Chapter 5

Computer Security

Chapter Outline

What You Will Learn in This Chapter

- How do you protect your information resources?
- What are the primary threats to an information system?
- What are the primary security threats faced by individuals?
- What primary options are used to provide computer security?
- How do you protect data when unknown people might be able to find it or intercept it?
- What additional benefits can be provided by encryption?
- What non-computer-based tools can be used to provide additional security?
- How do you prove the allegations in a computer crime?
- What special security problems arise in e-commerce?
- If you have to track everyone's computer use to improve security, what happens to privacy?

National Football League

How do you keep data secure? Any professional football team has dozens of coaches and players—whether it is American football or European soccer, the characteristics are similar. Teams win through cooperation—that means everyone needs to share information. Coaches create playbooks, players provide feedback, and scouts identify weaknesses in opposing teams. All of this information has to be shared—so teams increasingly put the data onto computers. But securing this data is critical. Imagine the problems that arise if an opposing team gets a copy of the latest player health reports and new plays. Yet there are dozens of players and coaches, most of whom are not computer experts (to put it politely, since you really do not want to insult a 300-pound linebacker). Plus, coaches and players are sometimes replaced or switch teams.

Teams increasingly have to offer more data to fans. Some stadiums are now offering wireless networks. But security again becomes critical. How do you keep the fans from accidentally interfering with the coaching networks? What other threats can you think of? Hundreds of things can go wrong with technology, and someone has to be responsible for protecting the systems and creating contingency plans to handle problems.

Introduction

How do you protect your information resources? What are the major threats? Figure 5.1 presents some of the issues: outside hackers, people intercepting data, attacks on the server, physical threats to the equipment (including natural disasters such as floods and fire), and internal threats from employees, as well as privacy issues such as abuse of personal data. Think about the problem for a second: Who stole more money in 2010 (or almost any other year): teenage hackers or CEOs? Computer security has to prepare for both of these threats and others.

Security is a challenging problem for any business. It has become even more difficult with computing devices and data used everywhere in the company, on the Web, and around the world. Many companies rely on part-time and contract workers and need to give them access to data to complete their tasks. Monitoring tools are needed to watch for security and privacy issues. Advances in encryption and biometrics have provided powerful tools, but security ultimately comes down to people. If a worker is careless with passwords, or a programmer makes a mistake, or a network engineer falls behind on updates, or an auditor fails to test an account, holes are created that can be exploited by a thief or miscreant.

On the other hand, organizations can go overboard with security rules. Computer security is a balance—you must protect the data but still enable workers to do their jobs. The challenge is that IT security workers often see their jobs as identifying potential problems and preventing them from occuring. If an attacker steals data, the security staff is likely to be blamed, but if security is so tight that workers need to create workarounds to do their jobs, management might never see the problem, much less blame the security staff. So there is an incentive to try and security as tight as possible—even if it interferes with jobs.

Encryption plays an important role in protecting systems. It can also be used to authenticate the sender of a message. A key aspect of security and encryption is

Trends

Security has been an issue for thousands of years, from the simple substitution ciphers of Caesar to the importance of codes and code breaking in World War II. As more data was moved to computers, several complications arose. One of the biggest obstacles has been the need to identify people. Passwords have been the most common method, but they cause many problems. Newer technologies are available, but they require standards and people will have to agree to use them. Since security requires identifying people, increased emphasis on security can result in a reduction in privacy. Firms have collected data on consumers for years, but only recently have technologies advanced to the point where it is relatively inexpensive and easy to collect and analyze data on millions of consumers. Despite Hollywood's portrayals, the greatest security threats come from insiders. On the other hand, it used to be difficult to attack servers, and required programmers with a deep knowledge of the system. Today, with millions of computers connected to the Internet, it is relatively easy for beginners to download code from a site and run automated attacks against known bugs in operating systems. This technique is commonly used for creating denial-of-service attacks on Web sites. As e-commerce expands in importance, it becomes increasingly critical to develop a more robust Internet protocol that can identify and stop denial-of-service attacks. Many security tools exist to protect servers and to encrypt data transmissions, but it is difficult to stop denial-of-service attacks that rely on flooding the server.

the need to identify users. Consequently, the flip side of many security policies is the loss of privacy.

The Internet, e-commerce, and cloud computing add some challenging aspects to security. E-commerce requires that portions of the computer systems be available to consumers and other businesses. Greater business benefits are generated when Web sites are integrated with corporate data—such as inventory levels so customers can determine if an item is in stock. Yet, allowing public access to these systems creates greater security risks. Furthermore, since the Internet is a shared public network, data needs to be protected in transmission—to ensure it is not intercepted or altered. Wireless networks are even more open to eavesdropping and interception. Because of the public nature of the Internet, even a well-protected system can be brought down with denial-of-service attacks.

Tightening security can easily lead to a loss of privacy. One way to improve security is to completely identify every person and every activity performed. But even completely honest people are not willing to give up that much privacy. So, security faces another trade-off. These trade-offs are important, but they make the job harder for the corporate security expert.

Threats to Information

What are the primary threats to an information system? Information threats are often described in two categories: Physical and logical. Some people add a third category: Behavioral. Physical threats are things that go wrong with the hardware and buildings—particularly fires, floods, earthquakes, and hurricanes. Logical security refers to the ability to define and control access to

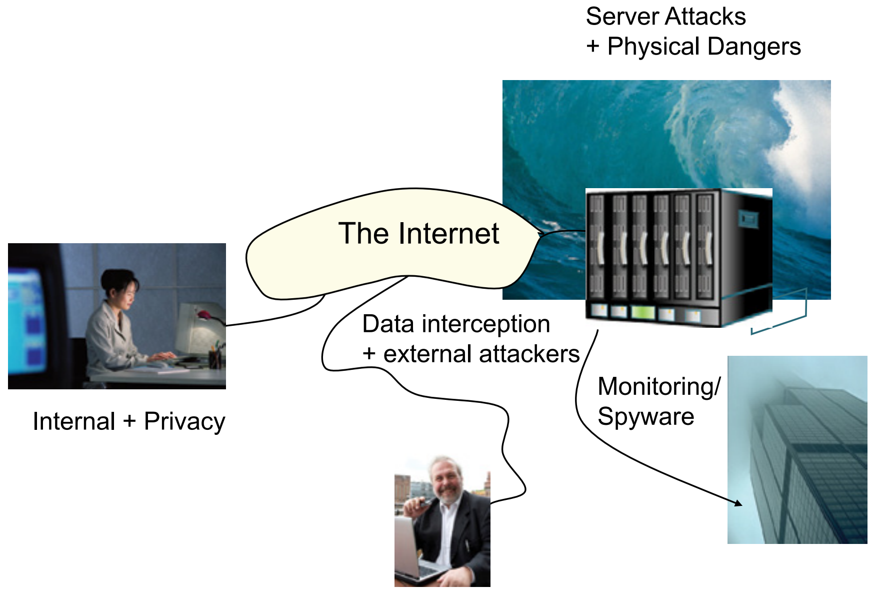


Figure 5.1

Security and privacy are important issues in the Internet era. People can intercept data, attack servers directly and indirectly, and companies routinely monitor all transactions.

data. Behavioral security refers to specific problems related to people. You might have strong physical and logical security, but employees who write their passwords on notes stuck to their computer, or give out private information over the phone can quickly defeat any security system.

Many potential threats exist to information systems and the data they hold. The complicated aspect is that the biggest information threat is from legitimate users and developers. Purely by accident, a user might enter incorrect data or delete important information. A designer might misunderstand an important function and the system will produce erroneous results. An innocent programming mistake could result in incorrect or destroyed data. Minor changes to a frail system could result in a cascading failure of the entire system.

You can detect and prevent some of these problems through careful design, testing, training, and backup provisions. However, modern information systems are extremely complex. You cannot guarantee they will work correctly all of the time. Plus, the world poses physical threats that cannot be avoided: hurricanes, earthquakes, fires, and so on. Often, the best you can do is build contingency plans that enable the company to recover as quickly as possible. The most important aspect of any disaster plan is to maintain adequate backup copies. With careful planning, organization, and enough money, firms are able to provide virtually continuous information system support.

A second set of problems arises from the fact that as technology changes, so do criminals. Today, only a desperate person would rob a bank with a gun. The probability of being caught is high, and the amount of money stolen is low. Do not take it as an invitation to become a thief, but the computer offers much easier ways to steal larger amounts of money.

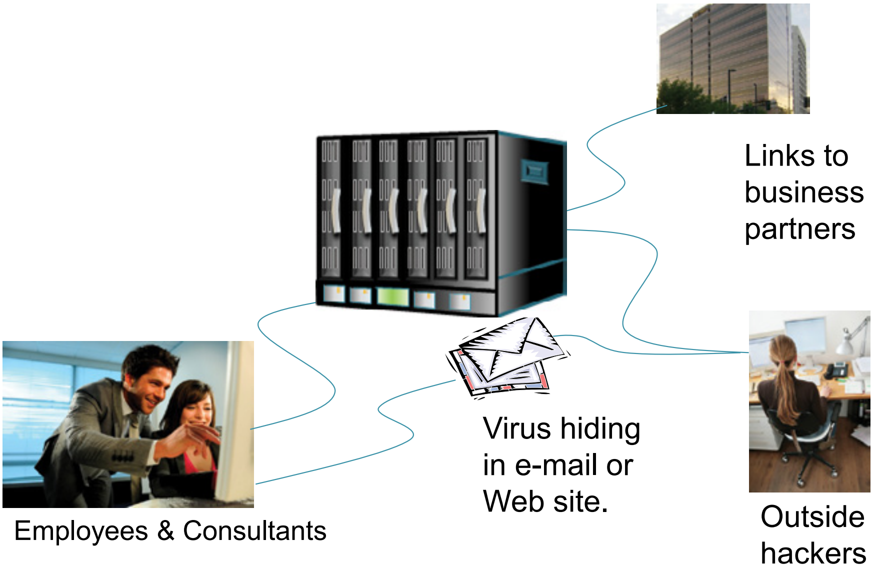

Links to business partners
Virus hiding in e-mail or Web site.
Employees & Consultants
Outside hackers

Figure 5.2

Threats to information. By far, the most serious threats are from insiders: employees, mistakes, consultants, and partnerships. Businesses have to trust insiders to stay in operation, but you need to put limits on the access to data. It is possible for outsiders to break into most computer systems, but it is fairly difficult. Viruses are a serious threat both to data and security in general.

The threats mentioned in Figure 5.2 provide a useful way to organize some of the concepts of computer security. In particular, the physical threats need to be separated from the logical or data attacks.

Disasters

Fortunately, fires, floods, hurricanes, and other physical disasters do not happen too often. But when a disaster does hit a company's data center, it could destroy the company. Without advance preparations, the loss of a data center could shut down the operations. How long can a company survive without transaction processing?

Today, there are many ways to plan for and recover from disasters. Figure 5.3 shows a traditional method of using scheduled backups and a disaster recovery services provider. When computer servers are expensive, it makes sense to contract with a company to provide a facility and possibly spare computers. One level of support, called a **hot site**, consists of a fully configured computer center. Specific computer equipment is already installed and ready for immediate use. When the MIS staff declares a disaster, they install the backup tapes on the hot-site computers and use telecommunication lines to run the day-to-day operations. Another alternative is to contract for a **cold site**, which provides fully functional computer room space, without the computer equipment. If a disaster occurs, either the company or the disaster recovery services provider can arrange for the neces-

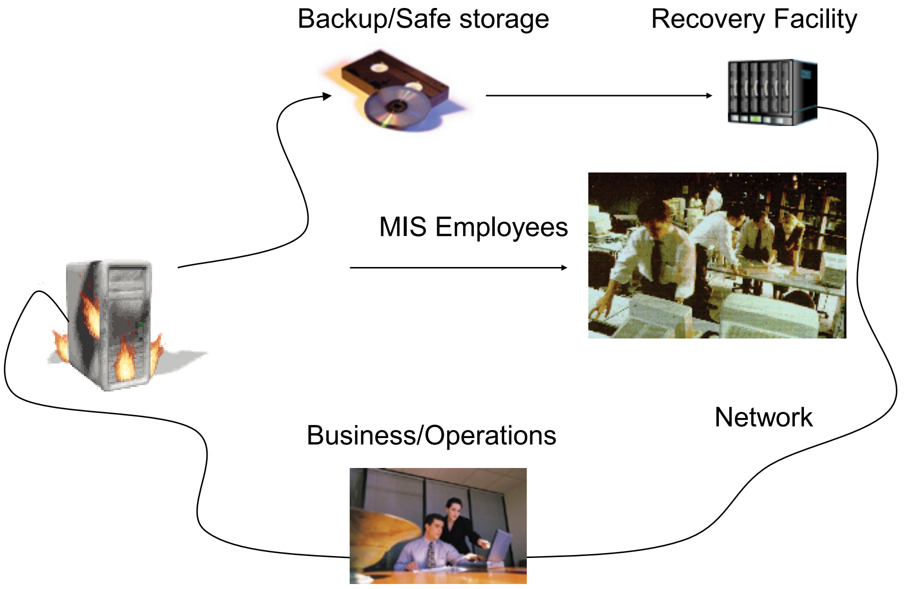


Figure 5.3

Disaster planning. 1. You have to back up your data. 2. You can contract with a disaster facility to have a site ready. 3. Create a detailed plan to move your MIS people and restore the system. 4. If a disaster strikes, shift the business network to the temporary facility. 5. Rebuild the original data center.

sary equipment to be shipped to the cold site. However, there might be a delay of several days before the new data center will be operational, so a cold site is often used in conjunction with a hot-site contract.

The problem with the traditional approach is that companies can no longer afford to run without computer support—even for a few hours. Fortunately, computer prices have also declined while network transfer speeds have increased. Consequently, it is possible for many companies to provide continuous backup—both in terms of data and processing capabilities. Figure 5.4 shows the basic concepts. Server clusters are created in separate locations and connected by a network. Each server contains redundancy in terms of multiple processors, disk drives, network connections, and even power supplies. If one component in the server dies, the others pick up the load instantly. Data is often stored on a network-attached storage area network, with its own duplication of drives and RAID configuration. Finally, in case a fire, flood, or network outage knocks out the entire facility, a second facility hosts another server cluster. Data from one site is continuously replicated to the second site. User applications are connected by a network so if one site goes down, everything shifts automatically to the backup site.

Large firms might build or lease their own remote sites with multiple server clusters. But even small companies can gain many of the same advantages are relatively low cost by using cloud computing. Large service providers on the cloud, such as Amazon's EC3, automatically provide servers in multiple locations. Companies can lease almost any level of computing which is handled off site by Amazon.

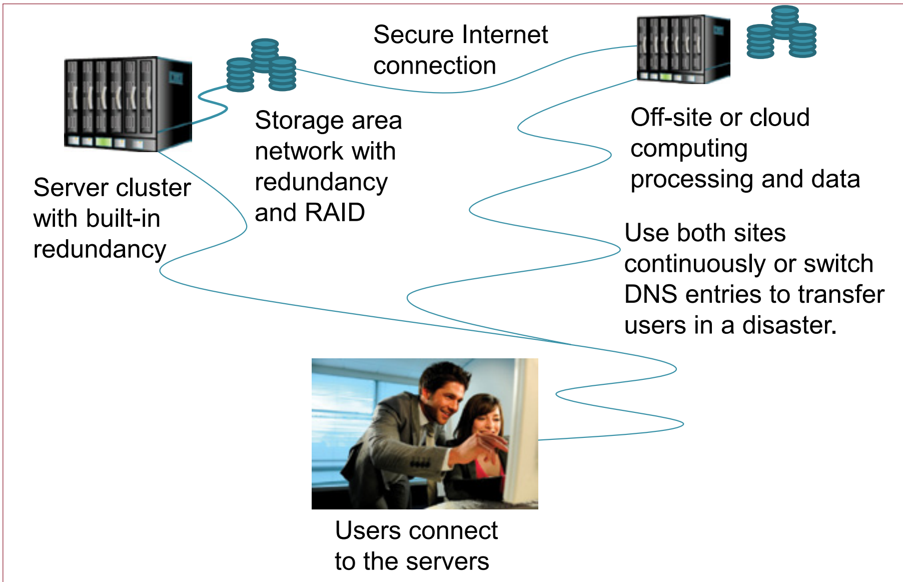

Secure Internet connection
Server cluster with built-in redundancy
Storage area network with redundancy and RAID
Off-site or cloud computing processing and data
Use both sites continuously or switch DNS entries to transfer users in a disaster.
Users connect to the servers

Figure 5.4

Continuous backup. Duplicate servers are installed at different locations and connected across a network—often the Internet. The servers themselves also have built-in redundancy. Data is written to multiple drives and multiple locations. If one site fails completely, the other site can instantly pick up the load.

Employees and Consultants

Employees are the heart of any company. Companies function and succeed by trusting their employees. Although almost all employees are honest and diligent, there is always the chance that one employee will use the company's knowledge, experience, and trust to misappropriate resources.

It can be difficult to identify people who might cause damage to the firm. Many companies today use psychological tests, background checks, and random drug tests to indicate potential problems. Most companies are wary of employees whose employment has been terminated. Businesses follow specific steps when employees leave, being particularly careful to remove the employees' access to company computers.

A more complicated problem arises with MIS employees. Programmers and analysts have to be trusted. Without them, there would be no software. However, it is generally best if the programmers are not the users of the program. Companies enforce a separation of duties among staff programmers and users. Think about what might happen if a bank teller was also responsible for writing the computer program used by tellers. It would be easy to use the computer to steal money from different accounts. Auditing transaction-processing systems is an important task for auditors.

