CHAPTER 4

IP SECURITY AND FIREWALLS

Chapter Goals

- Protective devices
- Denial of service
- Spies (Industrial and otherwise)
- Network taps
- Host security
- A firewall can log Internet activity efficiently
- Buying versus building
- A firewall cannot fully protect against viruses

4.1 INTERNET FIREWALLS

A firewall is a system or group that enforces an access control policy between two or more networks. The firewall can be thought of as a pair of mechanisms that exist to block traffic. A firewall's purpose is to keep unauthorized users out of a network while still allowing people to get their jobs done. It is scarcely possible to go anywhere, read a magazine or a newspaper, or listen to a news broadcast without seeing or hearing about the Internet. It is so popular that no advertisement is complete without a reference to a Webpage. While non-technical publications are obsessed with the Internet, technical publications are obsessed with security. It's a logical progression: Once the first excitement of having a superhighway in your neighborhood wears off, people notice that not only does it allow for rapid travel, but it also lets in a very large number of strangers to the neighborhood. (Not all of them are people you would have invited.)

The Internet is a marvelous technological advance that provides access to information and the ability to publish information in revolutionary ways. This book is about one way to balance the advantages and the risks to take part in the Internet while still protecting yourself.

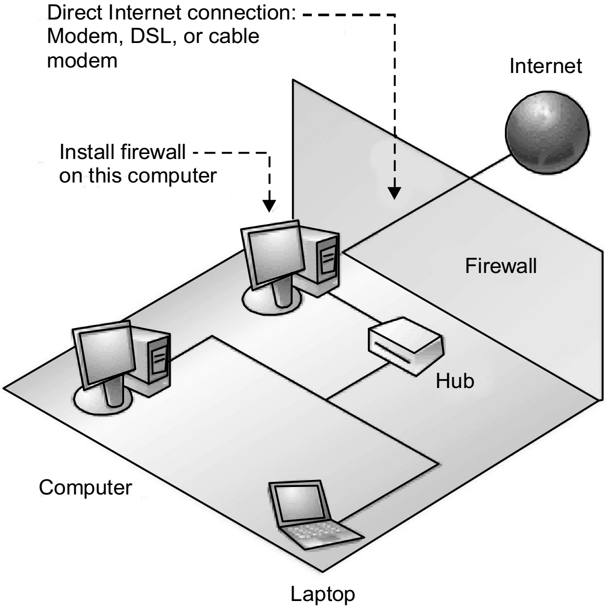

FIGURE 4.1 An example of a firewall

Later in this chapter, we describe different models of security that people have used to protect their data and resources on the Internet. Our emphasis in this book is on the network security model and in particular, the use of Internet firewalls. A firewall is a form of protection that allows a network to connect to the Internet while maintaining a degree of security. The section later in this chapter called "What is an Internet firewall"? describes the basics of firewalls and summarizes what they can and cannot do to help make a site secure. There are some important questions addressed here: What are you protecting on your systems? What types of attacks and attackers are common? What types of security can you use to security can you use to protect your site?

4.2 PROTECTIVE DEVICES

A firewall is basically a protective device. If you are building a firewall, the first thing you need to worry about is what you're trying to protect. When you connect to the Internet, you're putting three things at risk:

- Your data: The information you keep on the computers
- Your resources: the computers themselves
- Your reputation

4.2.1 Your Data

Your data has three separate characteristics that need to protected.

Secrecy

You might not want other people to know it.

Integrity

You probably don't want other people to change it.

Availability

You almost certainly want to be able to use it yourself.

People tend to focus on the risks associated with secrecy, and it's true that those are usually large risks. Many organizations have some of their most important secrets—the designs for their products, financial records, or student records—on their computers. However, you may find that for your site, it is relatively easy to separate the machines containing highly secret data from the machines that connect to the Internet. (Or you may not. You cannot carry out e-commerce without having information about orders and money pass through Internet-accessible machines.)

Suppose that you can separate your data in this way, and that none of the information that is Internet accessible is secret. In that case, why should you worry about security? Because secrecy isn't the only thing that must be protected. There are also important concerns about integrity and availability. (After all, if your data isn't secret, and if you don't mind it being changed, and if you don't care whether anybody can get to it, why are you wasting disk space on it?)

