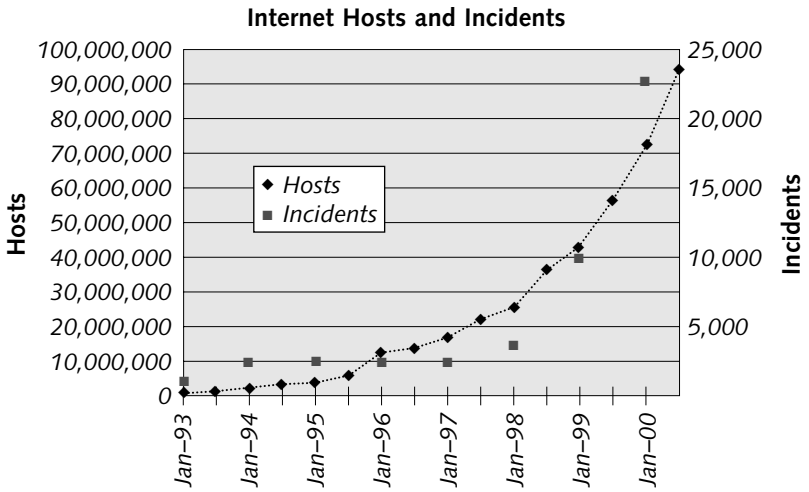

Figure 2.2 The rate of hacking incidents per year.

These access attempts weren't general incidents at some general Internet reporting center; they were specific access attempts made against a specific Macintosh on a widely used cable-modem Internet service. And this study, conducted by the authors, is backed up by many additional reports. At the January 2001 Macworld Expo trade show in San Francisco, during a network managers' forum, an audience member indicated that his newly installed firewall logged so many access attempts that he first thought that the firewall manufacturer was making up those attempts as a marketing ploy! And here's just one of the many reports that Open Door Networks has received on the subject:

"As is probably true with most of your customers, I have been astounded at how many unauthorized attempts to penetrate my computer there are."

Machines that the rest of us use on the Internet are getting attacked, and they are getting attacked at a significant and increasing rate. You do need to worry about online security!

Why Me?

We hope it's pretty clear by now that Internet security is an important issue even for the rest of us. But you still may be wondering why. Why would someone want to attack your machine if it has no secret documents, no Web site to deface, no credit-card numbers to steal (we hope)? What possible benefit could someone gain from accessing or destroying data on your machine?

These are all good questions. And they have two sets of answers. First, you may have more important data on your machine than you think. (We'll look at this issue in the chapter on the physical security of your machine.) But even if you're right about the lack of significant data on your machine (maybe all you do is play games), there is a second set of reasons why your machine is being attacked over the Net.

Here's the key point to realize about most access attempts on your machine:

No one is specifically targeting your machine.

You're right—pretty much no one cares about you in particular. Most hackers out there just want to break into *any* machine. Many are bored high-school or college students looking for a challenge. They want to be able to brag to their friends, "See? Look what I can do to this poor sucker's machine. Am I not cool?"

Being cool used to mean having a powerful car or being on the football team. Now, to a subset of the younger generation, it means being able to wreak havoc at long distance and to leave your mark. Hacking is (sometimes quite literally) the digital version of graffiti.

Another key point to understand is exactly how those access attempts to your machine are being made:

Almost all havoc-wreaking is done through prebuilt applications or scripts.

The havoc-wreaker doesn't need to be some geek who slaves away for nights on end on a specific application to go out and do his dirty work. He (and it usually is a he and a young he at that) simply needs to go to any of a variety of Web sites

and download any of a variety of applications or scripts. A simple double-click after that, and the hacker (or "script kiddie," as he's often called) is on his way.

But how does a script kiddie happen to end up hacking your machine? Again, why you? Pretty much because your machine was there, and it was your turn. As you'll see in the chapter on Internet basics, each machine on the Net has an address, just like a phone number. The hacker's script either picks Internet addresses at random or goes through them sequentially. The script uses various techniques to see whether there's a machine at that address and concentrates on address ranges that are more likely to have lots of vulnerable machines (such as the address ranges used by popular Internet providers). When the script finds a machine at a particular address, it moves on to try various built-in attacks against that machine. Those attacks usually are the ones that you'll see if you've added any sort of logging or monitoring features to your machine (see the chapters on analyzing security threats and personal firewalls for ways to do this). If any attack is successful, the script alerts the hacker running it or logs the machine's address to a file for future exploitation; otherwise, it moves on to the next address.

It may seem unlikely that of all the machines on the Net, yours is getting chosen at random eight times a day on average. After all, there are a hundred million machines. But remember that the rate of attacks is increasing faster than the rate of new users. A few years ago, lots of new users were getting on the Net but not lots of new hackers. Now the hackers are catching up. So with all those hackers running all those automated tools (on faster computers and faster connections), they just happen to hit your machine eight times a day! And if trends continue, the situation is just going to get worse.