Unscrupulous programmers have also been known to include "time bombs" in their software. Whenever the software runs, it checks a hidden file for a secret word. If the programmer leaves the company, the secret word does not get changed. When the program does not find the correct word, it starts deleting files. On large projects, these bombs can be impossible to spot (until they go off). Keep-

Reality Bytes: Hacking is Easy When You Tell Everyone the Answers

In a well-publicized case, attacker David Kernell broke into Sarah Palin's Yahoo e-mail account—largely by scouring the data that she publicly listed on various services. In 2010, George Bronk was arrested for using a similar technique to break into more than 3,200 e-mail accounts of women. He searched the victim's Facebook accounts for answers to security questions typically used to recover forgotten passwords at online sites. Once he was able to obtain the password, he changed the password, searched for nude photos and posted them on the victim's Facebook pages. He was charged in Sacramento Superior Court and faced six years in prison.

Adapted from Robert McMillan, "Nude Photos Stolen from Women's e-Mail Accounts," *Computerworld*, January 13, 2011.

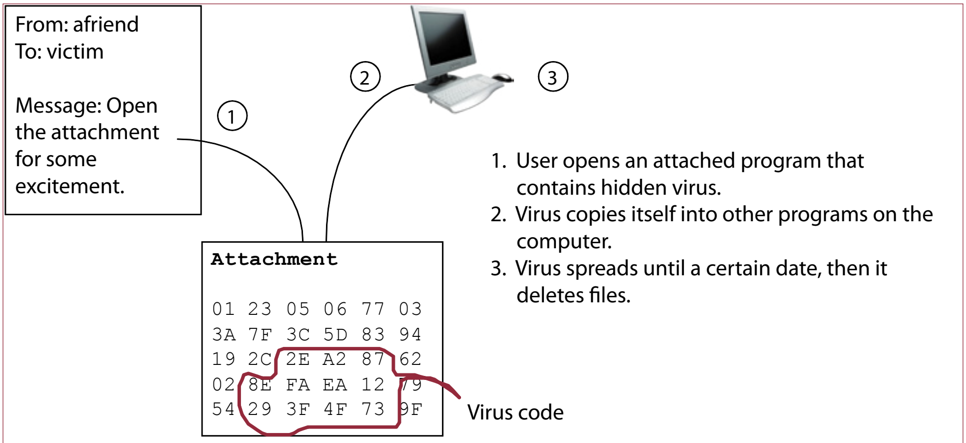
ing good backups can usually minimize the damage. As a related side note, the software industry is pushing states to adopt a new set of laws (UCITA) that makes it legal to include a shutdown time bomb if a software company has a dispute with a business that uses its software.

Another danger area is that programmers might include a trap door or secret password that allows them to gain access to the software even if they leave the company. Sometimes these trap doors are installed innocently, to enable programmers to make corrections faster. The important point is to make sure they are removed when the system is permanently installed.

An interesting twist on passwords arose in 2008 when Terry Childs, the system administrator for the San Francisco network refused to give up the administrative username and password. Apparently the department suffered from management and personality differences and he argued that no one else was qualified to be an administrator on the network. After sitting in a jail cell for 12 days he gave the login credentials to the mayor. Later, he was convicted of interfering with a network and sentenced to 4 years in prison. Ignoring the personality issues, the case does point out the necessity of providing backup access to administrative accounts. What would happen in a large organization if a network administrator died in an accident?

An interesting class of threats to securing your data arises from negligence instead of deliberate actions by the users. For instance, employees might accidentally delete data. Or carrying disks, tapes, or even laptop computers past magnetic fields can sometimes damage the files. In these cases, the best bet is to have backups readily available. More complicated problems arise when laptop computers are lost or even stolen. In addition to the data stored on the machines, the files often hold passwords for corporate computers. Many laptops provide passwords and encrypt the data to minimize these problems. One other problem that falls into this category is a warning to be careful about how you dispose of old tapes, disks, and computer equipment. Businesses run similar risks when they send computer equipment out for repairs.

In general, the best way to minimize problems from employees stems from typical management techniques. Hire workers carefully, treat employees fairly, have separation of jobs, use teamwork, and maintain constant checks on their work. Consultants present the same potential problems as employees. However, consul-



From: afriend
To: victim

Message: Open the attachment for some excitement.

```
Attachment

01 23 05 06 77 03
3A 7F 3C 5D 83 94
19 2C 2E A2 87 62
02 8E FA EA 12 79
54 29 3F 4F 73 9F
```

1. User opens an attached program that contains hidden virus.
2. Virus copies itself into other programs on the computer.
3. Virus spreads until a certain date, then it deletes files.

Figure 5.5

Virus activity. Once a virus is loaded on your machine, you will need an antivirus software package to remove the virus. Several versions are available at low cost. A virus can come from any software that supports executable code. Attachments sent through e-mail are currently the most common method of being infected.

tants tend to be hired for a short time, so the firm knows even less about them than about regular employees. Consultants are generally used for specialized jobs, so there may not be any internal employees who can adequately monitor their work.

Business Partnerships

As computers spread throughout every aspect of business, many companies share their data. For example, General Motors asks its suppliers to provide all information electronically. This electronic data interchange (EDI) means that business information is processed faster and with fewer errors. The problem is that in many cases, it means GM gives other companies considerable access to GM's computers and vice versa. For instance, if GM is thinking about increasing production, the managers might want to check supplier production schedules to make sure the suppliers could provide enough parts. To do it electronically, GM needs access to the suppliers' computers. To participate in business today, you must trust your partners. However, you have limited ability to evaluate all of their employees.

The issue of partnerships becomes more important in an Internet world of software and cloud computing. **Application service providers (ASPs)** on the cloud, such as NetSuite or Salesforce.com, run software on their Web servers and you store data on their sites—using only browsers to access the data and applications. Cloud computing has advantages such as: (1) experts set up and run the site so you do not have to hire specialists, (2) storing the data on the Web means it is accessible to your employees wherever they have Web access, and (3) you can start small and scale up to a reasonable size without hassles. From a security perspective, a potential drawback is that all of your financial data is stored on a site run by someone else. Of course, the reputation of the ASP depends on protecting your data and maintaining security, so it is probably safer than what a small business could handle independently; however, you should still investigate the ASP security procedures.

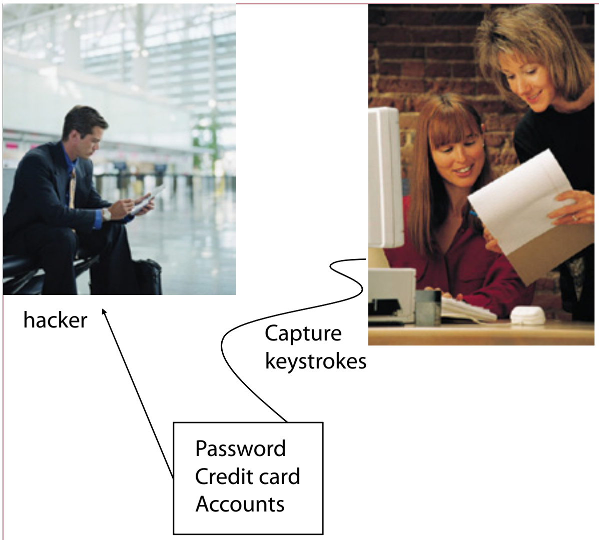


Figure 5.6

Spyware. Software loaded into your computer captures keystrokes, websites you visit, or other personal information. It transfers the data to a website run by a company or hacker who steals your money. The problem is particularly dangerous on public computers that are used by several people.

Outsiders

There is some threat from outsiders who might dial up your computer and guess a password. Using some common sense can minimize most of these threats. For example, in the 1980s, some groups gained access to computers because the operators never changed the default password that was shipped with the computer! The Internet causes additional problems because it was designed to give other people access to your machines. The key lies in providing people with just the level of access they need. The biggest problems today arise from a group labeled **script kiddies**, who download system scanning/attack software from the Internet and randomly search computers for holes. Another major problem with passwords is a technique hackers call **social engineering**. A hacker calls up a victim (you), tells some story, and convinces you to reveal your password. Never give your password to anyone.

In theory, modern computer security systems are effective and can prevent most outside attacks. The problem is that operating systems are complex software programs that have errors. Experts search these systems to find the errors, and ultimately, the vendor fixes the errors. However, this process can result in dozens of patches a year. Some businesses do not keep up with the patches, and some patches interfere with other programs and are not applied. Consequently, there can be thousands of systems connected to the Internet that suffer from published flaws. Software downloaded from the Internet can automatically search for these flaws and provide access even to inexperienced hackers. One key to protecting your servers is to make sure they have all the current operating system patches.

Reality Bytes: You Would Expect TSA to Understand Security

James Duchak was employed as a contractor at the Colorado Springs Operations Center of the U.S. Transportation Security Administration. He was a data analyst for about five years and updated the TSA servers with data pulled from the terrorist screening database and the U.S. Marshals Service Warrant Information Network. He learned in 2010 that he was being let go, and was training his replacement. His replacement noticed that Duchak deleted code that was used to format the birth dates for people entered into the system. In October 2010, Duchak, 47, pleaded guilty to the charges and was sentenced to two years in prison, $60,000 in restitution, and three years of supervised release. The restitution claim is interesting because the code should have been backed up and date formatting code is usually fairly easy to write.

Adapted from Robert McMillan, "Former TSA Contractor Gets Two Years for Damaging Data," *Computerworld*, January 12, 2011.

USB Drives

USB or flash drives are a useful technology for transferring files. But, that also makes them a prime target for carrying viruses and Trojans. Reports indicate that USB drives were a main vector for spreading the Stuxnet virus that appeared to be targeted to specific industrial machines, such as those used by Iran's nuclear processing. But, even simpler viruses, Trojans, and key-stroke loggers can be spread with USB drives. USB drives are physically small but can contain huge amounts of data or complex malware. Some organizations (including at times the U.S. military) have banned them, but they are now everywhere—including cameras and cell phones—so they are difficult to stop. Some software tools exist that can turn off USB ports in computers, or monitor them to prevent anyone from inserting USB drives.

On the flip side, USB drives can be used to improve computer security in some situations. In particular, if you need to use a shared or public computer, it is likely that the computer is already infected with any number of viruses or key-stroke loggers. If you only need to use the system to browse a few open Web sites, the risks are minimal. But public computers are risky when you need to connect to financial accounts. (Student labs might be a problem, but many schools are careful to monitor and remove common viruses.) USB drives have the ability to solve problem of infected public computers. You can install an entire operating system onto a USB drive along with software and a Web browser. Then if you need to use a public computer, you can reboot from the USB drive and run a system that you know is clean. You are only using the computer's processor and RAM, not its infected software. However, you should double-check the keyboard cable to ensure no one installed a physical device on the line to capture keystrokes. Of course, you need the operating system and licenses to install the software onto the USB drive.

Threats to Users

What are the primary security threats faced by individuals? Business face threats to data and servers, but they also face threats to user computers. Individuals face similar threats to their personal computers. Overall, the main threat is that an attacker can take over the computer—gaining administrator access to see all of the data and use the computer for any task. Several bad outcomes can arise from this threat. Your data and passwords can be stolen—resulting in someone impersonating you and stealing your money or trashing your reputation. By monitoring your use of the computer, the hijacker can steal credit card and bank account data. The attacker could also turn your machine into a zombie that is used to attack other computers. Or, it could be used to commit crimes—that would then be traced back and blamed on you.

Several methods are used to attack individual users. Some of them are difficult to detect and hard to prevent. All of them require users to be cautious and pay attention to their computers. Can you see the problem? Many people treat computers as simple machines that handle basic tasks and never need attention. Software and operating system vendors (notably Microsoft) have attempted to automate many of the maintenance tasks to ensure they get handled properly to protect user computers. But, from the perspective of society, it is not possible to protect all computers.

Virus/Trojan Horse

Everyone should know the ancient story of the Trojan Horse, where Greek soldiers hid inside a giant wooden horse which was then brought into the walls of the city of Troy—leading to the destruction and downfall of the city. In computing terms, a program or complex data file might contain a special section of code designed to take over your computer. When you run the program, the hidden code executes with your permissions and can take over your computer. A computer **virus** is a special Trojan Horse that first copies itself into other programs, and then tries to spread every time those programs are run. One complication is that many applications support macro programming languages, such as Microsoft's Visual Basic for Applications, where code is stored and executed within data files or Web pages. These programming languages provide powerful features to integrate applications but they provide even more opportunities for nasty code to sneak onto your computer.

As shown in Figure 5.5, the virus code can be difficult to spot. A virus can be picked up from many sources, but e-mail attachments are the prevalent method today. The obvious solution would seem to be the same as for the original Trojan Horse: Look inside the program to see if soldiers are hiding there. Of course, a person would never be able to look through the hundreds of thousands of files and programs on a computer by hand. Instead, antivirus software is used to scan your computer by looking through every single file. But the second complication is that it is difficult to recognize a virus. The most common approach is to keep a signature list of all known viruses and check every line in every file against every possible known virus.

Viruses and Trojan Horses remain a threat despite the use of antivirus software. The reasons are clear when you understand how the antivirus software works. For the most part, the software works on existing, known viruses. Anything new or anything that modifies itself can sneak through. Additionally, with the huge number of files and the growing number of known viruses, the antivirus software can take a substantial amount of processing time—which can slow down your computer. The software can also make it difficult to install, update, or create new software. Many commercial software packages even recommend disabling the antivirus software before attempting to install anything. Consequently, antivirus

Reality Bytes: Brute Force Password Attacks Using Amazon

Brute force attacks on passwords have always been a possibility—where a computer tests every possible combination of letters and numbers to find a password. But, with reasonable passwords, brute force attacks historically would take many years to find. The obvious solution is to split the task across multiple computers. Still, an attacker would have to find a way to get access to thousands of computers. With cloud computing, anyone can buy cloud computing time, such as that from Amazon's Elastic Compute Cloud (EC2) service. In 2010, Thomas Roth, a security consultant in Cologne, Germany, used a cluster of Nvidia graphics processors through Amazon to test 400,000 possible passwords per second. He used the system to break into a wireless network in 20 minutes at a cost of 28 cents per minute. With some improvements, he says he can break wireless passwords in 6 minutes. Roth noted that "The speed of computers is increasing incredibly fast, and so brute forcing will get faster and faster, and the new cloud offerings make parallelization of such use tasks easy and affordable,"

Adapted from Stuart J. Johnston, "Researcher Breaks Wi-Fi Passwords Using Cloud Computing Power," *eSecurity Planet*, January 12, 2011.

software can help clean files once a virus is identified, but it has not proven very useful in stopping attacks—particularly since new viruses are created every day.

Today, it is easy to create a virus—simply find a virus software kit on the Web, make a few changes, and send it to someone. You would need only minimal technical skills. Of course, it is illegal to create and release viruses and other destructive software (in most nations).

Instead, the best way to stop a virus is to avoid running software acquired from the Internet and to never open script attachments sent to you by e-mail—even if they appear to come from a friend. Be cautious, because some attachments that appear to be pictures are actually virus scripts. Most e-mail services now have filters that can block script attachments, but they tend to be heavy-handed and also block useful files.

Ultimately, the most important step with viruses is to make certain that you always have current backup files. Then, if a virus deletes your files, you can recover the data, run an antivirus software package, and remove the virus. It will cost you time, but at least you will save the data.

The problem with viruses and Trojan Horses is that they often install **spyware**—or software that sits on your computer and monitors all of your activity. It can capture your keystrokes and record Web sites visited, passwords entered, and credit card numbers. As shown in Figure 5.6, periodically, the spyware software sends the information to a Web site where it is collected by an attacker.

Viruses, worms (essentially viruses that do not destroy data), Trojan horses, and spyware are often called **malware**, because they are designed to do bad (mal) things to your computer system. Spyware tools are particularly dangerous on public computers—such as those at Internet cafés, print shops, or libraries. Someone could install the software and capture all of your keystrokes and passwords. You should avoid entering passwords and credit card data on computers that are shared with the public. Microsoft Windows includes software that scans your machine

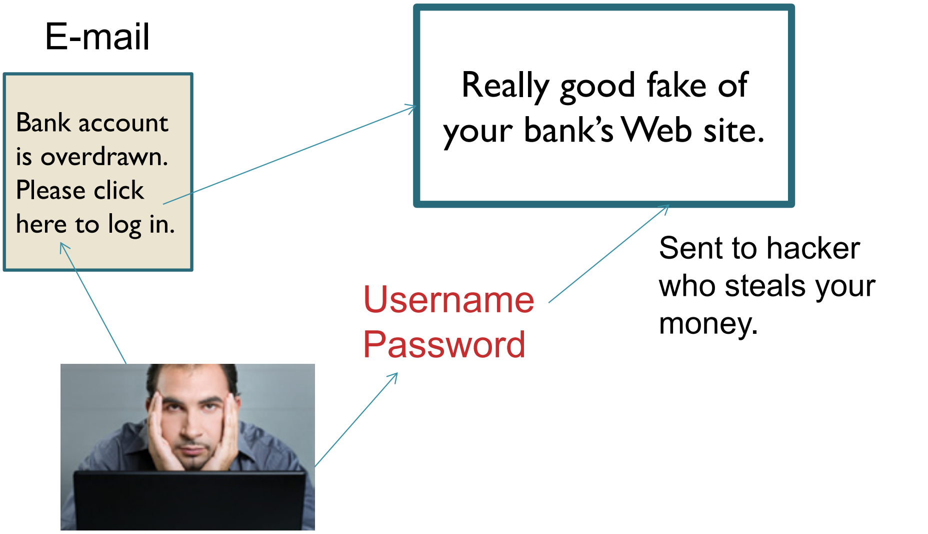

E-mail
Bank account is overdrawn. Please click here to log in.
Really good fake of your bank's Web site.
Username
Password
Sent to hacker who steals your money.

