CHAPTER 1

Computer Security Concepts

In This Chapter

The CIA triad

Identification, authentication, and authorization

Risk assessment

Security principles

Information warfare

Computer security is a relatively young discipline. After all, the widespread adoption of computers took place only during the past few decades. In the early days of computing, security relied on trust; owners of computer systems hired and directly controlled the system operators and depended on them to behave in an ethical and responsible manner. However, the explosion of networked computing and large-scale information systems has rendered that approach obsolete. Gone are the days when system owners had direct control of all users. We're now in an era in which remote network users comprise a significant portion of the users of many systems. The Internet servers that power the World Wide Web, electronic mail, and other popular services provide resources to a base of innumerable users located around the world.

The majority of a system's users are reliable, trustworthy individuals seeking to use the system for legitimate purposes. Unfortunately, to paraphrase the old adage, there's a bad apple in every bushel. In the 1980s, the stereotypical "bad apple" was an oily-faced teenager who used techniques, such as war dialing (dialing every possible telephone number in an exchange to search for modem connections), to discover and then penetrate as many systems as possible, merely to prove a point. The 1983 movie *WarGames* painted this picture well: Matthew Broderick played the innocent teenager whose hacking exploits brought the Pentagon to its knees and the world to the brink of a nuclear Armageddon. A great real-world example is Robert T. Morris, the famous graduate student who crippled the then-immature Internet in 1988 by unleashing the first worm. (For more details on Morris's Internet worm, see Chapter 9.)

Note

Hackers are not always malicious. Throughout this book, the term *hacker* describes individuals who seek to penetrate the security of a computer system. Note that *hacker* was coined to describe anyone extremely proficient at harnessing the power of a computer. To be designated a hacker was a badge of honor among computer pioneers. Many security professionals use the term *cracker* to describe hackers with malicious intentions.

During the 1990s, the computer security industry witnessed a revolution in the mainstream emergence of the hacking subculture. Hackers suddenly had different motives: greed, ideology, and revenge. In early 2002, a Russian hacker was arrested for attempting to extort $10,000 from a U.S. bank after breaking into one of its Web servers and stealing a customer list with names, addresses, and bank account numbers. Governments are getting into the act too: Almost every civilized nation has some sort of information warfare program designed to cripple the computing infrastructure of an adversary's military. Finally, a huge number of attacks have originated from disgruntled employees and former employees of companies who know and exploit the soft spots in a corporate security policy.

All these developments have forced the rapid evolution of the computer security profession. During the 1980s, computer security was the realm of the military, geeks, and academics. In the 21st century, it's one of the most important items on the checklists of IT executives. Holders of computer security certifications and advanced academic degrees are in high demand as corporations compete for a relatively small pool of qualified professionals.

This chapter takes a look at the basics of computer security — the building blocks of a comprehensive security posture. It covers these concepts in depth:

- Confidentiality, integrity, and availability
- Identification, authentication, and authorization
- Threats, risks, and vulnerabilities
- Security principles
- Information warfare

Admittedly, these are some of the less "sexy" topics in computer security. However, they're the components of an important theoretical base that every computer security professional must possess. Without a firm grounding in these basics, you can't see the big picture as you use the techniques described in later chapters to design and implement a sound security policy for your organization.

The CIA Triad

Information security has three main goals: Maintain the confidentiality, integrity, and availability of information resources. All the lessons you will learn in this book and security mechanisms you will encounter in the real world are designed to enhance at least one of these three principles. Together, they're often referred to as the "CIA triad," as shown in Figure 1-1.

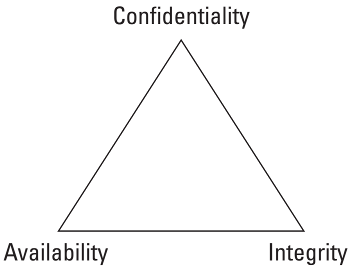

Figure 1-1: The CIA triad.

As you see in Figure 1-1, these three principles each compose a leg of the triad. Computer security professionals must strive to achieve all three because a weakness in one undermines the strength of the entire triad and opens a system or network to exploitation.