It Gets Worse

For many reasons, you don't want a script kiddie, or anyone else, to gain access to your machine. These reasons are pretty much the same as the reasons you don't want anyone to gain access to your house. There also are less obvious, but equally important, reasons. The main one is:

You may never know that someone has gained access to your computer let alone what they're doing or have done with the access they've gained.

Some attackers just leave some sort of calling card ("Kilroy was here!") and don't do anything malicious. But other attackers are much more subtle. They may implant an invisible file or application (often called a *Trojan horse*) on your machine that could do all sorts of bad things at some unknown time. For example:

- The hidden application could spy on everything you're doing and then make that information available to the attacker over the Net. It could notice what Web sites you go to, for example, or read your e-mail along with you. Worse yet, it could copy the passwords you type to access Web services or steal the credit-card numbers you enter in supposedly secure Web sites.
- The hidden application could be used to launch an attack on another machine. Attackers often cover their tracks by launching attacks indirectly, through a series of machines, sometimes in different countries. Then, when someone comes looking for the attacker, they find you instead. Although you may not be legally liable for the misuse of your machine in this situation, we don't think any of us wants to have the FBI or other law-enforcement agencies knocking on our door.
- The application could be used in concert with similar applications implanted on other machines for more advanced, distributed attacks. The most popular of these is known as a *distributed denial-of-service attack*. Your machine, and hundreds or thousands like it, could be used in concert to flood a particular Web site with traffic, effectively denying the services of that Web site to

legitimate users. In February 2000, such an attack was launched successfully against several major Web sites, including Yahoo! and CNN. And the FBI did go around knocking on a lot of doors.

Broadband Connections Are Especially Vulnerable

Any machine connected to the Internet in any way is susceptible to a random attack at any time. But machines hooked up by increasingly popular broadband connections are more susceptible than most others. *Broadband* in general refers to any high-speed Net connection, but for the rest of us, it usually means a connection through a cable modem or DSL (digital subscriber line). The two key characteristics that make broadband links particularly vulnerable to attack are the same characteristics that make broadband connections so popular in the first place: They're connected 24 hours a day, and they're high-speed.

Unlike traditional dial-up connections, in which you call in, surf the Net, and then disconnect, broadband connections are always active. Because broadband connections are always on, the amount of time a computer is vulnerable to Internet attack is greatly increased compared with dial-up. Any time your computer is on, it's online and vulnerable to attack. Thus, based on raw probability, your computer's going to get attacked much more often on a broadband connection than on dial-up. Beyond this, however, hackers are more likely to go after machines that are connected all the time because they know those machines will be there when they need them, either to activate a Trojan horse they've installed or for some other nefarious purpose. Hackers also may restrict their searches to Internet addresses that they know are used for broadband connections, because they know that machines on those networks will be more useful to them, further increasing the odds of an attack.

Broadband connections are not only always on but also (usually) many times faster than dial-up connections. Speed provides many advantages to a hacker. Hackers look for machines by sending out a query or "probe" to successive addresses until a machine answers and tells the hacker it's

there. If a hacker is looking only for machines with fast connections, he can find them quickly because they answer his probe faster. And when a hacker finds a machine, he can carry out attacks against it more quickly.

In the chapter on managing passwords, for example, you'll see that speed is essential to a dictionary attack, in which the hacker tries to figure out your password by trying every word in the dictionary. Such an attack is practical only on a high-speed connection. Additionally, if the hacker wants to use your machine as a launching point for other attacks, speed is critical as well.

Another characteristic of many broadband connections is that your machine is assigned the same Internet address for long periods of time. Even though many such connections claim to give your machine a dynamic address, that address rarely changes. So the hacker can pretty much count on your machine's being available at the same address whenever he wants to get at it—another big advantage to him over a machine on a dial-up connection, because its address changes each time it dials in.

Many of the rest of us still connect through dial-up connections, but broadband connections are increasing at a faster rate than other Net connections. Broadband connections grew from about 4.7 million at the end of 1999 to 11 million at the end of 2000, and the number is expect to grow to 20 to 30 million by 2004. So even if you're not using a broadband connection today, there's a pretty good likelihood that you will soon. You might as well start thinking about safety now.

But I Use a Mac!

Even after everything we've told you about how real the risks are, you might still be thinking, "But I use a Mac! Everyone says the Mac OS is secure and that the Mac is just 10 percent of the machines on the Net. Won't the hackers go after the Windows machines first?"

It's true that the Classic Mac OS (up through the 9.x series) generally is considered to be more secure than either the Windows or Unix operating system. Here are a few reasons:

- The Mac OS was designed for a single user.
- It was not designed to be logged into remotely.
- Its source code is not available publicly.
- It does an excellent job of preventing you from opening security holes accidentally, both through a clear user interface and through warnings when appropriate.
- It just seems to have fewer security holes.