Figure 5.7

Phishing. A fake e-mail contains a link to a fake bank Web site. You inadvertently click the link and enter your username and password. The attackers running the site can now log into the real bank and steal your money.

for some known, dangerous spyware. You can also use the Windows Task Manager to show you what processes are currently running on your computer. If you recognize a malware tool, you can stop the process to shut it down. But you have to be careful, because a standard computer runs many processes. You need to decipher the cryptic names of the processes to understand which ones are good and which ones are bad. It is usually best to use a spyware tool—which contains a list of the known malware tools.

Phishing: Fake Web Sites

Attackers often want to gain access to your computer or at least your credit card and bank account numbers. One attack method is **phishing** for passwords. As a side note, news writers have been converting words beginning with "f" to "ph" ever since the 1970s episodes of phone phreaking—where hackers used various methods to make free phone calls. Figure 5.7 shows one basic method of phishing. An attacker sends mass e-mails pretending to be from a big-name bank. A certain percentage of users will click the link in the e-mail which takes them to a fake Web site that looks like the bank site but is actually run by the attackers. If you do not recognize the fake and enter your username and password, the attackers can quickly turn around and log into the real bank site using your credentials. From there, they can transfer all of your money to their own accounts. Hundreds of variations exist.

If you are always alert and moderately paranoid, you can avoid becoming prey to a phishing attack. Avoid clicking links sent by e-mail. Always double-check the URL of a site that asks for a login. Verify that the security certificate exists and is assigned to the bank. But, some fish are not as smart as others, or you might be tired one night and not pay attention and take the bait.

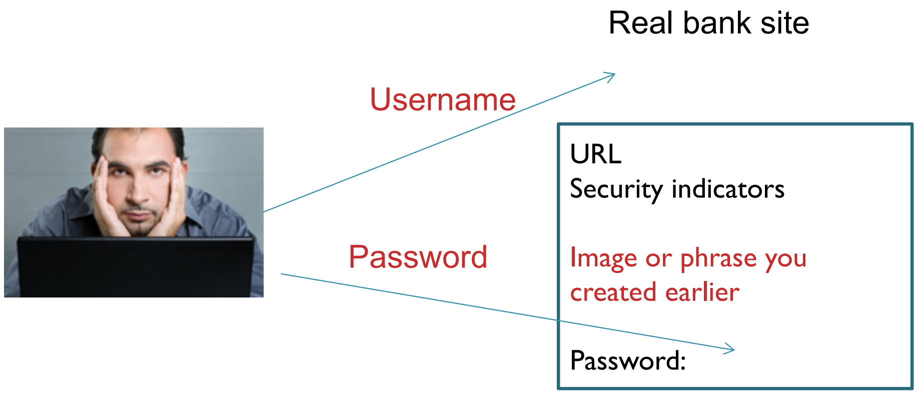


Figure 5.8

Two-step login. Customers enter an image or phrase at the real bank site. In future logins, the username is entered first, which retrieves the matching image or phrase. If the customers recognize the image, it is safe to enter the password. Fake/phishing sites would not have the correct image or phrase.

Banks have implemented some security features to make it easier for customers to recognize the real bank site versus fake sites. Figure 5.8 shows the basic process of a two-step login. Initially, customers select an image or enter a phrase that is associated with the username. These values are stored on the bank's server and would not be accessible to an attacker. During subsequent logins, the customer first enters the username or ID value for the account. The real bank site retrieves the matching image or phrase. When the customer recognizes the proper display, it is safe to enter the password. Of course, you should never use the same phrase or image for multiple sites. So, customers have to remember one more thing to log in. It is relatively easy for any business to implement a similar scheme, but it ultimately makes it more difficult for people to use the systems. And it raises the question of how far a company should go to protect customers from their own actions. Browsers have tried to implement warnings for known phishing sites, but sites can still get past the warnings. Ultimately, it comes down to people paying enough attention to avoid fake sites.

Updates and Patches

In the past couple of years, one of the favored methods of attacking your computer has been to exploit flaws in the operating system and software running on your computer. Software that was created with sloppy programming practices can create holes for outsiders to exploit. Many of the problems are caused by buffer overruns, where the program allocates a limited amount of memory for data and an attacker enters a carefully crafted entry that takes up more space than allocated. This extra data then overwrites the program code and your computer executes the attacker's code. Microsoft, Apple, and other software vendors have been working hard to find and fix these errors. Periodically, these vendors release patches to their software, which you need to load and install on your computer. The good news is that the companies are actively fixing the problems. The bad news is that every time they announce a problem, the attackers also learn of the issues. You need to immediately patch your computer before the attackers take advantage of the flaw.

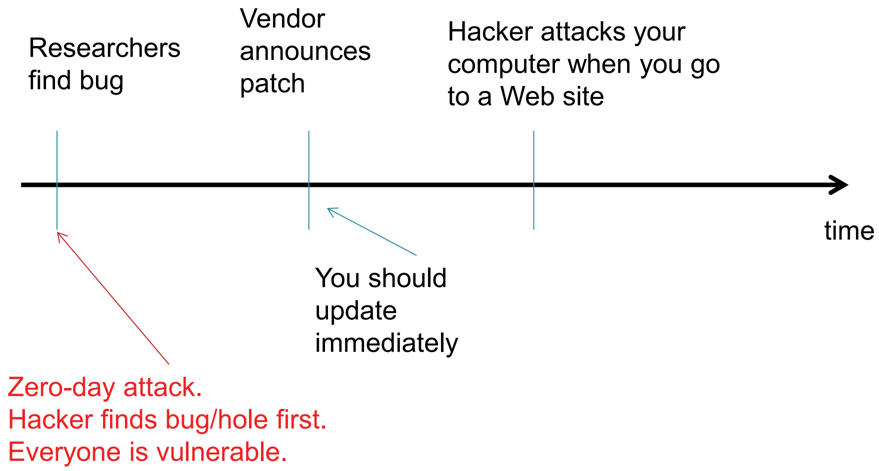

Researchers find bug
Vendor announces patch
Hacker attacks your computer when you go to a Web site
time
You should update immediately
Zero-day attack.
Hacker finds bug/hole first.
Everyone is vulnerable.

Figure 5.9

Zero-day attack. Attackers exploit a known bug or find their own and launch e-mails or even Web sites that can attack your computer. Because the bug has not yet been patched, it is easy for many computers to become infected.

Figure 5.9 shows a basic time line. A vendor or security researcher finds a problem and reports it to the software developer. The developer fixes the problem and releases a patch. Patches are released with varying levels of importance. Critical flaws that could allow an attacker to take over your machine are given the highest priority—particularly if the attack has already been seen “in the wild” or outside of a lab setting. You need to install these updates as soon as possible, and most computers should be set to automatically download and install critical updates when they are released.

This threat is magnified because attackers put scripts on the Internet that automatically scan for unprotected machines. These scripts make it possible for people with almost no computer skills to attack your system. Of course, there is still a risk that attackers can find flaws before software vendors find and patch them. These **zero-day attacks** could happen at any time, but they require considerably more work by the attackers and are likely to be aimed at specific targets. Still, you truly need to keep your system up to date to stop the known attacks. Many of these attacks are based on browsers and add-in software such as Java and Flash.

Intercepted Data

The Web and online content and services continue to be an increasing part of information systems and even daily life. Mobility and wireless connections are also gaining importance. Both of these trends lead to a potentially serious problem: Wireless data is relatively easy to intercept. Any device connected to the same network has the ability to monitor any packet sent on the network. The device is supposed to ignore packets not addressed to it, but it is relatively easy to tell it to capture all packets on the network.

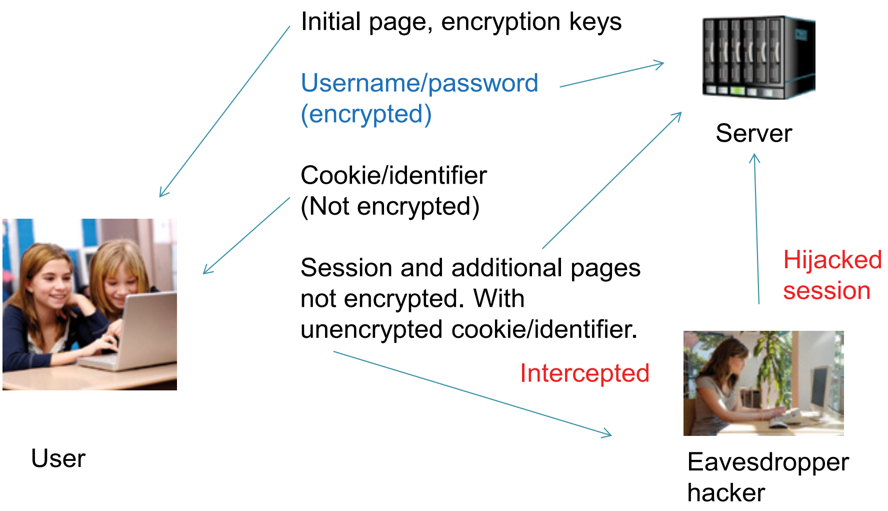


Figure 5.10

Intercept WiFi connections. Often, only the username and password are encrypted for many sites. But the session cookie that maintains the login is often unencrypted and it can be captured—allowing an eavesdropped to hijack the session and make changes as the user.

In late October 2010, Eric Butler released an add-on for the Firefox Web browser called *Firesheep* that makes it incredible easy for anyone to monitor WiFi traffic and hijack sessions from other users. Note, it is illegal to use another's computer account—no matter how easy it is to do. Figure 5.10 shows the basic process. A user signs into a Web service and the username and password are usually encrypted. The server generates a cookie and sends it to the user—so the user identity is maintained for the session without requiring a new login for every page. This cookie and subsequent activities are often unencrypted. The eavesdropper can grab the session cookie and hijack the session—making any changes to the user's account or Web contents.

Wireless transmissions are relatively open and broadcast over an area. The only way to protect the traffic is to encrypt everything. Web servers and browsers are designed to encrypt traffic, but most Web site designers tended to limit encryption to just the username and password pages. The feeling was that encryption slowed down the server, the browser, and the data transmissions. In the early days of the Web, these delays were measurable; so designers got in the habit of encrypting only what they felt were essential items. With faster computers and networks, sites will now be forced to encrypt all transmissions.

But, as a user of Web services, can you do anything while waiting for sites to turn on full encryption? You could simply avoid using any important services while connected to public wireless networks. Browsing Web sites to read the news is certainly not going to matter to anyone. Logging into a social network or e-mail site runs the risk of giving access to an eavesdropper—and with Firesheep, that eavesdropper could be anyone. The only other option is to sign up for a service that provides a **virtual private network (VPN)**. A VPN establishes an encrypted

Reality Bytes: Rogue IT Employees

Fortunately, most IT employees are extremely honest. They need to be honest because they have access to most of the company operations. But, that does not mean you should just ignore employees. Ronald Reagan's famous saying when negotiating a nuclear-arms reduction treaty with the Soviet Union seems to apply to many situations: "Trust but verify." In a different situation involving a Fortune 500 company, a rogue IT employee had "lost" 11 laptops over three years. A flag that should have raised questions earlier. Anyway, in 2008, a retailer in Pennsylvania had to hire a security consultant to investigate a problem after the Business Software Alliance (BSA) reported that the company might be using pirated software. The investigation found that the software was illegal, and that it was sold to the retailer by a company secretly owned and operated by one of its own IT employees. More digging found that the seven-year employee had been running a for-pay pornography site on the company's servers and that he had stolen 400 customer credit-card numbers from the retailer's Web site. And he was the only person who had the administrative passwords. The U.S. Secret Service and CERT provide a whitepaper that lists basic steps you can take to reduce threats from insiders. (http://www.cert.org/archive/pdf/CSG-V3.pdf) To recover the systems, the company sent the rogue employee on a long overnight flight to California, then used the five hours to reset every possible password and lock him out of the systems. When the flight landed, the COO met him at the airport and fired him on the spot. Although a background check might not have prevented the hiring of the rogue employee, it probably would have spotted is lie about having an MBA degree. Other people have suggested that his personality should have indicated some problems. One of the investigators said that "He was extremely confident, cocky and very dismissive of other people." Most good IT employees realize it is impossible to know everything, are willing to consult with other experts, and are helpful to employees.

Adapted from Tam Harbert, "Security Fail: When Trusted IT People Go Bad," *Computerworld*, January 18, 2011.

network from your computer (laptop) to the VPN server. No one can intercept the traffic between those two points. Companies often set up VPN services so workers can securely connect from home into the company network and operate as if they were on site. Several commercial companies provide VPN services to individuals for a monthly fee. If possible, you should test the VPN services before signing onto a long-term contract. You want to ensure that the company has fast and reliable connections and servers that are available whenever you need them. It takes several steps to install a VPN and it might interfere with some applications.

Computer Security Controls

What primary options are used to provide computer security?

Transaction and accounting data is clearly valuable to a company and needs to be protected. Computer security systems need to protect against three general problems: (1) unauthorized disclosure of information, (2) unauthorized modification, and (3) unauthorized withholding of information. These three problems are sometimes referred to as: confidentiality, integrity, and accessibility, leading to the too-cute acronym CIA. As an example of the first problem, you would not want hackers to get access to your customers' credit card data. An example of the second problem would be employees modifying their payroll records to change their pay rates. The third problem is less obvious, but just as important. Imagine what would happen if you needed to look at the latest inventory to decide how much to reorder, but the computer refused to give you access. This problem is often referred to as **denial of service (DoS)** and is a difficult problem faced by Web sites.

User Identification

One of the primary difficulties with providing computer security lies in identifying the user. For years, the most common means of identifying computer users is through usernames and passwords—because this method is easy to program. The programmers simply set up a database of users that contain a username and password. No standards are needed and every system can be independent. More recently, interest in biometrics has been increasing; particularly the fingerprint readers installed on laptops; but the lack of standards has prevented widespread adoption of these technologies.

Passwords

Each user is given an account name and a password that are known only to the computer and the user. If someone correctly enters both the name and the password, the computer assumes it must be the user. This method is cheap, fast, and does not require too much effort by the user. However, there are problems. The biggest difficulty is that users are afraid of forgetting their password, so they choose words that are easy to remember. Unfortunately, passwords that are easy to remember tend to be obvious to other people. For instance, never use the words *password* or *secret* as a password. Similarly, do not use the names of relatives, pets, or celebrities. Most of these can be obtained by looking in a phone book, talking to someone you know, or browsing your Facebook page.. In fact, you should not use any actual words. Most people use only a few thousand words in typical conversation. The goal is to make it hard for someone to guess the password. You need to choose passwords from the largest possible set of characters and numbers. Two other rules about passwords: Change them often and do not use the same password for everything. Most systems have a method to enable you to change passwords. Some systems force users to change passwords on a regular basis, such as every 30 or 60 days.

One drawback to passwords is that you need too many of them. Everything from ATM cards to phone calls to computer accounts uses passwords or personal identification numbers (PINs). It is too risky to use the same password for every account, but it is difficult to remember several different passwords, especially if you choose random letters and numbers and change them often. With so many passwords, it is tempting to write them down, which defeats their purpose. This conflict is the main reason a new system is needed to identify users.

Passwords are not a perfect solution to identifying users. No matter how well they are chosen or how often they are changed, there is always a chance that someone could guess the password. Companies are moving to **two-factor authentication**, where users need a password and a second method of identification. Password generators described in the next section are sometimes used as the second method. .

Figure 5.11

Biometric devices. Several methods exist to identify a person based on biological characteristics. Common techniques include fingerprint, handprint readers, and retinal scanners. The iris scanner is a relatively useful technology since it requires only a camera and is noninvasive.

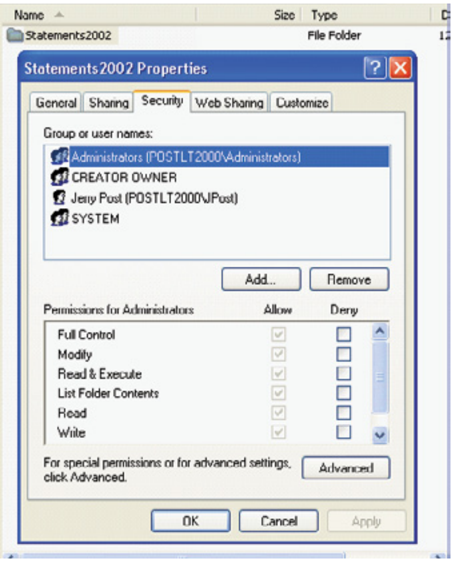
Password Generators

Password generators are small electronic cards that generate new passwords every minute. The same system is embedded on the main computer. When you want to log in, you simply enter the number on the card that you are carrying. Since the password is changed every minute, you do not have to worry about anyone guessing it or intercepting it. On the other hand, you have to carry around the card. You also have to enter a password when you log in to safeguard against loss or theft of the card. However, the password does not have to be changed constantly because the risks are lower. Banks and government agencies have been leading adopters of this technology for providing secure access by employees. The cards are relatively inexpensive, easy to configure, and can be revoked if they are lost or an employee leaves. The technology could become even more useful if it could be integrated into your cell phone. You cannot ask people to carry around dozens of security cards, so it makes more sense to integrate the security into a device they already carry. At this point in time, no one has built software to perform this task, but it would be relatively straightforward.

Biometrics

Biometrics is a field of study that attempts to identify people based on biological characteristics. The most promising devices are fingerprint and handprint readers. As shown in Figure 5.11, there are even devices that recognize the pattern of your iris (the colored ring surrounding the pupil of your eye). These systems work with a simple camera that can be installed cheaply. They are being tested now for identification at airports and in ATMs. The Canadian government is building a large-scale system to handle customs check-in for returning Canadian citizens.

As costs decline, the biggest drawback to biometric security devices is a lack of standards. You can use a fingerprint scanner to log into Windows, and the Windows ID can be used to get access to in-house systems. However, the biometric



Group or user names:

- Administrators (POSTLT2000\Administrators)
- CREATOR OWNER
- Jerry Post (POSTLT2000\JPost)
- SYSTEM

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Figure 5.12

Access control. In Windows, right-click the folder or file to set its properties. Under the Security tab, you can set permissions to any person or group.

data is not used beyond the single computer, and there are no standards for transferring the data securely to other servers.