Malicious hackers have developed their own triad, the DAD triad, to counter the CIA triad of security professionals. Each leg of the DAD triad is targeted at defeating the mechanisms associated with one leg of the CIA triad:

- Disclosure: Attempts to defeat confidentiality
- Alteration: Attempts to defeat integrity
- Destruction: Attempts to defeat availability

It sounds a little like the old Rock, Paper, Scissors game, doesn't it? I explore each one of these principles of malicious activity as I discuss the legs of the CIA triad they're designed to defeat.

Confidentiality

Confidentiality mechanisms enforce the secrecy of your data. As computer security professionals, you strive to keep your data from the eyes of unauthorized users. A variety of techniques are used to protect data, including

- Access control mechanisms: Prevent unauthorized individuals from accessing the system.
- File system security controls: Prevent individuals authorized to use a system from exceeding their authority and reading confidential information they shouldn't be able to access.

- Cryptography: Can be used to encrypt the contents of sensitive files and protect them from prying eyes, even when access control and file system security mechanisms fail.

Cross-Reference

See Chapter 4 for more information on access controls, Chapters 10 and 11 for more information on file system controls, and Chapter 6 for more information on cryptography.

The opposite of confidentiality is the disclosure of private information to unauthorized individuals. Disclosure can be accomplished by defeating access control mechanisms, violating file system security, or breaking an encryption system to obtain confidential information.

Everyone concerned with data security has some sort of classification policy. In many organizations, it is quite simple: Data is either confidential or it isn't. Other organizations have a formal tiered system in place to denote different levels of protection.

The first, and most famous, data classification scheme is that used by the U.S. government. Much of early computer security doctrine was written by and for the military, so many information systems were designed to implement this type of protection scheme. It was designed to provide increasing levels of security to information, which, if disclosed, would have an adverse impact on the national security interests of the United States. The government information classification structure includes these five classification levels, listed in ascending order of sensitivity:

- Unclassified: This information might be freely shared with the public without risk of damage to national security. This information is subject to public disclosure under the Freedom of Information Act (FOIA). An example of this type of information is a portion of the Code of Federal Regulations.
- Sensitive But Unclassified (SBU): This level is also known as For Official Use Only (FOUO); its information might not adversely affect the nation's security, but it is protected from FOIA release by one of nine exemptions to the law. This designation is often used for private information the government possesses about an individual.
- Confidential: This information would cause damage to national security if released to unauthorized parties. This is the lowest level at which information is considered "classified" by the government and requires all recipients to have formal security clearance.
- Secret: This information would cause *serious* damage to national security if released to unauthorized parties.
- Top Secret: This information would cause *exceptionally grave* damage to national security if released to unauthorized parties.

Private corporations often use similar categories to protect their trade secrets and other confidential information. These categories might have descriptions such as

For Public Release, Proprietary, and Company Confidential. The corporate information security policy should contain a detailed description of the information classifications used by the organization and the types of mechanisms that must be in place to protect information at various levels.

Cross-Reference

See Chapter 2 for more information on security policies.

Integrity

Integrity mechanisms protect data against unauthorized modification, including changes by individuals who don't have permission to modify data and unauthorized modifications made by individuals normally permitted to modify the data.

When data integrity is preserved, the data is called *reliable.* Users can be relatively certain that they are viewing information created by a legitimate source and that no unauthorized modifications have been made.

Several types of mechanisms are used to enforce data integrity. You might find that they are strikingly similar to the mechanisms used to enforce confidentiality. That's no coincidence. Remember that the legs of the CIA triad are interdependent. Therefore, you can use the same security mechanisms to support more than one leg of that triad. Some common integrity mechanisms include

- Access control mechanisms: Prevent unauthorized individuals from accessing the system and modifying data.
- File system security controls: Control the rights of data users. They might grant a large number of users permission to read data but prevent all except a select handful from modifying the data.
- Cryptography: The system of using digital signatures to confirm that a message wasn't altered in transit.

Cross-Reference

See Chapter 6 for more information on digital signature technology.

The opposite of integrity is alteration. Malicious individuals might attempt to alter data for a variety of reasons, including financial gain (such as changing the balance of a bank account) and deception (such as deleting a record that shows a particular person entered a building).

Availability

A frequently overlooked responsibility of security mechanisms is to provide for the availability of data. It's perhaps more obvious that the confidentiality and integrity of data is extremely important. After all, the disclosure of confidential information or the alteration of important data could wreak havoc on a business. However, data doesn't serve any useful purpose if nobody can access it.