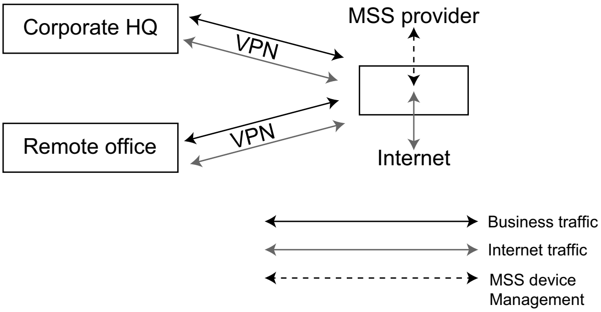

FIGURE 4.2 Using a protective device

Even if your data isn't particularly secret, you'll suffer the consequences if it's destroyed or modified. Some of these consequences have readily calculable costs: once data is lost, it is costly to have it reconstructed. If you were planning to sell that data in some form, you'll have lost sales regardless of whether the data is something you sell directly, the designs from which you build things, or the code for a software product. Intangible costs are also associated with security incidents. The most serious is the loss of confidence (user confidence, customer confidence, investor confidence, staff confidence, student confidence, and public confidence) in your systems and data. Consequently, this results in a loss of confidence in your organization.

> Computer security incidents are different from many other types of crimes because detection is unusually difficult. It may take a long time to find out that someone has broken into your site—sometimes you'll never know. Even if somebody breaks in but doesn't actually do anything to your system or data, you'll probably lose time (hours or days) while you verify that the intruder did not do anything. In a lot of ways, a brute-force "trash-everything" attack is easier to manage than an attack that doesn't appear to damage your system. If the intruder destroys everything, you restore from backups and start over. But if the intruder doesn't appear to have done anything, you spend a lot of time second-guessing yourself, wondering what he or she might have done to the system or data. The intruder almost certainly has done something—most intruders start attacks by making sure that they have a way to get back in before they do anything else.
>
> Although this book is primarily about preventing security incidents, it also includes responding to security incidents, and supplies some general guidelines for detecting, investigating, and recovering from security incidents.

4.2.2 Resources

Even if you have data you don't care about (or, perhaps you enjoy reinstalling your operating system every week), if other people are going to use your computers, you probably would like to benefit from this use in some way. Most people want to use their own computers or they want to charge other people for using them. Even people who give away computer time and disk space usually expect to get good publicity and good will; they aren't going to get it from intruders. Since you spend time and money on your computing resources, it is your right to determine how they are used.

Intruders often argue that they are using only excess resources; as a consequence, their intrusions don't cost their victims anything. There are two problems with this argument.

First, it's impossible for an intruder to determine successfully what resources are excess and use only those. It may look as if a system has a significant amount of empty disk space and hours of unused computing time. In fact, though, the user might be just about to start computing animation sequences that are going to use every bit and every microsecond. An intruder cannot restore resources when the user wants them, either. (Here is another way to think about this: I don't ordinarily use my car between midnight and 6 a.m. However, that doesn't mean I am willing to lend it to you without being asked. What if I have an early morning flight the next day, or what if I'm called out to deal with an emergency?)

Second, it is the computer user's right to use their resources the way they want to. That may mean that a significant amount of disk space remains empty and unused.

4.2.3 Reputation

When an intruder appears on the Internet with a stolen identity, anything he or she does is attributed to their victim. What are the consequences of this type of action?

Most of the time, the consequences involve other sites or law enforcement agencies trying find out why the intruder is breaking into these systems. This is not as rare an occurrence as it may seem. One site got serious about security when its system administration staff added a line item to the company's time cards after a conversation with the FBI about break-in attempts originating from the company's site.

Sometimes, such imposters cost more than lost time. An intruder who actively dislikes someone or takes pleasure in making life difficult for others may change a Website, send electronic mail, or post new messages that purposely claim to come from a company or individual. Generally, the people who choose to do this are doing it for spite, rather than believability. However, even if only a few people believe these messages, the recovery process can be long and humiliating. Anything even remotely believable can do permanent damage to a reputation.

For example, an impostor posing as a Texas A&M professor sent out hate email containing racist comments to thousands of recipients. The impostor was never found, but the professor is still dealing with the repercussions of the forged message. In another case, a student at Dartmouth sent out an email using the signature of a professor late one night during exams. The email claimed the professor had a family emergency: The forged email canceled the next day's exam, and only a few students showed up.