Biometric security devices have some important advantages. The user does not have to remember anything or carry keys around. They are reasonably accurate and difficult to fool by an unauthorized person. But the industry still needs standards so that the security information can be transferred securely and validated by the final server.

Some of the worrisome issues of biometrics have held back its adoption. Many people are concerned about privacy—the perceived ability of governments to track people if biometrics become widely adopted. Another concern is that to use biometrics, you must first register your information (fingerprint or iris scan) and have that data stored within the system. People worry that if someone steals this data, the thief could use it to impersonate anyone. The assumption is that it is easy to change passwords if they are stolen, but difficult to change your fingerprints. The fallacy to this argument is that the biometric data is never stored in raw form. Instead, a one-way hash is used that converts the raw data into a new, encrypted set of digital data. It is impossible to retrieve the raw data from the stored set. By using unique encoders each time the data is scanned, such as time stamps and fuzzy adjusters, it is possible to prevent these **replay attacks**, where an attacker captures data as it is entered and uses it on a different system or at a later time.

Access Control

As long as the computer can identify each user, you can control access to any piece of data. As manager of the marketing department, you could allow other managers to read the sales data but not change it. Similarly, as shown in Figure 5.12, the accounting department could allow managers to see the accounts pay-able data, but only the accounting department would be able to modify the data and write new checks. With a good security system, it is possible for the human resources manager to allow employees to look up work phone numbers in the corporate database but not to see salaries or other confidential information.

The common access controls available are read, write or modify, execute, and delete. With these security features, the owner of the information can give other users exactly the type of access they need. Windows and other operating systems support additional permissions for folders, so you can control exactly which files people can see, whether they can change permissions, or even deny specific tasks to individuals.

As a creator of data, it is your responsibility to set the appropriate access permissions. Today, most of your files will be shared through a Web site. You can set aside different directories for each group of users and assign permissions to each directory. To avoid accidents, you generally do not give anyone delete permissions. Your main choice is which users should be able to read the data, and which ones need to be able to change it. Of course, if multiple people have permission to change a document, you should set the document to track changes so you can see who made each change.

Administrator Access Rights

Virus, Spyware, and Phishing attacks present difficult problems in terms of security. These attack methods take over the permissions of the user. If you (the user) have high permissions, the attacking software can gain total control over your machine. One of the most common tricks is to install software on your computer that provides back-door access to an attacker. Because the attacking software has your permissions, you would generally not even know the software was installed. In early versions of personal computer operating systems, users were often made Administrators on the computer—giving you complete control over all features of the computer. This permission was generally needed to install new software and new hardware devices. However, it also gives attacking software total control over the computer. In most cases, users should not be included in the Administrators group. Microsoft Vista, and Windows 7 go a step further and ask you to verify the installation of new software. This approach was first proposed in 1987 (Post 1987), and is designed to notify you if an attacker is trying to install software or alter your machine. It can be a nuisance when you first configure a computer, but in daily use, the warning notices rarely appear. If they do, you should think carefully about whether you want to allow the software to alter your computer.

Single Sign-On and Lack of Standards

Figure 5.13 shows one partial solution to the large number of passwords is to use a **single sign-on** method. At least within a company, a central server handles all of the login tasks. For example, Microsoft's Active Directory uses a server based on **Kerberos** to authenticate users. This information is then provided to other servers throughout the company. Users log in once and the security server provides authentication to all of the authorized servers. At this point in time, it is not used for access to Internet sites.

It some ways, it would be nice if this feature could extend to Web sites across the Internet. Once you have logged into your machine, it could authenticate you to other computers on the Internet. This way, you would need only one password—or perhaps even a biometric scanner attached to your laptop. At this point in time,

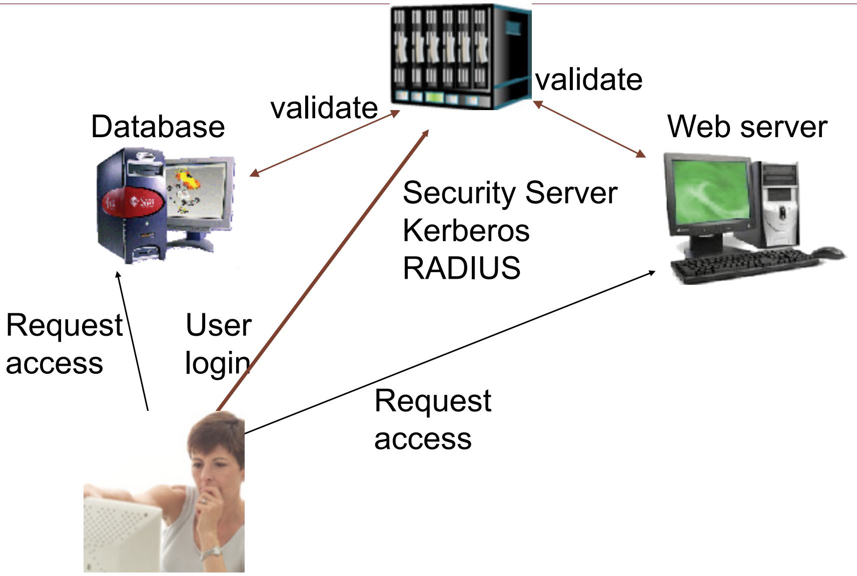


Figure 5.13

Single sign-on. A security server handles the initial login authentication. Any other servers or devices verify the user identification through a token that was issued by the security server.

the world is not even close to this solution. The problem: lack of standards. Few standards exist for collecting, storing, or sharing authentication data. Even if you buy a fingerprint reader for your laptop or cell phone, it cannot be used to verify your identity to external Web sites. So far, almost no work has been done on developing standards to support this level of authentication. The lack of standards is less important within a single company. Within a company, the MIS department has the authority to create and define its own standards, which gives it the ability to purchase and create software so that it can all be integrated. But, it will likely be several years before everyone sits down and agrees to the standards needed to share authentication information across the Internet.

Several vendors provide short-term solutions to manage passwords. Several store your Internet passwords in a file and then provide them to the server when you log in. Most browsers have a similar type of password caching mechanism. A couple of vendors provide USB drive-based solutions that work the same way. Passwords are cached in an encrypted file on the thumb drive and software delivers it to the Web site when you want to log in. Of course, if you lose the USB drive, you will lose your login information, so you need to be careful.

Encryption

How do you protect data when unknown people might be able to find it or intercept it? What additional benefits can be provided by encryption? Encryption is the foundation of many aspects of security. For example, encryption protects messages sent across the Internet and protects files stored on servers. Cryptography has been around for thousands of years, but computers have radically altered the types of codes available. One important

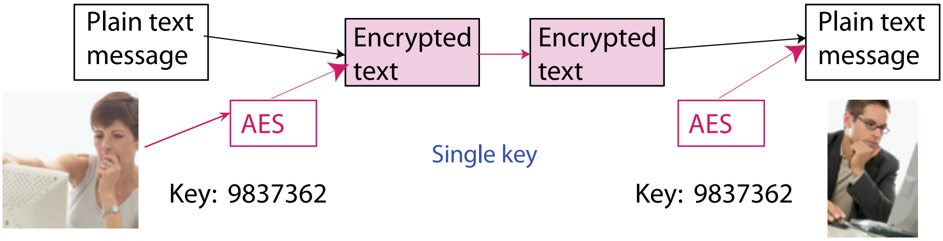


Figure 5.14

Single key encryption. Both the person who encrypts the message and the person who decrypts it use the same key. The systems are fast, but it is difficult to safely distribute the key.

feature to remember in terms of cryptography and computers is the concept of **brute force** attacks. If a hacker knows the algorithm method used to encrypt a message, it might be conceivable to have a computer test every possible key to decode the message. The essence of stopping a brute force attack is to have a key that is so long that it would take millions of years to try every combination. The problem is that computers get faster every year. So encryption technologies that were secure 20 years ago can be broken in hours today. Also recognize that a process that takes a million years could be completed in one year using a million computers. And, today, it is possible to find a million computers to use.

Encryption should be seriously considered for any communications that are sent between computers. Without encryption, it is relatively easy for unauthorized people to deliberately or accidentally read or change the messages. Encryption is available with many personal computer software packages. Almost all spreadsheets and word processors permit you to encrypt your file when you save it. To read it back, you have to enter the correct password. You also can find encryption packages on the Internet that will protect your e-mail messages.

Single Key

For many years, single-key encryption codes were the only systems available. Figure 5.14 shows the basic steps required to encrypt and decrypt a message with a single-key system. Both the sender and receiver have the software that handles the encryption and decryption. Both people also need to have the same key, which is the difficult part. How do you deliver a secret key to someone? And if you can deliver a secret key, you might as well send the message the same way.

On the other hand, single-key systems are fast. They can encrypt or decrypt a message with almost no delay. Since the late 1970s, most of the business world standardized on the Data Encryption Standard (DES). However, this system only supported keys of 56 bits, and by 2000, messages encrypted with DES were broken in under 24 hours by brute force attacks in various contests. Triple DES was popular for a while—essentially encrypting the message three times. But in 2001, the U.S. government chose a new method known as the **Advanced Encryption Standard (AES)** because it is fast and users have a choice of a key length of 128, 192, or 256 bits. Keep in mind that longer keys make the message more secure (harder to break by brute force) but increase the time it takes to encrypt and decrypt the message.

Technology Toolbox: Encryption

Problem: You need to send a file to someone without it being read by anyone else.

Tools: or single key encryption you can use Office and protect the file with a password. Dual-key encryption requires buying and installing certificates. You can also use BitLocker or other commercial programs to encrypt an entire drive or USB drive. The easiest way to secure a data file is to encrypt it by adding a password. With Office 2010, once the document has been created, use the menu: File/Info tab/Protect Document /Encrypt with Password (in the Permissions section). You will be prompted to enter a password and then enter it again to ensure you typed it correctly. The file is encrypted with AES when it is saved and the password is required to open and decrypt it. You can then e-mail the file to someone and not worry about it being intercepted. However, you must still find a way to tell the recipient the password. Obviously, you cannot send it by e-mail. A phone call would be better but not perfect. That is the heart of the problem with single-key encryption.

It is possible to purchase and install digital security certificates to automatically encrypt e-mail. After the certificates are installed, and the e-mail client (Outlook) is configured, e-mail and attachments can be encrypted by checking a single box. The problem is that everyone participating has to obtain and install security certificates and exchange public keys with everyone else. And the certificates usually expire after a year, so everyone has to repeat the process each year. The detailed steps are explained on Web sites that sell the personal security certificates.

A related issue is the need to encrypt an entire drive—either the main disk drive on a computer or a USB drive. Laptops and USB drives are particularly dangerous—every week, thousands of people lose both of these items. Laptops might seem secure—you need a password to log in—but it is relatively easy to remove the hard drive, put it in a case and read the entire drive by plugging the case into another computer. Several encryption programs can be purchased to encrypt the entire disk drive (or volume). Windows 7 (Ultimate and Enterprise) comes with the BitLocker Drive Encryption program. Other systems require you to purchase a commercial program. BitLocker is installed by opening the Control Panel and selecting the BitLocker Drive Encryption option. It works best if the computer has a Trusted Platform Module (TPM) chip, which is often installed in business-level laptops (especially Lenovo). The software requires additional configuration if the computer does not have a TPM—check the Internet for details. Basically, the encryption keys can be stored on a USB drive which must be inserted to startup the computer. The TPM is easier and safer because it stores the key on a hardware chip in the computer. BitLocker is also useful for encrypting USB drives, where a password is required to unlock the drive.

In a corporate environment that uses Active Directory and Group Policies, the BitLocker encryption keys can be stored centrally. The policies can even require that USB drives use BitLocker encryption or the system will be blocked from writing to them.

Quick Quiz:

1. 1. Why would a business want to use encryption?
2. When would it be useful to set up dual-key encryption for e-mail?
3. In a typical company, which drives should use drive-level encryption?

Reality Bytes: Don't be an Idiot

Despite the repeated press reports (and fake actions in Hollywood movies), computer security systems have improved considerably over the past few years. But, a weak link exists in every system: the component between the chair and the keyboard (you). It is easy to break into a system or steal money if you give away your password—or download and run software that gives control to hackers. In a 2010 scam, criminals called thousands of people and ran a basic scam. They claimed to provide free security checks and used a variety of "social engineering" scams to get passwords and account information. Microsoft paid for a survey of 7,000 computer users in the U.K., Ireland, the U.S., and Canada. In total, 15 percent of the respondents had received a phone call from the scammers. In Ireland, the rate was as high as 26 percent. Of those who had received the call, a whopping 22 percent followed the instructions and gave the scammers access to their computers. The victims lost $875 on average (but only $82 in Ireland). Perhaps they will consider it an educational fee. When a random person calls and asks for passwords, accounts, to run software or go to a specific Web site; just hang up the phone.

Adapted from Nathan Eddy, "Microsoft Survey Reveals Extent of Emerging Internet Phone Scam," *eWeek*, June 17, 2011.

Encryption is useful for almost any type of data that you need to protect. For example, you can save a Word document or Excel with a password, which encrypts the document with AES. If you want anyone else to open the document, you will have to provide the password. However, be sure to remember the password. Without it, you cannot retrieve any of the data. A few companies sell software that attempts to crack the Microsoft Office passwords. The process takes a long time if you use long, complex passwords, but keep in mind that these passwords might not be foolproof.

A second common use of encryption is useful for laptops. Windows (and other programs) include the ability to encrypt the entire hard drive. Without encryption, it is possible to remove the disk drive and connect it to another computer—which will be able to read all of the data on the drive. With encryption, the drive is tied to the specific computer, and the data cannot be read without logging into the specific drive. Since laptops are commonly lost or stolen, this level of encryption provides a useful method to protect the data from theft. The integration with Windows makes it relatively easy to install. On the other hand, encryption makes it more complicated to upgrade hard drives.

Public Key Infrastructure

Public key infrastructure (PKI) is a substantial leap in encryption technology. The method arose from a military-political question. Given a U.S. embassy in the middle of a foreign nation that can intercept all communications, how can a secret message be transmitted out of the embassy when there is no way to exchange a secret key? The answer was found by two mathematicians (Diffie and Hellman), and later refined into a system (and company) named after three other mathematicians (RSA: Rivest, Shamir, and Adleman). The solution is to create an encryption system that uses two keys: a **public key** and a **private key**.

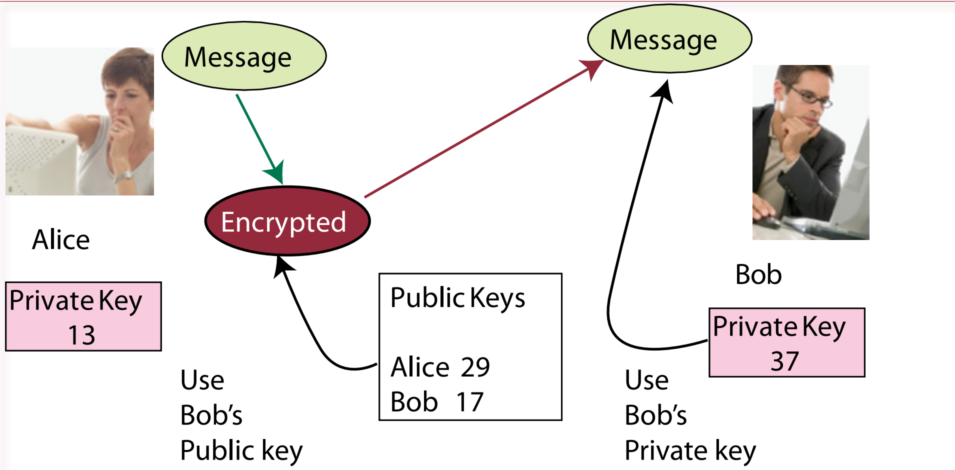


Figure 5.15

Dual-key encryption. Alice sends a message that only Bob can read. With a dual-key system, one key encrypts the message, the other decrypts it. Once Bob's public key is applied to the message, only Alice's private key will retrieve the message. Keys are usually very large prime numbers.

Dual Key Encryption

The essence of a dual-key system is that it takes both keys to encrypt and decrypt a message. Whichever key is used to encrypt the message, the other key must be used to decrypt it. Figure 5.15 illustrates the process. The beauty of the system is that anyone can be given your public key—in fact, this key can be published in a directory. Then, whenever someone wants to send you a secure message, he or she simply uses the RSA algorithm and your public key. At that point, the message is gibberish and can only be decrypted using your super-secret private key. No one can read or alter the message. However, someone could destroy it before it reaches you.

Today's Web browsers use this method to encrypt credit card transmissions. The Web server sends your browser a public key. The browser encrypts the content and sends it across the Internet. Only the Web server can decrypt the contents—using the private key. A similar system called **Pretty Good Privacy (PGP)** is available on the Internet to encrypt e-mail messages.

The one drawback to dual-key encryption systems is that they tend to be slow—particularly for long messages. One common solution is to use dual-key encryption to establish the identity of the parties and to exchange a one-time secret key to be used for the rest of the transmissions. The single-key system is fast and protects the transmitted data, and the initial dual-key system makes it possible to distribute the secret key without anyone stealing it.