Distributed denial-of-service attacks

DoS attacks pose a significant risk to computing systems around the world, especially those that rely on Internet connectivity. Originally, DoS attacks could be blocked by simply finding the source of the attack and filtering out traffic from that range of IP addresses. Hackers would shift from system to system in an attempt to defeat this type of defense, but a diligent administrator could keep the system up and running with lots of hard work. However, the advent of distributed denial-of-service (DDoS) attacks poses a new challenge that is much more difficult to counter. In DDoS attacks, hackers compromise a large number of intermediate systems and install DDoS toolkits on them. When their "army" of infected computers is large enough, they send a trigger signal to all the systems, instructing them to launch a DoS attack against a particular victim. From the victim's perspective, the attack is coming from many different directions and is hard to filter out. Additionally, if the victim attempts to trace back the attack, she first lands at all the intermediate systems, most of which probably had no idea that they were compromised and being used in an attack.

Availability requires compromise. If confidentiality and integrity mechanisms are carried out to an extreme, they might prevent authorized users from accessing data and using it in a legitimate manner. Additionally, hackers might launch an attack designed exclusively to prevent authorized individuals from accessing computing resources. This type of attack, known as a *denial-of-service* (DoS) attack, is quite common. In fact, a well-publicized string of DoS attacks in February 2000 virtually shut down several major e-commerce Web sites, including Yahoo!, Amazon.com, and eBay.

Identification, Authentication, and Authorization

To provide the security services necessary to support the three legs of the CIA triad, security professionals must have systems in place that perform three main functions:

✦ Allow users to identify themselves to the protected resource

✦ Provide a means for the resource to objectively confirm the identity of the user

✦ Provide the administrator of the resource with mechanisms to specify which users might access the resource and the actions those users might perform

The three-step identification, authentication, and authorization process supports these three requirements. This section explores each step in further detail.

Identification

Identification mechanisms allow users to identify themselves to a resource. They provide no proof of identity; they merely provide the means for a user to profess her identity.

The most common identification mechanism now in use is the username (or login ID), often composed of a combination of letters from the user's first and last names. Systems must have a means of identifying individual users to achieve accountability. If more than one person logs on to a system with the same identification, there is no way to discern which person performed certain activities when analyzing system audit logs.

Authentication

Authentication takes identification to the next level: It allows a user to prove his identity to the satisfaction of the resource. Many different authentication mechanisms exist, but they are all based on three main principles. The user must provide one or more of these elements to the system:

- Something the user knows: This private piece of information is known only to the user. It most commonly takes the form of a password provided to the system in combination with the username. By providing the username, the user is identifying himself to the system. However, many people might know (or be able to guess) a username. When the username is supplemented with a password, the system is reasonably sure that the user is who he claims to be. Other examples of something-the-user-knows authentication include answers to personal questions (such as the user's mother's maiden name) and formulas used to compute the answer to a challenge-response question.
- Something the user is: This physical characteristic is unique to the user. The user might be asked to submit to a fingerprint reading, a retinal scan, or an iris scan or might be asked to speak a phrase into a voiceprint device. These types of measurements, based on biological features of the user's body, are known as *biometric measurements.*
- Something the user has: This element relies on the physical possession of a device, such as some form of key, access card, or other physical device that somehow interacts with the security system to prove the user's identity.

To provide more secure computing environments, you should implement more than one of the preceding mechanisms. This procedure is known as *multifactor authentication.* One of the most common examples of multifactor authentication is the SecurID system, by RSA Security. This system uses an authentication card that generates a new 64-bit authentication code every 60 seconds. When the user is ready to be authenticated, she reads the current authentication code from the SecurID device, combines it with a personal PIN, and uses the resulting code to log on to the system. This technique achieves added reliability because it ensures that the user has both physical possession of the SecurID token (something the user has) and personal knowledge of the PIN (something the user knows).

Mother's maiden name

For many years, financial institutions and others concerned with security used the mother's maiden name as an authentication mechanism because of the assumed obscurity of this knowledge. However, the widespread adoption of this technique has watered down the assurances it provides. If you're using this authentication technique, you might want to change to another mechanism.