As supporting evidence for the Mac's superior security, in 1999 the U.S. Army chose the Macintosh as the Web server for its main site after its Windows-based server was hacked by a 19-year-old. The World Wide Web Consortium (W3C) also states publicly that "the safest Web site is a bare-bones Macintosh running a bare-bones Web server."

It's true that Windows machines represent 90 percent or so of the machines out there on the Net. In this case, however, the Mac's smaller installed base ends up being a good thing. Remember, most attackers aren't looking for your specific machine; they're looking for any machine. And because the methods of breaking into a Windows machine are different from those for breaking into a Mac (or a Unix machine), most hackers are looking specifically for Windows machines. The popularity of Windows machines also has a snowball effect. Because most hackers are looking for Windows machines, most of the automated scripts that are written target those machines, so most of the script kiddies, who can't do much on their own, end up attacking Windows machines. And when the script kiddies grow up and *really* start to learn things, guess what machines they write new scripts for?

Once again though, specific statistics are a good idea:

In the Open Door study we mentioned earlier in this chapter, fully 40 percent of all the attacks detected specifically targeted Windows machines, with another 2 percent targeting Unix machines. Not a single Mac-specific attack was detected during the month of the study.

So, using a Macintosh does go a long way toward enhancing your overall safety against certain type of attacks. But we could not identify a good 58 percent of attacks as being against a specific type of machine. Also, many other security issues (especially those we list in Chapter 3) apply pretty much equally to all types of computers. In fact, some might even apply to Macs to a greater degree.

Moreover, as many of you are aware, the Mac OS is transitioning to Mac OS X. Mac OS X has, at its core, the Unix operating system. Apple has done a great job of hiding the inherent complexities of Unix underneath the covers of Mac OS X, but those complexities are still there. Many of those complexities are directly related to the myriad security issues that have always been associated with Unix. Unix is the environment of choice for many hackers, who love its command-line complexity and open source code. But until now, there hasn't been much of an installed base for hackers to go after. With the sudden flood of Unix-based machines that Mac OS X is unleashing, you can bet that the Mac is going to become a much bigger target very quickly. As the Mac moves from Mac OS 9 to Mac OS X, and from an '80s OS into the 21st century, it also moves from a secure, little-targeted OS to a less secure, more-targeted OS, with many more unknowns. We'll have a lot more to say about the transition to Mac OS X in later chapters, but it's definitely something to start thinking about now.

See our book's companion website at www.peachpit.com/macsecurity/ *for up-to-date information on Mac OS X security.*

What, Me Worry Too Much?

We hope that you now see the need to worry about security while you're online. Some of you may now even be so scared that you're thinking about pulling the network connection on your Mac right away, especially if that connection's through a cable modem or DSL. But is it possible to be too worried?

Yes.

If you really pulled the plug on your network connection and never connected to the Net again, we would have done you a great disservice. Like most good things in life, the Net is a double-edged sword. But it's 95 percent good edge and 5 percent bad. You don't *not* drive your car because you might get into an automobile accident, and you don't stay home all the time because you're worried that someone might break in. But you do put on your seat belt when you drive, and you do lock your house when you leave for a trip. So there is an appropriate degree of worry for every situation.

How much should you worry? Only you can make that decision. As is true of everything else, the degree to which you worry about online security should be proportionate to the risks involved.

Consider two Mac users. The first connects through a dial-up modem for maybe an hour a day. He uses his Mac mainly for reading e-mail and doesn't keep any important documents or data on the Mac. The second is online through a cable modem and uses both the Net and the Mac quite extensively, sending and receiving e-mail, doing online banking, and keeping track of stock portfolios through the Web. She also keeps financial records and even a book that she's writing on the Mac, plus some work-related items. Clearly, the second Mac user should worry about the security of her machine more than the first. This is not to say that the first user shouldn't worry but that he can afford to worry less, because he has less to lose.

Degrees of worry should translate into degrees of security. As you'll see, you can take many security measures to protect your Macintosh while you're online, just as you can take many security measures to protect your house. You can lock the door; you can lock the windows; you can put in an alarm system;

you can build a security gate. Different degrees of security are appropriate for different situations.

We feel that everyone should at least understand and implement the general security principles outlined in the rest of Part 1 of this book. Beyond that, you'll need to assess things for yourself. As a rough guideline, here are some factors that should increase your "worry index" and, thus, your security measures.

Do you:

- Have a permanent connection to the Net?
- Have a high-speed connection to the Net?
- Leave your Mac on all the time (with a permanent connection to the Net)?
- Depend on your Mac or the Net to do your job?
- Make extensive use of e-mail, especially for exchanging documents?
- Keep important documents or records on your Mac?
- Shop online or use other forms of e-commerce?
- Use Mac OS X, Windows, or Unix?
- Have more than one Mac on the Net?
- Provide any services from your Mac, such as file sharing or a Web site?

You may not understand the reasons behind all of these questions yet, but you certainly should by the end of this book.