Authentication

A second aspect of dual keys has even more uses. PKI can be used for **authentication**. Consider the case where Bob works for a bank, and she receives a message that claims to be from Alice, and it says to pay you $1 million. How does

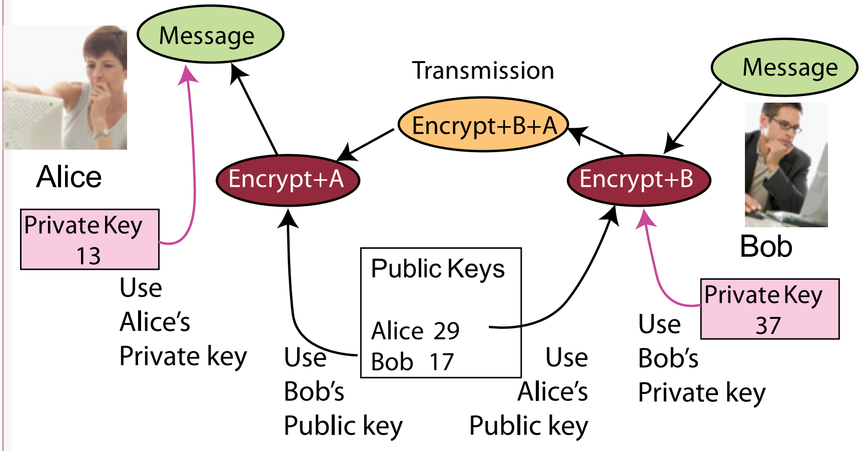


Figure 5.16

Dual-key encryption for message authentication. Alice sends a message to Bob at the bank. Using her private key ensures that the message must have come from her. Using Bob's public key prevents anyone else from reading or changing the message.

Bob know that the message is authentic and not forged by you? Consider the case where Alice want to pay you some money (but only $100).

Figure 5.16 shows the answer. To make sure that only Bob can read the message (and that no one else can modify it), Alice encrypts it with her public key. To ensure that the message is authentic, Alice also encrypts it with her private key. Remember that the keys always work in pairs. When Bob receives the message, she uses Alice's public key and her private key to decrypt it. If the message is decrypted correctly, then it was not modified in transit, and it could only have come from Alice. This process is used to create **digital signatures**. In 2000, the federal government passed a law declaring digital signatures to carry the same legal authority as a traditional signature for legal purposes.

Certificate Authorities

The proper name for dual-key encryption is public key infrastructure (PKI). Why is the word *infrastructure* so important? Think about how a hacker might attack the system in Figure 5.16. What if Alice did not know much about technology and encryption? So, posing as Alice, you create a private key and publish the public key in a directory under Alice's name. Then you send your e-mail message to the bank pretending to be Alice, using "her" public key and asking the bank to pay you $1 million. The message decrypts fine, and Bob believes the message is legitimate. Similar problems can arise by impersonating the bank.

To make the PKI system work, it is critical that the directory of public keys accurately represent the people indicated. So, some organization needs to be in charge of the public directory, and people who wish to use it need to verify their identity before registering a public key. At the moment, several commercial companies operate as **certificate authorities** and sell digital encryption certificates to anyone. Almost no oversight or regulation exists in the industry. At one level, the browser developers (Microsoft) control which companies get listed as trusted root providers in the browser, but there is no governmental regulation. The U.S. mili-

Reality Bytes: Microsoft gets Binged

Just to show that insider theft can happen in any company, Microsoft sued a former Bing toolbar promotions director for allegedly stealing $460,000 from the company and trying to walk away with another $1.5 million. Microsoft claims that Robert D. Curry set up a fake company (Blu Games) and submitted fake invoices for services it never performed. Microsoft claimed that Curry created false documents and even forged his manager's signature. As promotions director, his job was to convince companies to encourage people to download the Bing toolbar to increase the use of the Bing search engine. Microsoft spotted the problem only after Curry convinced the finance department to increase the amount of funds for the project to $3.7 million. He was then going to transfer the $1.5 million to his company through a legitimate vendor (Pentad). But, the size of the transaction apparently caught the eye of internal auditors.

Adapted from Gregg Keizer, "Microsoft Claims Employee Stole $460,000 from the Company," *Computerworld*, January 27, 2011.

tary (and probably others) does run its own certificate servers but those are used only within the military networks.

These public companies, including Verisign and GoDaddy sell **digital certificates** that verify the identity of the person and generate the public/private key pairs. Companies and individuals can purchase these certificates, and you are supposed to verify your identity before receiving the certificate. However, in 2001, Verisign announced that it accidentally issued a digital certificate to an imposter who claimed to be from Microsoft. Eventually Verisign caught the mistake and invalidated the certificate, but the incident points out that the process is far from foolproof. The troubling point is that for the PKI system to work, the certificates and keys must be controlled by a trusted organization.

A handful of public CA firms exist today—leading to some competition in price, but there is still no oversight. In fact, you can easily install a server and generate your own security certificates. These certificates are useful for your own employees. Companies can install them on employee computers and use the certificate to identify a user instead of relying on passwords. Generating your own certificates reduces your costs. However, they are not useful for e-commerce, because your company will not be recognized by the customer's browser. You can look at your Web browser options to see the list of Trusted Root Certification Authorities. This list represents CAs that are automatically recognized by your browser. A certificate issued by anyone else creates a warning message.

Encryption is used in many areas in computer security, but it is not the only factor in security. It is important to protect data during transmission, and it is useful to encrypt sensitive data on disk drives. But, decryption keys need to be stored someplace, so attackers often target those storage locations. So, the security threat simply shifts to a different level. Any security system needs to incorporate multiple levels of protection. Encryption is one level of security that is designed to solve specific problems.

Encryption also presents issues to society—which are covered in more detail in Chapter 14. For now, note that encryption is available to everyone: individuals, businesses, criminals, spies, and terrorists. Consequently, many government

Reality Bytes: Hacker Arrests

The hacker group “Anonymous” obtained huge publicity during the WikiLeaks discussions of late 2010. The group encouraged people to download its software so their computers could be used to attack business and governmental sites. In mid-2011, the Spanish police arrested three individuals claimed to be senior members of the Anonymous group within Spain. A computer found at the home of one of the individuals was alleged to have been used to launch attacks against many Web sites. Anonymous responded by initiating a denial of service attack against Spanish police computers, and denying that the three arrested were part of the group; or that Anonymous was even a group. Earlier, Dutch police arrested two teenagers in December 2010; and the UK police arrest five males in early 2011. In the U.S. the FBI searched homes of several alleged members of Anonymous, but no arrests were made. Turkish police arrested 32 people in early June 2011. In early June 2011, NATO declared that Anonymous and similar groups were a threat to international security.

Adapted from Cassell Bryan-Low, “Spain Arrests Three in Hacker Crackdown,” *The Wall Street Journal*, June 10, 2011; and Ben Rooney, “Turkey Arrests 32 in Hacker Swoop,” *The Wall Street Journal*, June 13, 2011.

agencies want methods to decrypt messages. The U.S. government has proposed several encryption methods that contain back-door keys that would allow agents to decrypt messages easily.

Additional Security Measures

What non-computer-based tools can be used to provide additional security? A fundamental issue in computer security is that logical controls are never enough to protect the computer. For example, anyone who has physical access to the computer can either circumvent the security controls or destroy the data. Besides, many employees have extended access to the data and applications. To be safe, you need to implement some standard business policies. You also need to train users periodically to warn them about new attacks and remind them to never give their passwords to anyone else.

Audits

Accountants have long known that to maintain security over data, it is necessary to perform audits. There are too many ways for unscrupulous people to make changes to stored information. Audits are used to locate mistakes and to prevent fraud. Existing criminology practice states that in many cases, the threat of getting caught (by an audit) will convince most people to be more careful and to avoid fraudulent behavior. The same principles extend to security audits. By monitoring computer activity, auditing financial records, and periodically checking to see whether everyone is obeying security regulations, users are encouraged to follow the security guidelines of the company.

Of course, audits cost money and they interfere with the daily operations of the firm. As a result, it is important to schedule audits carefully and to keep an eye on the costs as well as the potential benefits. Several professional organizations (such as the EDP Auditors Association) can help security employees learn more about the latest technologies and teach them what to look for in audits. The

Reality Bytes: Find the Weakest Point

A common problem in security is that you can strongly protect one point, only to lose because the system is vulnerable at a different location. Security certificates are strong protection for transmitting data on the Internet. The encrypted traffic is extremely difficult to break. But, in 2011, someone, possibly in Iran, was able to obtain server security certificates from Comodo in the names of Google, Microsoft, Skype, and Yahoo. Melih Abdulhayoglu, the CEO and founder of security company Comodo noted that "One of the origins of the attack that we experienced is from Iran. What is being obtained would enable the perpetrator to intercept Web-based email/communication and the only way this could be done is if the perpetrator had access to the country's DNS infrastructure (and we believe it might be the case here)." Fortunately, Comodo identified the attack and revoked the bogus certificates. Browser vendors (Google, Microsoft, and Mozilla) quickly followed by tagging the certificates as invalid within their browsers. The ability to withdraw and flag certificates is an important Web security feature. But it still requires that certificate authorities identify problems and react quickly.

Adapted from Gregg Keizer, "Firm Points Finger at Iran for SSL Certificate Theft," *Computerworld*, March 23, 2011.

American Institute of Certified Public Accountants (AICPA) also provides standards and audit guidelines that are useful at combating fraud.

Physical Access

Because it is so difficult to provide logical security to a computer, other mechanisms have been developed. Many of them rely on controlling physical access to the computer. For instance, computers and terminals should be kept in controlled areas. They must certainly be kept away from visitors and delivery people. Many types of locks and keys can be used to protect terminals and personal computers. Similarly, all documents should be controlled. Paper copies of important reports should be shredded. All financial data is routinely audited by both internal and external auditors. Sometimes hidden control data is used to make sure procedures are followed.

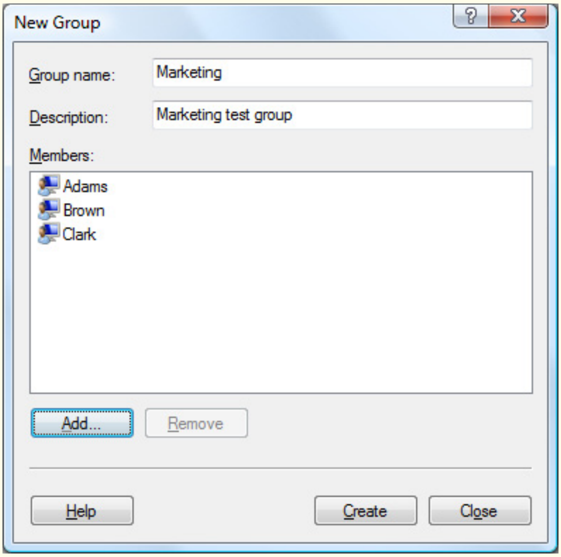
Monitoring

Another effective security provision is to monitor access to all of the data. Most computers can track every change to every file. They can keep a log of who accesses each file. They track every time someone incorrectly enters a password. An audit trail of every file change can be provided to management. That means it is possible to find out who changed the salary data, what time it was changed, and from which terminal.

Remember that every device connected to the Internet is given a unique number as an address. Every Web site that you visit can track this number. In some cases, you can only be identified down to the company you work for, but in many situations, companies can monitor exactly what each machine is doing at any time. Additional software can be installed on computers to provide even more detail—including storing all keystrokes.

Technology Toolbox: Assigning Security Permissions

Problem: You need to share some files with members of the marketing department.
Tools: Windows has the ability to set detailed security permissions on folders and files.



Group name: Marketing
Description: Marketing test group
Members:
Adams
Brown
Clark

In a student lab, you might not have permissions to create folders and set file permissions. Some versions of Vista might not support detailed security options. Browse to a location where you want to put a shared folder. Create the new folder.

In a business setting, the users and groups have probably already been created by the network administrator. If you need to create groups and users, use the Start menu/All Programs/Administrative Tools/Computer Management. If you do not see the administrative tools, you need to enable it by setting the properties of the main taskbar, or use Start: compmgmt.msc /s. Right-click the Users icon and select New User. Make up a username and password for a user. Repeat this until you have three sample users. (If the users are already defined on the network, you can skip this step.) Right-click the Groups icon and select New Group. Name it Marketing and provide a description. Click the Add button and enter the usernames of the three users you just created.

Return to your folder and right-click the folder icon and select the Sharing and Security option. Click the option to share the folder and name it Marketing. Click the Permissions button and Remove the Everyone group. Add the new Marketing group and assign Read permission. Click the Apply button, then click the Security tab. Click the Add button and enter the Marketing group so they have read access. Click the Add button and enter the name of one of the users. Give this person Modify (and Write) permissions. This user will be able to read and change files stored in this folder—the others will only be able to read them. Log on as one of the new users and testing the file permissions. Note, if you are familiar with command-line commands (DOS), you can use the runas command without logging off. When you are finished, remove the Marketing group and users using the Computer Management tool.

Quick Quiz:

1. Why is it important to define groups of users?
2. Why is it important to delete this test group and users when you are finished?

- Audits
- Monitoring
- Background checks:

http://www.lexisnexis.com/risk

(bought ChoicePoint)

http://www.knowx.com/

(also lexis nexis)

http://www.casebreakers.com/

http://www.publicdata.com/

Figure 5.17

Employee background checks are important. For a fee, several websites help small businesses perform basic background checks to verify SSNs and check public criminal records.

Hiring and Employee Evaluation

Because insiders raise the greatest security issues, it makes sense to be careful when you hire employees. Employers should always check candidates' references. In more extreme situations, employers can check employee backgrounds for criminal records. There are several instances of disgruntled employees causing security problems. In many cases, the best security solution is to establish close relationships with your employees and encourage teamwork. Employees who work closely together can defuse potential problems and informally monitor the work of other employees. Figure 5.17 notes that several Web sites will search public records to perform basic background checks for small businesses. Validating social security numbers is an important step for many U.S. businesses.

Computer Forensics

How do you prove the allegations in a computer crime? Sometimes, stopping computer attacks is not good enough. You want to catch the crooks or attackers and have them charged with the appropriate crime. The problem is that you have to be extremely careful when you collect evidence that will be used in a criminal case. In particular, the investigator has to be able to guarantee the authenticity of the evidence from the moment it is collected to when it is presented in court. This process can be tricky with digital evidence. It is not a task for amateurs. You have to bring in a professional investigator to handle the evidence correctly. Of course, few police departments have people trained in computer crime, and they are probably busy chasing murderers and drug dealers.

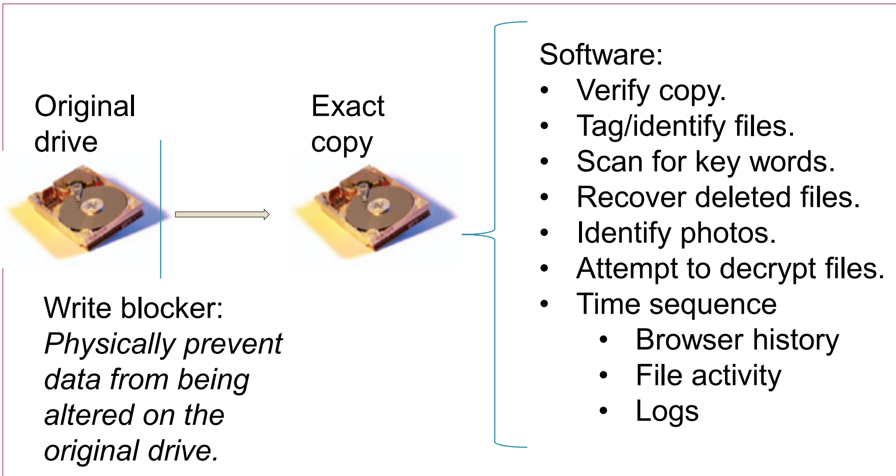


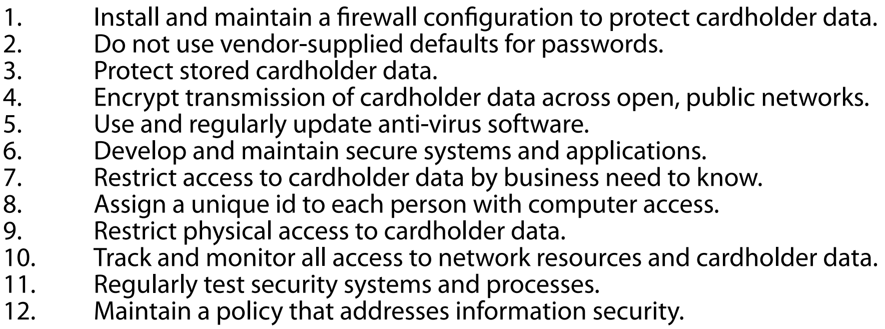
Figure 5.18

Computer forensics. Careful steps must be followed to protect the integrity of the evidence and the chain back to the alleged criminal. Once the data is copied, special software is used to recover deleted files and search for keywords, images, and activity sequences. A human investigator is still needed to interpret the results and direct the search.

Some private companies help with investigations, but make sure you contact your lawyers and the prosecuting attorneys early in the process. Several technical companies exist to help examine computer evidence, such as recovering data from hard drives and decrypting files. Throughout the entire process, you have to keep good records. Most actions have to be logged; and be sure to record the date, time, and people involved. Also, remember that computer logs and backup tapes often get recycled after a certain time, so be sure to maintain secure copies. Figure 5.18 shows some of the capabilities of commercially available forensic hardware and software. Typically, a drive is cloned with a special device to prevent data from being altered on the original drive. Copies of the cloned drive are then created and used for searching. Special software recovers deleted files and performs keyword searches. Photos are often important and are organized by the software. Some software can highlight time sequences based on file dates, computer logs, and the browser history. Increasingly, the challenge lies in the vast amount of data stored on computers. Computerized searches are required to cover the amount of data, but a human investigator is needed to identify keywords and look through potential matches. Even if the computer can find photo and movie files, the computer is not very good at finding objects or classifying images in photos or video. The task of examining computer files is time consuming and highly detailed. But, several job openings are available for specialists trained in computer forensics.