Other popular multifactor authentication techniques include these combinations:

- A password and a biometric measurement (something the user knows and something the user is)
- A physical key and a password (another example of something the user has and something the user knows)
- An access card and a biometric measurement (something the user has and something the user is)

The choice of authentication mechanisms for your organization will vary greatly, depending on your security policy and the level of access to be granted. For example, a financial institution might require three-factor authentication before granting access to a system that allows the transfer of funds. On the other hand, an order-entry system for a manufacturing company might require only single-factor authentication in the form of a traditional username and password.

Authorization

After a user has identified herself and has satisfied any applicable authentication mechanisms, the system must have some means of deciding what level of access to grant her. This process is known as *authorization,* and it controls the exact privileges granted to system users.

An important feature of any authorization system is its *granularity,* a measure of how specific system authorizations can be. For example, a system that allows administrators to grant only “all or nothing” access to users has a low degree of granularity. On the other hand, a system that allows administrators to grant different levels of permission (for example, read, write, delete) to different users on individual files has a high level of granularity. High levels of granularity provide the greatest degree of security but also create the highest degree of overhead for the security administrator.

Risk Assessment

Security professionals must continually work to protect their systems from both internal and external risks. This section takes a brief look at how threats and vulnerabilities combine to form risks to a system's security and how those risks can be leveraged by malicious individuals to compromise that security.

Threats

Threats are anything that might cause damage to your system. A *threat* is any potential activity that might violate the confidentiality, integrity, or availability of your computing resources. Some threats are familiar to security professionals from disciplines outside information security. For example, all security specialists know the threat posed by severe storms, theft, fire, and similar occurrences.

However, a whole new range of threats becomes apparent when you focus on the information security arena. You must consider the threat posed to your system by hackers, faulty backup mechanisms, electronic component failure, and countless other eventualities.

To effectively deal with threats, you must prioritize them. The SANS Institute recommends that you look at the threat prioritization task from three different perspectives:

- Business goals: You must analyze the objectives and goals of your organization and evaluate threats based on that analysis. For example, if you manufacture widgets at a single factory that contains high-value, unique equipment, you would prioritize threats that endanger that factory because it is both irreplaceable and critical to the business.
- Validated data: The idea behind validated data is learning from your mistakes. It entails keeping a record of any security compromises that take place on your network. If you see the same technique being used again and again, that threat should probably receive a relatively high priority. After all, if thieves kept walking in the unlocked front door of your house, you would probably start locking that door after a few burglaries.
- Industry best practice: Expand on the use of validated data and learn from the mistakes of others as well. All systems should be protected against a number of well-known computer security threats. These threats are highly publicized to security professionals and hackers alike, so you would be foolish to leave your system open to them. An example is the use of vulnerability listings, like the SANS Top 20 Vulnerabilities list, shown in the following sidebar.

Top 20 Vulnerabilities

The SANS Institute, in conjunction with the U.S. Federal Bureau of Investigation, puts out a list of the top 20 computer security vulnerabilities each year. These are the vulnerabilities that, in their joint opinion, pose the greatest danger to computing systems. The list also serves as a helpful security checklist for administrators performing a threat and vulnerability assessment. The top 20 sources of computer security vulnerabilities, according to SANS, are

- Internet Information Services
- Microsoft Data Access Components (Remote Data Services)
- Microsoft SQL Server
- NETBIOS (unprotected Windows networking shares)
- Anonymous login
- LAN manager authentication
- General Windows authentication
- Internet Explorer
- Remote Registry access
- Windows scripting host
- Remote procedure calls (RPC)
- Apache Web Server
- Secure shell (SSH)
- Simple Network Management Protocol (SNMP)
- File Transfer Protocol (FTP)
- Remote commands (rsh, rcp, rlogin)
- Line printer daemon (LPD)
- Sendmail
- BIND/DNS
- General Unix authentication

In this checklist, the first ten items apply to Windows systems, and the second ten items apply to Unix systems. For full details on these vulnerabilities and the countermeasures that can be used to protect against them, see the full text of the SANS/FBI listing at `www.sans.org/top20/`.

Vulnerabilities

Vulnerabilities are the second major component of risk analysis. A *vulnerability* exists when a weakness in your security posture opens you up to a potential threat. For example, if you have a leaky roof, it's a vulnerability that leaves you in danger of damage from a heavy rain.