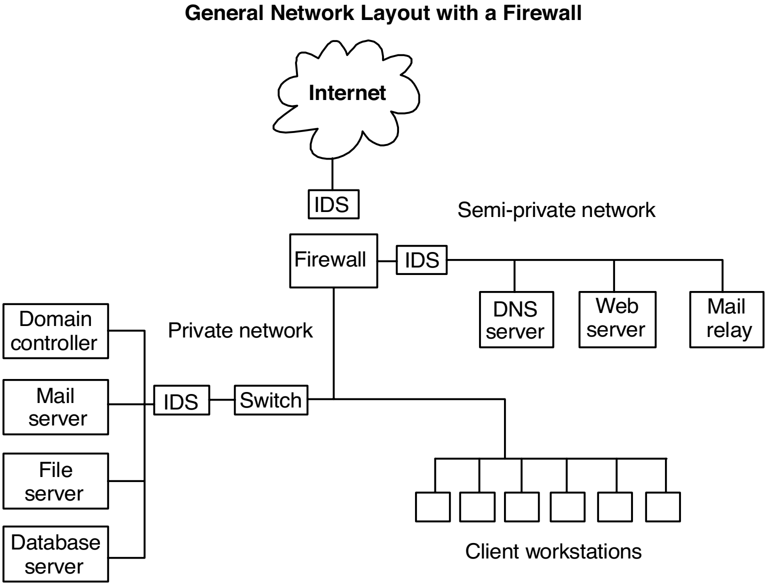

FIGURE 4.3 General network layout with a firewall

It's possible to forge electronic mail or news without gaining access to a Website, but it's much easier to show that a message is a forgery if it's generated from outside the forged site. The message coming from an intruder who has gained access to your site will look exactly like yours because they are pretending to be you. An intruder will also have access to details that an external forger won't. For example, an intruder who has all of your mailing lists available and knows exactly who you send mail to has inside information.

Currently, attacks that replace Websites are very popular; one list shows more than 160 successful attacks simply replaced the sites via boosting by the attackers, but a significant portion of the attacks were directed at the content of the sites. A site that should have touted Al Gore's suitability for the U.S. presidency was replaced by a similar anti-Gore site. Political movements in Peru, Mexico, and China have been involved in cyberattacks, and many entertainment sites, including those for pop stars, pro Wrestling, and the Boston Lyric Opera, all suffered as well.

Even if an intruder does not steal an identity, a break-in at a site isn't good for a company's reputation. It shakes people's confidence in an organization. In addition, most intruders will attempt to go from one company's machines to other companies' machines, which is going to make their next victims think of the first site as a platform for computer criminals. Many intruders will also use a compromised site as distribution site for pirated software, pornography, and/or other stolen information. It is difficult to recover when a business or person's name is linked to software piracy or pornography.

What's out there to worry about? What types of attacks are you likely to face on the Internet, and what types of attackers are likely to be carrying them out? In the sections that follow, we touch on these topics, but don't go into any technical detail. Later chapters describe the kinds of attacks in some detail and explain how firewalls can help protect against them.

4.3 TYPES OF ATTACKS

There are many types of attacks on systems, and various ways of categorizing these attacks. In this section, we break attacks down into three basic categories: intrusion, denial of service, and information theft.

4.3.1 Intrusion

The most common attacks on computer systems are intrusions. With *intrusions*, hackers are able to use someone else's computers. Most attackers want to use these computers as if they were legitimate users. Attackers have dozens of ways to obtain access. They range from social engineering attacks (where a hacker discovers the name of a high-level individual in the company, calls a system administrator claiming to be that person, and then saying their password needs to be changed right now so that they can get important work done) to simple guesswork (the attacker tries account names and password combinations until one works) to intricate ways to get in a system without knowing an account name and a password.