E-Commerce and Cloud Computing Security Issues

What special security problems arise in e-commerce? E-commerce and cloud computing use the same security technologies available to any business. However, some aspects of online businesses are more sensitive and require more careful security planning. These issues are highlighted in this section, with



1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for passwords.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Assign a unique id to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Figure 5.19

Payment card industry security rules. Any merchant or business that handles credit card data must agree to abide by these rules. Source: https://www.pcisecuritystandards.org

a discussion of the common solutions. The earlier sections already covered the issues of data transmission and the importance of encryption. Most Web sites use dual-key encryption through a system known as **secure sockets layer (SSL)**. Online Web services should use SSL for all communications. Servers also need to be protected against direct attacks. One layer of protection is provided by segmenting the network holding the servers using firewalls. Additionally, intrusion detection and prevention methods can be used to monitor for various attacks. One other serious problem is denial of service attacks—which are difficult to solve for an individual company.

Theft of Data from Servers

Because of the powerful encryption systems available, interception of transmissions is a relatively minor problem—as long as you use the encryption techniques. Instead, the servers connected to the Internet have become tempting targets. Several incidents have been reported of hackers stealing millions of records of customer credit card data from e-commerce firms. While credit laws protect consumers, the loss of a credit card is still painful and time consuming. In addition, the e-commerce firm faces liability issues if it did not adequately secure the data.

Securing servers uses the same technologies as any computer system: (1) make sure the latest operating system patches have been applied, (2) set access control rights to the smallest number of people possible, (3) encrypt the sensitive data, (4) hire trusted employees, and (5) monitor access to the sensitive data. A sixth step (firewalls) is explained in a later section. Figure 5.19 shows the primary categories that are required by the major credit card companies. Merchant banks and the card companies require vendors to agree to these conditions or they will not allow you to handle credit card data. They also require you to pay for periodic tests by an outside approved company. No support or negotiation is provided for any of the terms. The card companies have effectively become a monopoly in their attempts to push security (and blame) onto the merchants. Consequently, it is increasingly difficult for small merchants to handle their own credit-card processing. Instead, anything less than huge firms should use payment mechanisms through a third-

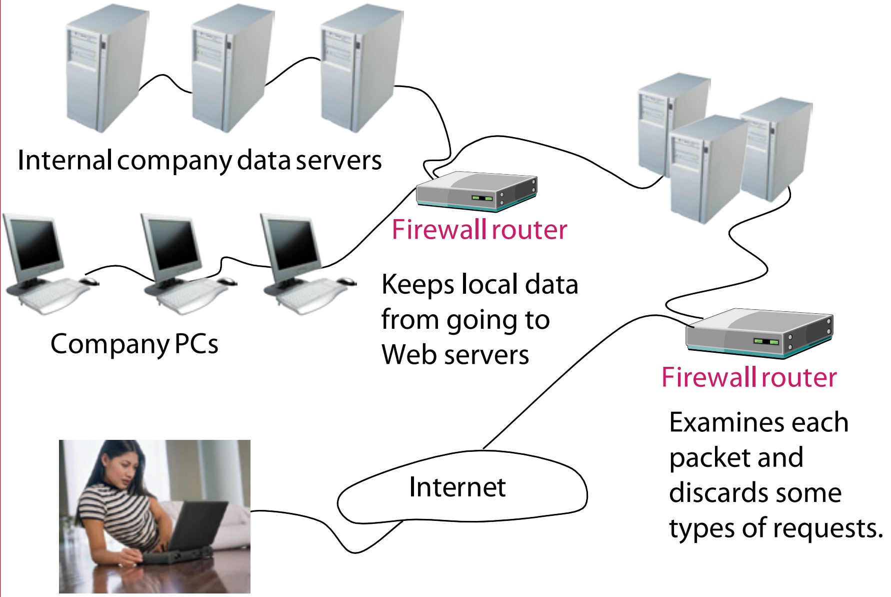

Internal company data servers
Firewall router
Company PCs
Keeps local data from going to Web servers
Firewall router
Examines each packet and discards some types of requests.
Internet

Figure 5.20

Firewalls. Firewalls are packet analyzers that are used to keep local data from moving to the Internet and to limit the actions allowed in from the Internet. Firewalls examine each packet of data on the network and block certain types to limit the interaction of the company network with the Internet.

party, such as PayPal, Google, FirstData, or even Amazon. These firms all charge fees for handling the credit cards, but you avoid most of the risk and the costs of maintaining detailed security systems.

Firewalls

The Internet and e-commerce add some complications to protecting company data. You need to give customers access to some important company data to provide the best e-commerce site. For example, customers like to know if an item is in stock before they place an order. To offer this service, you need to connect your Web server to your company inventory system. But any time you open a connection from the Internet to your company data, you have to be extremely careful to control that interaction. Security access controls and database security controls are two important provisions.

Beyond access control, simply connecting your company computers to the Internet could cause problems within the network itself. You do not want company network traffic being sent to the Internet, and you do not want outsiders to be able to see your internal computers—giving them the chance to try and break into your servers. Figure 5.20 shows how firewalls are used to isolate sections of the network. **Firewalls** are essentially routers that examine each packet of network data passing through them and block certain types to limit the interaction of the company network with the Internet. The Internet protocols were designed as an open network to transport many types of data and to enable computers to connect in many different ways. For example, servers have logical ports on which they listen for re-

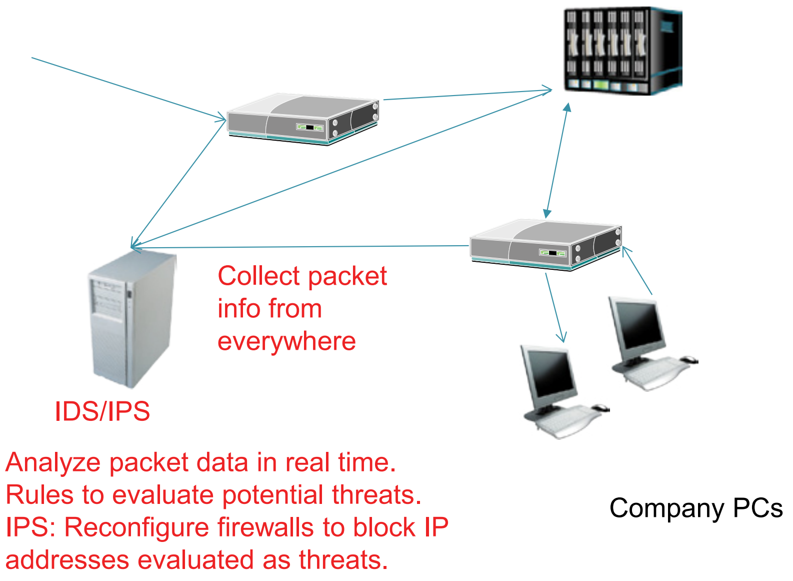

Collect packet info from everywhere
IDS/IPS
Analyze packet data in real time.
Rules to evaluate potential threats.
IPS: Reconfigure firewalls to block IP addresses evaluated as threats.
Company PCs

Figure 5.21

Intrusion detection and prevention. The IDS monitors packets and logs from routers, servers, and special network devices. It has rules to recognize certain attacks and can monitor for changes in traffic patterns. An IPS can shut off a network connection if it detects a threat.

quests. Since only a few of these ports are used for common Internet activities, the firewall is configured to block all of the other ports to prevent outsiders from finding a back way into one of your servers.

Firewalls are also used to segment your network. Internet traffic can be controlled based on a set of rules. These rules can include the IP source and destination address, the incoming and outgoing ports, and the protocol or primary purpose of the packet. By adjusting the rules, security experts can force Internet traffic to specific servers and prevent that traffic from going anywhere else on the network. It is common practice to put Web servers in a special section of the network that only allows certain traffic into and from the servers.

Intrusion Detection and Prevention

Monitoring the networks and servers is an important step in providing a secure system. If nothing else, you need to know if someone has broken into your servers—preferably before the police knock on the door and tell you. As shown in Figure 5.21, an **intrusion detection system (IDS)** is a combination of hardware and software that continuously monitors the network traffic. The hardware is similar to that used in a firewall, but instead of blocking the packets, it performs a more complex analysis. The systems use a set of rules to monitor all Internet traffic and search for patterns. For instance, a common attack often begins with a sweep of a target's network to look for open ports. The IDS observes this repeated scanning, blocks the requests, identifies the source, and sends a warning to the security manager. An IDS is an effective monitoring tool, but the cheaper ones tend to generate too many false warnings.

Reality Bytes: RSA Hack from the Top

RSA Security, a subsidiary of EMC, is one of the big players in computer security. The company was one of the first to develop and sell dual-key encryption and SSL certificates. When the original patents expired and competitors undercut its prices, the company turned to other technologies and services. In particular, the company is known for its SecurID, which is a small device that generates a new password key every minute. The keys are synchronized to the server, so the passwords are only good for one-time use and change constantly. The process makes it relatively difficult for anyone to attack a login to a protected server. So, instead of attacking the protected computers, in 2011, hackers went after RSA itself. Apparently, someone was able to breach the security and obtain access to the underlying keys. These attackers then used the data to break into computers at defense contractor Lockheed Martin. Not long after, RSA issued millions of replacement security tokens for virtually every customer.

Adapted from Siobhan Gorman and Shara Tibken, "Security 'Tokens' Take Hit," *The Wall Street Journal*, June 7, 2011.

An **intrusion prevention system (IPS)** begins with an IDS but adds the ability to shut down a network connection that has been identified as a threat. For instance, if the system detects a repeated scan from a specific IP address, it will set a rule in the main Internet router and tell it to discard any incoming packets from that IP address. Typically these blocking rules are set in place for a specific amount of time and then released after the immediate danger has passed.

The main problem with and IDS and an IPS is that servers today are constantly under attack. An IDS will identify almost continuous scans of various types from around the world. An IDS that triggers alerts for every one of these attacks would constantly be sending out warnings. Humans would be overloaded and ignore the warnings. Using an IPS to block out some of the obvious scans is a partial answer. But, remember that many organizations use network address translation—which means IP addresses are shared and reused. So, if a crazed lunatic from a large university uses a PC to scan outside servers, the IPS on that server could respond by blocking the server for a large chunk of users at that university. The problem with an IDS and IPS is that it is difficult to draw this line between identifying attacks and allowing people to use the servers.

Denial of Service

Denial-of-service attacks have gained importance in the last few years. The essence of an e-business site is the ability to reach customers 24 hours a day. If someone floods the site with meaningless traffic, then no one can use the service and the company may go out of business. Several variations of DoS have been used in the past couple of years, sometimes dragging down large chunks of the Internet at one time. Most of the techniques take advantage of flaws in the Internet protocols or in their implementation on a particular type of server. Figure 5.22 illustrates the process. A hacker breaks into some weakly protected computers and loads a special program that is hidden. On a signal, the machines all send requests to the targeted server. With some known Internet design flaws, these messages can

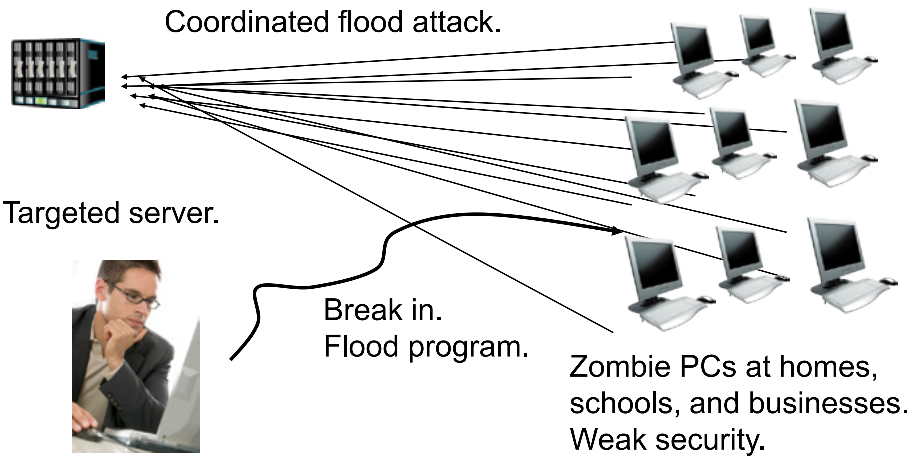

Coordinated flood attack.
Targeted server.
Break in.
Flood program.
Zombie PCs at homes, schools, and businesses. Weak security.

Figure 5.22

Denial of service attack. A bored hacker first breaks into weakly protected home and school systems and loads a hidden program on thousands of machines. At a signal, all of the zombie machines send messages to the server, preventing everyone else from using it.

be multiplied so that a few thousand messages become millions and bog down the server. This type of attack is hard to trace to the original source unless investigators find monitor logs on the zombie machines. Several Internet sites provide simplified instructions on how to perform these attacks, so even weak hackers or "script kiddies" can create havoc.

In many cases, a hacker has to break into thousands of computers to turn them into zombies that can be used for DoS attacks. Some attackers use scanning tools to search for PCs that lack critical updates and then attack individual computers. These attackers then install their software and link the computers to a central server that sends control messages to the zombies. The attackers can then lease these botnets to other hackers. An interesting twist to this process arose in 2010 and 2011 during the release of war data and an investigation of Julian Assange, the founder of Wikileaks. A hacking group (Anonymous) decided to use their botnet to attack Web sites of people and organizations that were critical of Wikileaks. They also decided to expand the size of their botnet by letting people volunteer to have their computers become zombies. Of course, they did not use those terms, but apparently, some people did volunteer. Voluntarily adding your computer to a botnet conducting illegal activity is a really bad idea.

Stopping a DoS attack on your servers can be exceedingly difficult. Most companies will not have the resources to deal with the attack. The goal of DoS is to flood the network and servers with activity. One answer would be to add servers or network capacity to handle the load. One possible solution is to pay for cloud services such as Amazon's EC2 which spreads the processing across multiple servers in many locations and has multiple Internet connections around the globe. But, servers and bandwidth cost money, and the flood attacks could dramatically increase these costs.

Reality Bytes: Anything on a Network has Security Risks

In April 2011, Sony realized that someone had hacked its game network and taken complete control over the server. The network was used to run the PlayStation video-game service for more than 75 million customers. Sony had to take the entire system offline and rebuild many of the components. It took almost two months to restart the network. Later, Sony found attacks on a second network. Nintendo also found attacks against its game network. Many early networks were built without security as a primary component. Taking security on as an afterthought often causes problems. In June, Sega confirmed that its gaming network had also been attacked and that almost 1.3 million people lost their personal information. However, the Sega personal information was mostly limited to name, birthday, and e-mail addresses. The company uses external credit card processors to handle payments and does not store any financial data on its own servers.

Adapted from Ian Sherr, "Sony Shuts Down PlayStation Network Indefinitely," *The Wall Street Journal*, April 25, 2011; and Daisuke Wakabayashi, "Sega Confirms Cyberattack," *The Wall Street Journal*, June 19, 2011.

Occasionally, researchers and Internet-based companies will call on people to find a way to reduce the threat from DoS attacks. For a while, it was suggested that ISPs should be responsible for their clients. In a way, the imposition of data caps by ISPs is a response to this threat. If a client computer is spewing huge amounts of data—it is likely that this data is bad, either as spam or DoS attacks. The ISP should be able to recognize these offenders and shut them down. Of course, ISPs are reluctant to shut down paying customers; however, they are finding it easier to bill them more money for excessive use. In effect, these actions push the responsibility back to the owner of the computers. Microsoft helps users a little by embedding tools into Windows to monitor from some known highly-active spyware and botnet tools. In the end, it makes sense to use economics to encourage people to monitor their own computers.

Privacy

If you have to track everyone's computer use to improve security, what happens to privacy? Computer security is a complex topic. One of its most challenging aspects is that many of the tools available to improve security can also reduce individual privacy. For example, a single sign-on system used across the country could be used to track people through their purchases, when and where they used a computer, when they passed through toll booths or boarded planes, or almost anything else. Even without single sign-on, the security systems enable companies to track detailed usage by employees and customers.

These issues are explored in detail in Chapter 14. For now, you need to remember that many proposed security controls scare even honest people—because of the loss of privacy. As a businessperson, you must be aware of these problems and establish policies to minimize the effects and keep customers happy.

Summary

Companies have to trust employees, consultants, and business partners, but this group presents the greatest security threats. To maintain secure systems, companies often perform background checks on employees, separate tasks so multiple people can observe the work of others, and monitor financial transactions. Natural disasters are a threat to the physical assets, but their business damage can be minimized by having continuous backups in different locations. Cloud computing makes these facilities available even to small companies. The Internet provides more avenues of attack for outsiders—particularly through phishing schemes and attacks on unpatched systems. The best defenses are to install all current operating system patches, to assign access rights carefully, and to monitor the computer usage with an intrusion detection system. However, denial-of-service attacks are particularly hard to prevent.

Encryption protects data during transmission. It is particularly useful for sending credit card data over the Internet. It can also be used to provide digital signatures that authenticate users to validate the source of messages. If computer crimes are detected, the law requires careful collection and analysis of the data using validated computer forensic tools. Experienced experts are generally required to conduct these investigations.

A Manager's View

Computer security is a critical issue for any company. For Web-based businesses, careful controls and continual vigilance are mandatory. Information systems have many potential weaknesses and threats. But overall, electronic security can be stronger than any other form—if it is maintained by experts. Encryption is a key component in securing systems, communications, and protecting privacy. The drawback to security is that it imposes limits on employees and customers. Some tasks become more difficult and some loss of privacy occurs. To protect corporate and personal data, we have to be able to trust the people who collect the data.