Risks

On their own, vulnerabilities and threats don't pose a security risk. However, when a threat combines with a vulnerability, you have a situation known as a *risk*— something that should be corrected. Security experts often describe risk using this equation:

Risk = Threat × vulnerability

There's a good reason that the multiplication operator (×) is used to describe the relationship between threats and vulnerabilities. A risk is high only when both the threat and vulnerability are high. This concept is illustrated in the risk matrix shown in Figure 1-2.

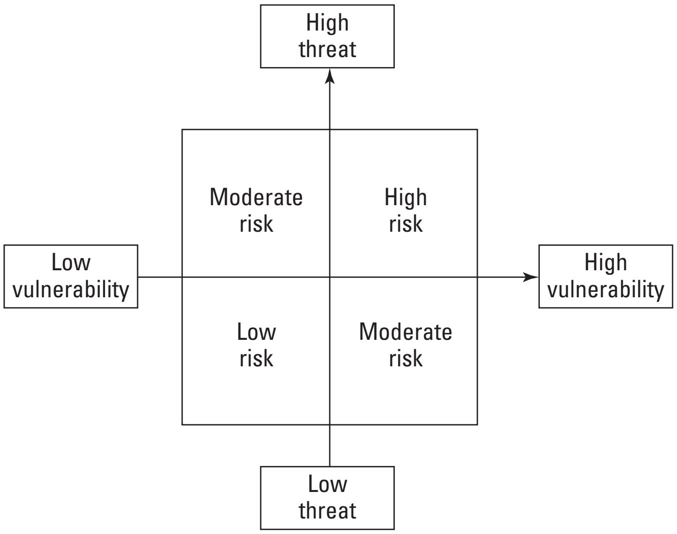

Figure 1-2: The risk matrix.

These examples illustrate the use of the risk matrix:

- You are the network administrator for a company located in California, an area prone to massive earthquakes. Your primary operating facility has a major crack in a load-bearing wall. The risk is high because you have a high threat (you're in California) and a high vulnerability (a crack in a load-bearing wall). This situation should receive immediate attention.
- You are responsible for security at a wastewater treatment plant in Miami. Several water pipes are in the wall adjacent to your main computing facility, and you worry that the pipes might freeze and burst, flooding the computer room. The risk is moderate because you have a low threat (freezing in Miami) combined with a high vulnerability (pipes in the server room). After you have protected yourself against all high-risk situations, you might want to consider implementing safeguards against this risk.
- You are worried about the likelihood that a thief might steal three blank floppy disks left on your desk in your office. The office building is patrolled by guards, and your office door is always kept locked. The risk is low because you have a low threat (nobody would want to steal blank floppies) combined with a low vulnerability (the building is guarded, and the door is locked). You probably wouldn't want to commit resources to protecting against this risk.

Granted, some of the situations described here might seem unlikely, but they serve well to illustrate the point. Most situations you encounter in the real world aren't so cut-and-dried, but contain shades of gray between the high-risk and low-risk categories. It's your job as a security professional to assess the risks and determine the best allocation of your security resources to protect your organization against them.

Compromise

Occasionally, even the most well designed set of security policies and mechanisms will fail; this situation is known as a *security compromise.* If you detect a compromise on your network, you should immediately respond according to the terms of your incident response policy. You should undertake a series of actions to isolate the incident and minimize the damage to your protected systems and, if desired, gather evidence to use in a later investigation and possible prosecution of the offender.

Cross-Reference

Incident-handling procedures are discussed in greater detail in Chapter 5.

This section is merely an introduction to the complex field of risk analysis. You can explore these concepts in greater detail in Chapter 3.

Security Principles

While you're conducting your initial exploration of computer security topics, be sure to take a few minutes to examine four key security principles you will encounter throughout your study of this book, your preparation for the SANS GSEC examination, and your professional career in the computer security field. You should be intimately familiar with these concepts because they are the "bread and butter" of information security:

- Defense in depth
- Least privilege
- Separation of privileges
- Security through obscurity (the inadvisability thereof)

Defense in Depth

The term *defense in depth,* coined by the SANS Institute, refers to building a solid, layered system of security mechanisms based on a sound, comprehensive security policy. The theory is that even if one or more of the layers of protection fails, the critical data at the core of the model will still be protected by the remaining mechanisms.