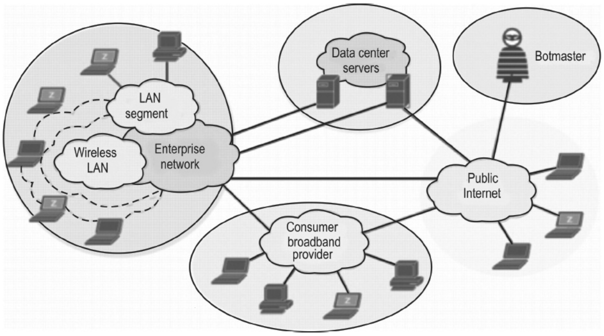

FIGURE 4.4 Common intrusions

Firewalls help prevent intrusions in a number of ways. Ideally, they block all ways to get into a system without needing an account name and password. Properly configured, they reduce the number of accounts accessible from the outside that are vulnerable to guesswork or social engineering. Most people configure their firewalls to use one-time passwords that prevent guessing attacks. Even if you do not use these passwords and authentication and auditing services, a firewall will give you a controlled place to log attempts to get into your system, and, in this way, they help detect guessing attacks.

4.3.2 Denial of Service

A *denial of service attack* is aimed entirely at preventing users from using their own computers.

In late 1994, writer Josh Quittner and Michelle Slatalla were the target of an "electronic mail bomb." Apparently in retaliation for an article on the cracker community they'd published in Wired magazine, someone broke into IBM, Sprint, and the writers' network provider, and modified programs so their email and telephone service was disrupted. A flood of emails couldn't get through; eventually, their Internet connection was shut down entirely. Their phone service also fell victim to the intruders, who reprogrammed the service so that the callers were routed to an out-of-state number where they heard an obscene recording.

Although some cases of electronic sabotage involve the actual destruction or shutting down of equipment or data, more often they follow the pattern of flooding seen in the Quittner-Slatalla case or in the case of 1988 Morris Internet worm. An intruder so floods a system or network—with messages, processes, or network requests—that no real work can be done. The system or network spends all its time responding to messages and requests and can't satisfy any of them.

While flooding is the simplest and most common way to carry out a denial of service attack, a clever attacker can also disable services, re-route them, or replace them. For example, the phone attack in Quittner-Slatalla case denied phone service by re-routing the phone calls elsewhere. It is possible to mount the same kind of attack against an Internet service.

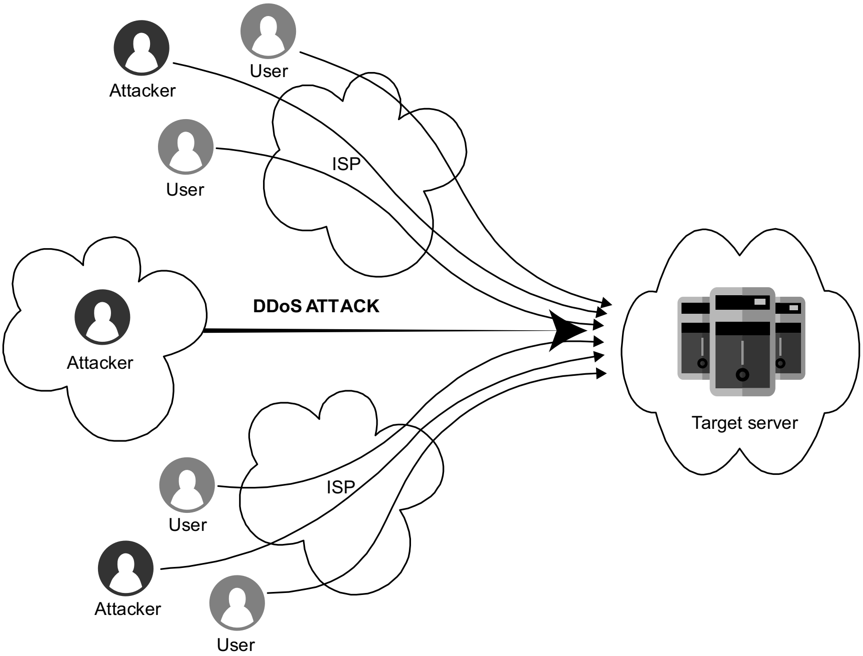

FIGURE 4.5 An example of a distributed denial of service (DDoS) attack

It is almost impossible to avoid all denial of service attacks. For example, many times, administrators set accounts to become unusable after a certain number of failed login attempts. This prevents attackers from simply trying passwords until they find the right one. Unfortunately, this approach provides attackers with an easy way to mount a denial of service attack: they can lock any user's account simply by trying to log in a few times.