Key Words

Advanced Encryption Standard (AES)
Application service providers (ASPs)
Authentication
Biometrics
brute force
certificate authorities
cold site
denial of service (DoS)
digital certificates
digital signatures
Firewalls
hot site
intrusion detection system (IDS)
intrusion prevention system (IPS)
Kerberos
malware
phishing
Pretty Good Privacy (PGP)
private key
public key
replay attacks
script kiddie
secure sockets layer (SSL)
single sign-on
social engineering
spyware
two-factor authentication
virtual private network (VPN)
virus
zero-day attacks

Web Site References

Computer Crime

CERT	www.cert.org
Computer Crime Research Center	www.crime-research.org
Computer Security Institute	www.gocsi.com
FBI: Internet Crime Complaint	www.ic3.gov
Interpol	www.interpol.int/Public/TechnologyCrime
US CERT	www.us-cert.gov
National Security Agency	www.nsa.gov
Department of Justice/cyber crime	www.cybercrime.gov

Review Questions

1. What are the primary threats to information processed by computers?
2. How do viruses spread over the Internet? How do you stop them?
3. Why is data backup the most important aspect of security?
4. How do you protect yourself from false Web sites?
5. Why is it important to ensure updates and patches are installed soon after they are released?
6. What methods are available to identify computer users?
7. What are access controls and how are they used to protect information?
8. What are the advantages and disadvantages of dual-key encryption compared to single-key encryption?

9. How can dual-key encryption be used to authenticate a message?
10. Why are certificate authorities so important in a public key infrastructure?
11. Why do we not have a better system to identify users of Web sites?
12. What threat are audits trying to protect against?
13. If you wish to investigate a computer attack, what is the most important rule you need to follow?
14. What are the main issues in protecting e-commerce Web sites?
15. Why are wireless transmissions more of a security problem than wired systems?
16. What is a denial-of-service attack? Why is it so important in e-commerce? Why is it so difficult to prevent?
17. What is a firewall and how does it protect a company from Internet attacks?
18. How does an intrusion detection system work?

Exercises

1. Run Windows update on your computer and select the custom option. How many updates are available? List them. Do the same for Office update.
2. Review newspapers, magazines, and Web sites and find one case of an actual security problem, such as theft of data. If possible, identify the value of any losses and whether the criminal was caught. Summarize steps that could have been taken to prevent the incident.
3. Find at least two biometric login devices and their prices.
4. Research the current access control methods provided by your favorite social network site. Briefly describe how you would assign permissions to two sets of data to two groups of people. Group A can see the first set of items but not the second, and group B can see the second set but not the first.
5. Research the status of password-crackers. What length of password can be broken in a reasonable time (say less than a month)?
6. Assume you are running a small business that needs to hire employees. Find a site that you can use to do a simple background check on the applicants. Explain why you chose this site.
7. The hacker group *Anonymous* uses software to stage denial-of-service attacks against various targets—often political. Unlike most attackers, the group sometimes publicly invites people to "sign up" and add your computer to its group of attackers. Explain why it would be a bad idea to join this organization.
8. Talk to a friend or relative who works for a large company and ask about the types of monitoring that the company performs on its employees.

9. Use the Windows Task Manager to list all of the active processes on your computer. Search the Internet to identify the purpose of at least ten of the processes.

10. Assume you have a server with about 500 gigabytes of data. Identify the hardware and software you could use to make backups. Be sure to specify the price and estimate the amount of time it will take to back up the data.

Technology Toolbox

11. Write a short paragraph or spreadsheet. Encrypt and save it and e-mail it to a teammate. Identify a relatively secure way to exchange the password.

12. Find out if your computer has a Trusted Platform Module (TPM) that could be used with BitLocker drive encryption.

13. Most computer systems have administrator accounts that provide complete access to the computer for at least one person. Briefly explain what security issues this might cause.

14. Use the Web to find the best price on a security certificate that you can install on a business Web server. Assume that you will need the server for at least five years. To be safe, check your Web browser to ensure that the certificate authority is listed in the Trusted Root certificates.

15. If you have the appropriate network permissions, or using your own computer, create a Marketing group and three users on your computer. Create a folder and set the permissions so that the Marketing group can access the files in the folder. Add your instructor to the group and include a test file that he or she can read.

16. Check the security permissions on your computer—particularly the My Documents folder (or wherever you store most of your files). Is the folder secure or should you set different permissions?

Teamwork

17. Create a subdirectory on a computer that enables you to set access rights. Select a user or group and set permissions so members of that group can read the data but cannot change it. All other users (except yourself) cannot read the data.

18. Conduct a small survey of students (not in your MIS class). Find out how often they back up their data, the last time they updated their operating systems, and how many of them have been infected by a virus in the last 6, 12, and 24 months.

19. Create a simple chart in a spreadsheet and encrypt it. Send a version to each person on your team using a different password/key so that they can add a couple rows of data and return it. Combine the results into one spreadsheet. Comment on any problems you encountered.

20. As a group, create a list of questions that you would ask a potential employee who is interviewing for a job as a computer security expert at your company.

21. Each person should describe a movie scene or TV show episode that involve some type of computer security or attack. Explain whether the event is realistic. Swap the descriptions with team members and have each person add a list of actions that could be taken to prevent the attack.

Rolling Thunder Database

22. What privacy problems might exist at Rolling Thunder? What rules or procedures should you enact to avoid problems? Write a privacy statement for the company.

23. If Rolling Thunder Bicycles adds an Internet site to order bicycles and deal with customers, what security procedures should be implemented to protect the data?

24. Research the costs and steps involved in setting up a secure Web server for Rolling Thunder that can be used to sell bicycles over the Internet.

25. Write a disaster plan for Rolling Thunder. Identify how the backup tapes will be handled and the type of system you will need if a natural disaster hits.

26. Identify and briefly describe the top security threats that would be faced by Rolling Thunder. Outline the primary steps you would take to reduce the risks.

27. Particularly in terms of security, would Rolling Thunder be better off just hiring a company to build and run an e-commerce site?

Additional Reading

Bequai, August. *Technocrimes*, Lexington, MA: Lexington Books, 1989. [Security Pacific and other cases.]

Harriss, H. 1999. "Computer Virus Attacks Have Cost Businesses $7.6 Billion in 1999." Computer Economics Report dated June 18, 1999. (http://www.info- ec.com/viruses/99/viruses_062299a_j.shtml) [Increased costs of virus attacks.]

Faltermayer, Charlotte. "Cyberveillance," *Time*, August 14, 2000, p. B22. [Worker monitoring statistics.]

Forno, Richard and William Feinbloom. "PKI: A question of trust and value," *Communications of the ACM*, June 2001, vol. 44, no. 6. [A good summary of the difficulties of trusting public key certificate authorities.]

Feig, Christy. "Medical privacy rules to take effect," CNN, April 12, 2001.

http://www.cnn.com/2001/HEALTH/04/12/medical.privacy/index.html?s=2 [Notice of new federal medical privacy rules.]

Ashley Fantz and Atika Shubert, “WikiLeaks ‘Anonymous’ Hackers: ‘We Will Fight,’” CNN Online, December 9, 2010. http://articles.cnn.com/2010-12-09/us/hackers.wikileaks_1_julian-assange-arbor-networks-websites?_s=PM:US [Anyone can join a botnet—but that is not a good idea.]

Government Technology, “Ex-San Francisco Network Engineer Convicted of Network Tampering,” April 28, 2010. http://www.govtech.com/security/Ex-San-Francisco-Network-Engineer-Convicted-of.html. [Conviction of Terry Childs for refusing to give up the administrative username/password to the city’s network.]

Gregg Keizer, “New Firefox Add-on Hijacks Facebook, Twitter Sessions,” Computerworld, October 25, 2010. [Announcement of Eric Butler’s Firesheep add-on that captures all unencrypted wireless traffic.]

Oakes, Chris. “Privacy Laws Aim to Protect the Hunters as Well as the Hunted,” *International Herald Tribune*, March 23, 2001. [Good analysis of European Union privacy controls.]

Post, Gerald, “Improving Operating System Security,” Computers & Security, 6(5), 1987, 417-425.

Thurman, Mathias (pseudonym). “What to do when the Feds come knocking,” *Computerworld*, June 4, 2001, 62. [Situation where hacker used a stolen laptop to attack other systems, and computer logs helped show the employee was innocent.]

Whiteside, Thomas. *Computer Capers: Tales of Electronic Thievery, Embezzlement and Fraud*, New York: Crowell, 1978. [Early cases of computer fraud and abuse.]

http://csrc.nist.gov/encryption/aes/ [Reference source for AES algorithm.]

http://www.visabrc.com/doc.phtml?2,64,932,932a_cisp.html [Reference to Visa CISP security.]

Cases: Professional Sports

The Industry

Professional sports raise billions of dollars a year in the United States and around the world. Actually, European professional soccer teams usually top the lists in terms of revenue. In the United States, baseball teams brought in $3.6 billion in revenue in 2001 (“MLB” 2002), basketball teams $2.7 billion in 2003 (“NBA” 2004), and football teams almost $5 billion in 2002 (Ozanian 2003). In 2010, baseball brought in $6.1 billion, basketball $3.8 billion, football $8 billion, hockey $3 billion, NASCAR $0.9 billion, soccer (top 20 teams worldwide) $5.2 billion (Forbes 2011).

These numbers include gate receipts as well as other revenue sources such as television payments. Of course, the teams also have enormous costs in the form of player (and coach) salaries. In total, sports franchises are the most popular segment of the entertainment industry. If you add in the amount spent on gambling (where it is legal, of course), sports are incredibly popular.

Information systems play several roles in sports management. Coaches, players, and scouts use information systems to track performance and opponents, store game files, diagram plays, and communicate information. IT is also used in the front office to sell tickets and merchandise. Like any other business, administrators have to derive financial information and evaluate customers and suppliers. Because of the popularity of the Internet and the role of television, sports teams have also begun to implement sophisticated networks within the stadiums for use by high-end customers.

Since the teams generally use networks to share information during games, security is critical. Any public networks have to be built separately from the team networks. Fans might be frustrated if a public network crashes or is hacked, but a team could be severely crippled if its main coaching system goes down or is compromised.

Additional Reading

Badenhausen, Kurt, “Yankees Soar, Mets Plunge on List of Baseball’s Most Valuable Teams,” *Forbes*, March 23, 2011.

Baseball: http://www.forbes.com/lists/2011/33/baseball-valuations-11_land.html

Basketball: http://www.forbes.com/lists/2011/32/basketball-valuations-11_land.html

Football: http://www.forbes.com/2010/08/25/most-valuable-nfl-teams-business-sports-football-valuations-10_land.html

Hockey: http://www.forbes.com/lists/2010/31/hockey-valuations-10_land.html

Forbes, “MLB,” April 15, 2002.

Forbes, “NBA Valuations,” February 9, 2004.

Ozanian, Michael K., “Showing You the Money,” *Forbes*, September 15, 2003.

Case: Professional Football

Football requires a large number of players, and that means a team needs a large number of coaches. The information technology system becomes relatively more complex to handle the increased number of users and machines. Brian Wright, IT director for the Chicago Bears, notes that "the NFL in general is looking closely at security and how best to protect the information in our business. One of the things we identified was the need for better user authentication" (Vijayan 2004). The team installed a USB authentication key that staff members use to log onto the network. They must also enter a PIN. The strength of the dual-factor authentication is that the PIN is relatively easy to remember, but outsiders cannot hack into the network because they would need the physical USB key.

The Denver Broncos focused on providing more information for fans—particularly the fans who watch the game from the luxury box seats. The IT department installed flat panel touch screens and a high-speed network into every box. Using the GamePlus system, fans can touch the screen and bring up the view from any camera in the stadium. Rick Schoenhals, IT director for the Broncos, notes that "I just know technology is gaining a bigger place in sports venues and sporting events. We're opening a new venue and we don't want to find out someone who opened next week is doing these great things with technology and we're not doing it. We can't be complacent in any area, including technology" (George 2002). The GamePlus system consists of 135 screens. The Broncos are trying to offset some of the costs by selling corporate sponsorships that display logos throughout the game. Because Denver was the first team to implement this type of system, the costs were relatively high.

Local area and wide area networks are important to improve communication within football teams, and many teams were early adopters. The Carolina Panthers installed a 100-mbps network in 1997. Roger Goss, MIS manager for the Panthers, comments on the speed by noting: "We needed that because the coaches create complex graphics, like playbook diagrams and game plans, and download them from servers to workstations" (Wallace 1997). The team also uses frame-relay links to other teams and to the NFL office. The connection is used to share statistics and to notify the league about trades and waivers. With 83 users, the system is heavily used on Monday to Wednesday when the coaches are creating and distributing game plans, and scouting reports arrive for the next opponent.

Sports teams are increasingly aware that fans want up-to-the-minute information on many aspects of the game. In 2000, the Washington Redskins created a Mobile Flash application to offer team news via Web-enabled cell phones and PDAs. Fans can sign up to receive daily e-mail messages about trades, statistics, and player injuries. The Redskins were the first NFL team to implement the wireless system—although others provide e-mail newsletters.

When the New England Patriots built a new 68,000-seat stadium in 2002, the network was a critical element. The voice and data networks alone cost about $1 million. The network uses Nortel Passport switches with a gigabit Ethernet backbone. It links 80 luxury suites and provides more than 2,000 ports at 100 mbps. The network is important to the teams and the fans. It is also important for renting the stadium to businesses during the week. Pat Curley, the IT director, notes that "no other stadium has this setup. It makes it very exciting, and very challenging" (Cummings 2002). The network supports the various coaching and scouting systems used by teams. The Patriots scouts use notebook computers with comments and data uploaded to the central servers for the coaching staff. The coaching system also stores digitized video so coaches can watch specific plays. Pat notes that the coaching system runs on a separate LAN. She says "we've designed everything to be separate so that people who need Internet bandwidth, such as the suite users and press, will have access but it won't conflict with or steal our bandwidth. Plus, it's more secure" (Cummings 2002).

After observing some of the problems that arose in New Orleans with Hurricane Katrina, Bill Jankowski, senior director of IT for the Baltimore Ravens decided it was time to establish a formal backup system for his team's data. Signing a contract with AmeriValut Corp., he transferred 200 GB of data to their servers, and every night ships update changes to their secure systems. For $3,000 per month, AmeriVault stores all of the team's video clips, injury data, and purchase data from the team's SQL-Server based transaction processing system (Fisher 2006).

Data security often extends beyond the digital world. Minnesota Vikings player Michael Bennet learned that the hard way in 2003. He received credit card statements with bills from various convenience stores. But the card did not really belong to him. Instead, an off-duty police officer working as a security guard for the team had stolen various documents from players and applied for credit cards in their names. The identity thief was caught in part from video surveillance tapes taken at one of the stores where he used the card. Several other well-known athletes have had problems with identity theft as well (ESPN 2003).

The high visibility of American football and television seems to attract attention. Just prior to the 2007 Super Bowl, the Web sites of the Miami Dolphin Stadium and the Miami Dolphins team were hacked and loaded with malicious code that attempted to infect any computer visiting those sites. The infection was first identified by customers who had the Websense security software installed on their PCs—it would not allow them to visit those sites because it detected the malicious code. Eventually, the owners of the sites were notified and they cleaned up the attack. Dolphins spokesman George Torres said that "we are working on the technology side to review all the code and do whatever we need to, on a security basis, to prevent this from happening again" (McMillan 2007). The code had links to servers in China that attempted to download Trojan programs on the visiting PCs. The code took advantage of a known exploit in the browser with patches issued by Microsoft.

The Dallas Cowboys were one of the earliest adopters of information technology and analytical tools. Much of the technology and data is now available to all teams, but the Cowboys are still leading the way at storing and handling data. In 2006, the team installed Isilon Systems servers to handle 19 terabytes of video data—enough to hold two entire season's worth of game video online. Video tapes of the games arrive from the NFL on Monday, Tuesday, and Wednesday. Robert Blackwell, director of coaching video for the Cowboys noted that "by the end of the day on Thursday, every game" is converted to digital format and stored in the system. By the end of the year, the system holds video for 263 games. Mr. Blackwell plans to continue adding storage so all video can be kept online and instantly available to coaches. The team also has a backup Isilon system that it carries to training camp (Fisher 2006). In the meantime, the NFL might want to talk with the Big-12 college football teams, including the Texas Longhorns. Instead of flying video tapes around the country, in 2006, the organization selected XOS Technologies to transfer digital copies of the videos to each team via the Internet. Each university in the Big 12 Conference can download entire games in about two minutes per gigabyte of data, or approximately two hours for one game film. Raymond

Thompson, VP of product marketing at XOX Technologies said that “you won’t find anyone in the Big 12 who doesn’t love Internet Exchange because of the time saved and the ease of getting it done” (Rosencrance 2006).

The Dallas Cowboys built one of the newest football stadiums in 2010-2011. The stadium hosted the 2011 Super Bowl and the giant scoreboard /replay screen above the field is only one of the most noticeable technology features in the stadium. In addition to the scoreboards, clocks, retractable roof, and lighting, the IT system runs point-of-sale terminals, ticket sales and so on. The stadium has 3,100 flat-screen televisions to show game scenes throughout the stadium, plus Wi-Fi, IP phones, and 300 IP security cameras. Housed in the stadium is a HP-based data center with 127 HP blade servers, 100 terabyte SAN, and high-speed network. OK, the data center runs team and stadium operations plus operations for team owner Jerry Jones’ 35 other companies. But, the system has a dedicated staff of 13 IT workers (Taft 2011). Other stadiums are adding information features. The Meadowlands installed Wi-Fi capacity to support fans uploading photos and video. For Jets games, fans can access a FanVision device that feeds game stats and customized replays (Patterson 2011).

Questions

1. How can well-known stars protect themselves from identity theft?
2. What threats exist for portable computers used for scouting and how can those risks be minimized?
3. Would fans pay for mobile access to games? How much? What type of network would be needed to handle the data?

Additional Reading

Copeland, Lee, “Redskins Tackle Wireless Access,” *Computerworld*, October 31, 2000.

Cummings, Joanne, “Network of Champions,” *Network World*, July 22, 2002.

ESPN, “Vikings QB Culpepper, four Others Were Victims, August 20, 2003.

Fisher, Sharon, “Football Tackles Disaster Recovery,” *Computerworld*, November 10, 2006.

George, Tischelle, “Football Fans See Games From A New Angle,” *Information Week*, January 30, 2002.

McMillan, Robert, “Sites Scoured of Malware after Offsides Hit,” *Computerworld*, February 2, 2007.

Rosencrance, Linda, “Texas Longhorns, Other Big 12 Teams, Now Swapping Game Films Digitally,” *Computerworld*, September 18, 2006.

Taft, Darryl K., “IT & Network Infrastructure: HP Technologies Drive the Dallas Cowboys’ Stadium,” *eWeek*, January 14, 2011.

Patterson, Thom, “Super Stadiums of the NFL,” *CNN Online*, February 7, 2011.

Vijayan, Jaikumar, “Chicago Bears Boost Network Defenses,” *Computerworld*, May 28, 2004.

Wallace, Bob, "LAN Blitz Sharpens Panthers' Claws," *Computerworld*, September 29, 1997.

Case: Basketball

The summer of 2003 was not a good year for the electricity grid in the northeastern United States. A combination of errors caused the international loop around Lake Erie to overload and shut down the power grid for the entire Northeast. Jay Wessel, the IT director for the Boston Celtics, was attending a picnic at 4:30 P.M., and he notes that when the grid crashed, "every cell phone and pager in the place went off" (Kontzer 2003). Because most of the blackout was focused in New York, he lost only some e-mail servers. Other teams had entire systems shut down. But, it convinced Wessel to look into ways to provide backup in case his facility lost power. The problem he encountered is that most backup facilities were also located in the same areas. He notes that "it doesn't really do me any good to back up my data 10 miles away" (Kontzer 2003). Like many other businesses, Wessel is also looking for solutions to the problems with virus and worm attacks. By keeping systems patched, his losses have been minimal, but he is frustrated with the frequency of patches required.

The Women's NBA teams have added a new twist to marketing basketball. When the Portland Trail Blazers acquired a new team in 2000, management turned to a CRM system to target sales to season ticket holders. They also merged demographic data from external marketing lists and Ticketmaster. Tony Cesarano, database marketing manager, notes that the system significantly improved the efficiency of the sales team and was able to sell 6,400 season tickets in four months. He notes that "in the past, we would have manually keyed the WNBA sales information into a Microsoft Excel spreadsheet, which would have been time-consuming and could have introduced inaccuracies into the database" (Baron 2000). The Trail Blazers are using customer relationship management (CRM) tools to boost sales of season tickets for the men's team. The system has consolidated the data that used to be scattered on spreadsheets of the 50 sales and marketing employees. It tracks individual ticket holders as well as corporate customers. One of the big gains was to minimize overlap, where multiple salespeople often called on the same prospects. The system has proved useful in managing requests by ticket holders to change their seat locations. It can quickly bring up unsold or released seats as well as track priority values of important customers. The organization ultimately expanded the system to their Web site. Cesarano notes that the process is complicated: "We'll have to manage a much larger volume of data coming off the Web. We'll also have to figure out how to clean up the data, to make sure that we're using only useful, legitimate, and accurate data" (Baron 2000).

The NBA in total boasts a fan base of over 50 million people for the 29 teams. In an attempt to boost the level higher, the NBA installed a customer relationship management system from E.piphany. Bernie Mullin, senor vice president of marketing, notes that "we're going to have a 360-degree view of the fans and customers of the NBA. We've never had that before at the league or team level" (Songini 2001). The system pulls data from all of the customer-interaction points: ticket sales, All-Star nomination ballots, the NBA store Web site, individual team databases, and the NBA store in New York. The main focus is to place the data into a data warehouse and provide analytical tools to sell more tickets. The plan is to track sales by various events to answer questions such as whether certain teams provide bigger draws, or if some months or days draw bigger crowds. The main NBA office in Secaucus, New Jersey, has about 1,000 employees. The NBA has several data collection and online systems to maintain. Two staffers attend each game with touch screen laptops to collect data. The data is transferred back to the main system at headquarters in real time. It can be used by fans to create custom highlight reels.

In 2007, the NBA created a site for fans in the Second Life Web site with games, interactivity, and community features. Visitors can gather in an arena to watch a 3D diagram of a game as it is being played in real life. The site also has a copy of the NBA Manhattan store to sell virtual merchandise for player's avatars. Through their avatars, fans can also play games, such as HORSE and a slam-dunk contest.

The Orlando Magic also implemented CRM software to help boost ticket sales. A primary focus of their system is to identify and track customer complaints. If customers have problems, the system can direct them to the appropriate vendor and monitor vendor compliance with contracts. Julie Gory, fan relations and retail manager, notes that "we are a watchdog department that looks at things from a fan's perspective. Whatever happens from when the fan leaves their driveway—everything from parking, the cleanliness of the restrooms—when we hear of issues, we make notes and input them to GoldMine and can review them on whatever basis we want" (Songini 2002). Gory decided not to use the NBA CRM software because it was too expensive—the NBA was going to charge them about $100,000. The system was also more complex and harder to use.

Video is critical to coaches and players. Digital video provides enormous benefits over tape because it can be edited and indexed quickly. The New Jersey Nets were the first team to implement a comprehensive system from Ark Digital Technologies. The system lets coaches quickly grab the clips they want based on various statistics. Ark CEO Alan Kidd notes that "during halftime, coaches could show clips of the first half by type, for example, jump shots or post positioning" (Kreiser 2002). Ark has also created a digital video coaching system. The system can show basic drills. Ultimately, it can be coupled with the game-day videos so players can go to a Web site and compare their performance with the drills (www.arkdigitalsystems.com).

In 2006, the Celtics began actively using analytical software from SratBridge to analyze ticket sales and prices. Daryl Morey, senior VP of operations for the Celtics uses the tool to fill the 18,600 seats by changing prices and offering package deals. He said that "until we had this tool, it was very difficult to create dynamic packages, because our ticke providers didn't have a rapid way to see which seats were open. Now we can actually see in real time every single seat and how much it is sold for." The analytical tool has also revealed that in certain sections fans prefer aisle seating, so the organization has learned to focus on marketing the interior seats for sales promotions (Havenstein 2006).

In 2007, the Atlanta Hawks and Thrashers implemented a new payment system for season ticket holders. Those who signed up for a Chase credit card can use their cell phones to pay for food or merchandise at 200 POS terminals in the arena. Additionally, their phone's Web browsers can read RFID tags embedded in posters in the concourses, directing them to a site where fans can view and download game information, videos, and promotions (Mitchell 2007).

By 2010, the NBA had its own 85-person IT department with a CIO. The team is responsible for game-time issues handling networks and computers, as well as maintaining the NBA Web site and New Jersey tech center on a daily basis. For the finals games, video and stat loggers tag video clips with metadata so anyone can quickly find video clips based on various criteria. CIO Michael Gliedman noted that "We come up with a whole set of metadata that can be used in lots of ways," including by video game developers (Brown 2010).

The NBA produces and distributes an enormous amount of video, with 1.9 billion videos viewed from the NBA.com Web site in the 2010/2011 season. (Los Angeles Times 2011). NBA Digital supports season passes to watch games online and also provides the NBA Game Time app for Android and Apple phones which displays game statistics and scores.

Questions

1. What privacy issues arise from the NBA using a CRM system to track customer purchases?
2. How can the CIO of a basketball team provide backup facilities for a small-to-medium-sized network?
3. How long will it take for digital video coaching technology to be implemented at the college level?

Additional Reading

Baron, Talila, "Team Scores With Apps That Net Ticket-Buyers," *Information Week*, February 21, 2000.

Brown, Bob, "NBA Finals Showcasing Technology as Well as Basketball Skills," *Network World*, March 11, 2010.

Goff, Leslie, "NBA's IT Team Makes Play With Web, CRM Initiatives," *Computerworld*, June 11, 2001.

Havenstein, Heather, "Celtics Turn to Data Analytics Tool for Help Pricing Tickets," *Computerworld*, January 9, 2006.

Kontzer, Tony, "Data Backup: Rethinking The Unthinkable(s)," *Information Week*, August 18, 2003.

Kreiser, John, "Virtual Coaching," *Information Week*, July 22, 2002.

Los Angeles Times, "NBA, a Hit in Online Video, is Looking to Grow in Social Media," April 15, 2011.

Songini, Marc L., "NBA Shoots For Data Analysis," *Computerworld*, May 28, 2001.

Songini, Marc L., "Orlando Magic Shoot for Customer Satisfaction," *Computerworld*, December 5, 2002.

Wagner, Mitch, "The NBA Builds A Second Life Virtual Playground with Potential For Real Fun," *Information Week*, May 5, 2007.

Case: Baseball

Sports fans, particularly in baseball, are often crazy about souvenirs. They will collect almost anything. So, it is not surprising that outdated copies of baseball contracts found their way to an e-Bay auction set up by Scott Gaynor, a sports memorabilia dealer. Bob Tufts, who played for the San Francisco Giants and the Kansas City Royals in the early 1980s, found that his contracts were among those offered for sale. While there is nothing illegal per se about the sale, there was an important twist: As employee contracts, most of the documents contained the social security numbers of the players. With some big-name players in the group (read "money"), the risks were quite high. Bob Tufts observed "I'm shocked to find out how easy it is for people to get their hands on files like these" (Rovell 2003). With a home address, the social security number, and a guess at a mother's maiden name, criminals could have created fake bank accounts. The commissioner's office requested that the auction be stopped and the contracts returned. Some of the bids had reached $200 before the items were pulled.

The Internet is increasingly important for attracting fans to all sports. Since baseball has been number-intensive for years, Web sites are an important source of data on games and players. In 2001, all major league baseball teams agreed to consolidate and standardize their Web sites. All of the sites are now run from the MLB servers. All sites were given a common look. An interesting aspect to the change is that revenue from sales on the site is split across all of the teams. Bud Selig, the commissioner, observed that "the most significant part of our whole Internet activity was the unanimous vote to share the revenue. That was a very dramatic change in thinking, because disparity is the biggest problem we have" [Wilder 2001]. Bob DuPuy, chief legal officer in the commissioner's office adds that "Of course, we agreed to share revenues that don't currently exist. I don't think we could do it at a later date when there was revenue disparity" (Wilder 2001). The site is operated by a separate company created by the team owners and run in New York City. The new organization was initially funded with $1 million a year for three years from each of the 30 teams ($30 million a year). In a somewhat risky move, the MLB site sells video access to games. The risk is that it could alienate traditional television broadcasters—who provide a substantial part of baseball revenues. But the site is still subject to local blackout rules, and the picture quality is not even close to television standards. So, its market would most likely consist of out-of-area fans.

Season tickets present interesting problems for clubs and fans. About 80 percent of them are owned by corporations—particularly the luxury suites. Robert McAuliff, CEO of Season Ticket Solutions, notes that "season ticket holders… miss 25 to 50 percent of games every year" (Rosencrance 2001). The challenge for teams is that filling seats increases revenue through sales of food and souvenirs. The challenge for fans is that they want to efficiently use their investments. The Phoenix Diamondbacks, as well as other teams, have purchased software that enables season ticket holders to manage their seats. The Web site allows ticket holders to check on who is using the tickets, and which dates still have seats available.

Web casting ball games is an interesting legal and marketing area. Are people willing to pay for Web broadcasts? Do they want to select specific games? (Currently, MLB offers a subscription but only to specific games.) Would such a system encroach on television broadcasts? Is there a profit? Many of these questions remain unanswered, and it is not clear that anyone is seriously addressing them yet. In 2000, William Craig and George Simons created a company and the iCraveTV Web site in Canada. The company picked up signals from 17 broadcast stations in the United States and Canada, digitized the signals and offered them for free on its server. Rebroadcasting signals is legal in Canada. But it is a violation of U.S. copyright laws. The company was quickly sued by several U.S. sports agencies as well as the Motion Picture Association of America, because the company did not block the signals to U.S. customers. The company quickly made an out-of-court settlement and shut down the site (McGeever 2000). So, many questions remain about whether fans want to see Internet, or even cell phone video of games. And, if so, how much they might be willing to pay and whether those fees would offset any lost television advertising revenue.

With its experience and in-house staff, MLB has become the leader in Web casting large events. In 2006, more than 5 million people watched March Madness college basketball games on the Web—thanks to MLB technology. MLB sells the services to at least 25 clients, providing a profitable stream of revenue for MLB. Bob Bowman, CEO of MLB.com, observed that "content publishers were being underserved. A lot of companies are having a hard time picking out a digital strategy…Music has iTunes, but that is not a total solution. So it was obvious that we had something if we used it right." (White 2006). Mr. Bowman and others are concerned that the ISPs might make life more difficult for them—the phone companies have stated that they want to charge fees for carrying bandwidth-intensive programs like streaming video. Mr. Bowman notes that "Just receiving a live feed and sending a compressed version over the Web is difficult. We didn't anticipate how in-depth it all was." The 30 MLB teams financed MLB.com with an infusion of $60 million and jointly own the organization. The site relies heavily on Akamai Technologies to distributed the content to its 18,000 servers worldwide—reducing the bandwidth demands on any one server.

MLB.com charges $80 a season for fans to watch almost any live game they choose. The site also uses software from Open Text to store and tag all of the content—providing customers with access to video clips, statistics, and other data in a non-linear format. That is, fans can search for and select events to see, including highlight clips and summaries of games. Justin Shaffer, VP and chief architect for MLB.com noted that "we wanted to take advantage of new media in order to provide a better experience for baseball fans worldwide via MLB.com…As we continue to catalog and distribute exciting game footage for our fans, our partnership with Open Text ensures that we can easily provide those fans with the types of products that match their needs, whether it's game summaries, highlights or other specialized cuts of video" (Rosencrance 2005). In 2009, MLB launched its own network on cable TV. Video from every major league game is routed to the Secaucus NJ studios, compressed into HD and standard definition video and then routed to satellites for transmission by cable companies (Mark 2009).

Once fans are at the stadium, they need to pay for things like souvenirs, food, and beer. And no one wants to stand around fishing for change and signing credit-card slips. The San Francisco Giants were an early adopter of contactless payment readers. Newer credit cards have RFID chips embedded in them and customers simply hold the card a couple of inches from the reader to activate the payment. Not many customers have the RFID cards yet, but it simplifies payments for those who do have them. Ken Logan, IT director, also plans to issue season ticket holders with a special card that gets them into the stadium and handles payments at the concessions by linking through a database back to the holder's credit card. So far, Logan said “the only drawback is just keeping people from spilling a beer on it. They get pretty dirty and sticky” (Mitchell 2007).

Any business wants to track its customers, and baseball is no exception. Teams routinely send out e-mails and promotional information to ticket holders. In 2011, a staffer for the New York Yankees sent a standard newsletter to several hundred season ticket holders. The only problem is that a spreadsheet was attached to the message that contained personal data for 18,000 season ticket holders. The spreadsheet did not contain credit card data but it did have phone numbers, addresses, names, seat numbers, and Yankee account numbers (McMillan 2011).

One of the more amazing technologies to be introduced to baseball was tested in 2009 by Sportvision, a Bay Area company that developed the yellow first-down marker for football. The new camera and software system is designed to automatically track the location of every ball and every player on the field. It will have the ability to generate data on how fast fielders respond to hits, how hard they throw the ball, and other statistics that have never existed before. The data could introduce big changes in how defense is evaluated in baseball (Schwarz 2009). The system was first tested in San Francisco and uses four high-resolution cameras to capture three-dimensional data. Sportvision tested the FIELDf/x system in the San Francisco stadium in 2010 and was preparing to deploy it to other stadiums.

Umpires play a key role in any baseball game. As much as fans like to complain about some of the calls, the talent and knowledge of the umpires is amazing. It takes training and practice to stay up-to-date as a major league umpire. So MLB and IBM teamed up to install special Web-based software to help umpires. Umpires use WebSphere technology to build mashups of the game, calls, and players. They can leave notes for umpires at the next game. The portal lets them view videos of certain plays, help analyze controversial calls, and provide detailed explanations of rulings (Boulton 2008).

Questions

1. How are player privacy rights different from average citizens?
2. What procedures can be implemented to help protect players from identity theft?
3. What are the benefits and drawbacks to centralizing the team Web sites for MLB?
4. How could a team provide individual customized access to baseball games via the Internet?

Additional Reading

Boulton, Clint, “IBM, MLB Connect on WebSphere Web 2.0 Deal,” *eWeek*, July 18, 2008.

Mark, Roy, “MLB Network Launch Powered by Motorola,” *eWeek*, January 9, 2009.

McGeever, Christine, “Webcaster Under Fire,” *Computerworld*, January 21, 2000.

McMillan, Robert, “NY Yankees Staffer Accidentally e-Mails Customer List,” *Computerworld*, April 28, 2011.

Mitchell, Robert, “No Contact: Could Smart Phones Spur Contactless Payment Card Adoption?” Computerworld, June 11, 2007.

Rosencrance, Linda, “Watching the Bottom Line From Box Seats,” *Computerworld*, August 6, 2001.

Rosencrance, Linda, “MLB.com Scores with Open Text,” *Computerworld*, April 26, 2005.

Rovell, Darren, “Confidential Information Pulled From Online Auction,” *ESPN*, June 17, 2003.

Schwarz, Alan, “Digital Eyes Will Chart Baseball’s Unseen Skills,” *The New York Times*, July 10, 2009

White, Bobby, “Major League Baseball Steps Out As Coach in the Game of Web Video,” *The Wall Street Journal*, March 27, 2006.

Wilder, Clinton, “Redefining Business: A New Game Plan,” *Information Week*, April 9, 2001.

Summary Industry Questions

1. What information technologies have helped this industry?
2. Did the technologies provide a competitive advantage or were they quickly adopted by rivals?
3. Which technologies could this industry use that were developed in other sectors?
4. Is the level of competition increasing or decreasing in this industry? Is it dominated by a few firms, or are they fairly balanced?
5. What problems have been created from the use of information technology and how did the firms solve the problems?