Most often, denial of service attacks are un-avoidable. If you accept things from the outside world, be it electronic mail, telephone calls or packages, it is possible to get flooded. The notorious college prank of ordering a pizza or two from every pizzeria in town to be delivered to your least favorite person is a form of denial of service: it's hard to do much else while arguing with 42 pizza deliverers. In the electronic world, denial-of-service is as likely to happen by accident as on purpose (such as a persistent fax machine faxing something to a voice line). The most important thing is to set up services so that if one of them is flooded, the rest of them can still function while the problem is found and corrected.

Flooding attacks are considered "unsporting" by many attackers because they are not difficult to carry out. For most attackers, they are also pointless, because they do not provide the attackers with the information or the ability to use your computers (the payoff for most other attacks). Intentional flooding attacks are usually the work of people who are angry at a particular person or company, and such people are quite rare.

With the right tools and co-operation, its fairly easy to trace flood packets back to their source, but that might not help determine who is behind the attacks. The attacks almost always come from machines that have themselves been broken into. Only a really low-level attacker generates an easily traced flood of packets from their own machine. Sometimes flooding attacks are carried out by remote control. Attackers install remotely controlled flooding software on systems that they break into over the course of many weeks or months. This software lies dormant and undiscovered until some later time, when they trigger many of these remotely-controlled installations to simultaneously bombard their victims with massive floods of traffic from many different directions at once. This was the method behind the highly publicized denial of service attacks on Yahoo!, CNN, and other high profile Internet sites early in the year 2000.

Unintentional flooding problems are more common than intentional ones, as we discuss in the "Stupidity and Accidents Section" later in this chapter.

Some denial of service attacks are easy for attackers to carry out, and these are relatively popular. Attacks that involve sending a small amount of data that cause machines to reboot or hang are very popular with the same sort of people who like to set off fire alarms in dormitories in the middle of the night, for much the same reason; with a small investment, an attacker can annoy a very large number of people who are unlikely to be able to find him afterwards. The good news is that most of these attacks are avoidable. A well-designed firewall will usually not be susceptible to them and will prevent them from reaching internal machines that are vulnerable.

4.4 NETWORK TAPS

Some types of attacks allow an attacker to get data without ever having to directly use a system's computers. Usually, these attacks exploit Internet services that are intended to give out information, inducing the services to give out more information than was intended, or to give it out to the wrong people. Many Internet services are designed for use on local area networks, and don't have the type or degree of security that would allow them to be used safely across the Internet.

Information theft doesn't need to be active or particularly technical. People who want to find out personal information could simply ask (perhaps pretending to be somebody who had a right to know): this is referred to as *active information theft*. They could also tap a phone: this is *passive information theft*. Similarly, people who want to gather electronic information could actively query for it (perhaps pretending to be a machine or a user with valid access) or could passively tap the network and wait for it to flow by.

Most people who steal information try to get access to a user's computers; they are looking for user names and passwords. Fortunately for them, and unfortunately for everybody else, that's the easiest kind of information to get when tapping a network. User name and password information occurs quite predictably at the beginning of any network interaction, and such information can often be reused in the same form.

How would a hacker proceed if they wanted to find out how somebody answers her telephone? Installing a tap would be an easy and reliable way to get that information, and a tap at a central point in the telephone system would yield the telephone greetings of hundreds or thousands of people in a short period of time.

What if the attacker wants to know how somebody spells his or her last name, or what the names and ages of his or her children? In this case, a telephone tap is a slow and unreliable way to get that information. A telephone tap at a central point in the system will probably yield that information about some people. It will certainly gather some secret information that could be used in interesting ways, but the information is going to be buried among the conversations of hundreds of people setting up lunch dates and chatting about the weather.

Similarly, network taps, which are usually called *sniffers*, are very effective at finding password information but are rarely used by attackers to gather other kinds of information. Getting more specific information about a site requires either extreme dedication and patience, or the knowledge that the information will reliably pass through a given place at a given time. For example, if an attacker knows that the victim calls the bank to transfer money between her checking savings accounts at 2 pm every other Friday, it is worth tapping that phone call to find out the person's access codes and account numbers. However, it is probably not worth tapping somebody else's phone, on the off chance that they will do such a transfer because most people don't transfer money over the phone at all.