An example of defense in depth appears in Figure 1-3.

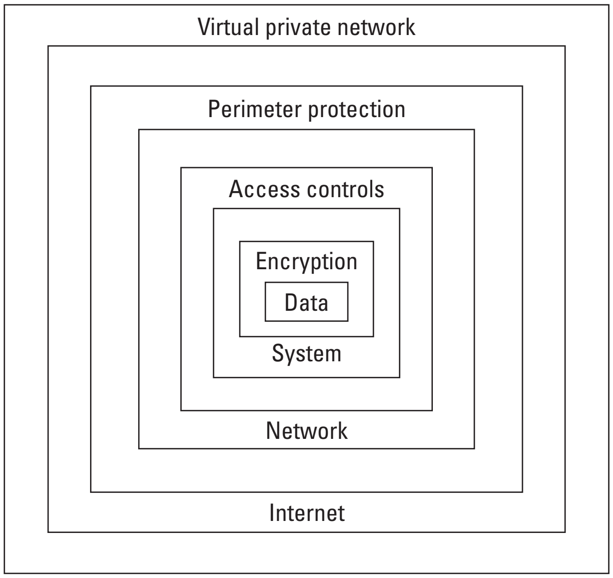

Figure 1-3: Defense in depth.

In this example, the critical data is at the core of the defense mechanisms. The data itself is protected by encryption technology. This encrypted data file then resides on a computer system, which is protected by access control mechanisms. The computer system resides on a network safeguarded by perimeter-protection devices, such as firewalls and packet-filtering routers. Finally, the network is attached to the Internet. The connection between the network and the Internet is facilitated through a virtual private network (VPN) connection that provides tunneled network security for users accessing the data over the Internet.

As you can see from this example, defense in depth is a comprehensive approach to security. An intruder attempting to attack the confidentiality, integrity, or availability of this data from the Internet would have to bypass at least four security mechanisms before reaching the desired target.

Don't consider defense in depth a spot solution. You must ensure that each computer on your network has safeguards against malicious activity. For example, if you invest significant time and energy building the safeguards shown in Figure 1-3 but allow users to access the data from home using a VPN connection without maintaining any standards for their home computers, you're basically throwing your whole investment out the window. A hacker merely needs to compromise the home user's system to gain trusted access to the network. These are the things you must consider when planning an overall network security implementation.

Least Privilege

The principle of *least privilege* states that every security subject (user, process, or other object) should have only the minimum set of permissions required to accomplish its assigned task. This principle applies the economic principle of conservatism to the assignment of security permissions. After all, if a user doesn't need a particular permission to do his job, why should he have it?

Most users can be assigned permissions from a department-based template with slight additions and removals based on their specific job responsibilities. However, in a real-world setting, applying the principle of least privilege can become a political nightmare. In Chapter 2, you find out about the importance of senior executive buy-in when promulgating your organization's security policy. It's a prime example of why that upper-level support is so critical: You need that clout behind you when you need to take away existing permissions in the spirit of enforcing least privilege.

Notice that I say that the least privilege principle should be applied to every *security subject* and not to every *user.* This distinction is an important one. Most operating systems provide the capability to grant permissions to programs and processes in addition to users. In varieties of the Unix operating system, the administrator might designate programs as *setuid* programs. These run with the permissions of the program's owner, regardless of the permissions assigned to the user who calls the program.

Cross-Reference

Setuid programs are covered in greater detail in Chapter 11.

Separation of Privileges

The *separation of privileges* principle, which complements the least privilege principle, states that permissions should depend on the presence of more than one condition. This principle ensures the integrity of the security system, even if one of the security mechanisms is somehow compromised.

A good example of the separation of privileges principle comes from the way superpowers manage missiles with nuclear warheads. As you might know, the launch of a nuclear missile requires that two different operators insert their keys and turn them simultaneously. The key slots are placed far enough apart that no single person could possibly reach between the two and turn them simultaneously. In this case, each person acts as a protection mechanism. If a rogue missile officer wanted to launch a nuclear attack, she would have to recruit a peer coconspirator to successfully launch a missile.

Many information security protection mechanisms operate in a similar manner. For example, many accounting systems require two supervisory users to electronically authorize large transactions before issuing a check. This type of system is facilitated by encryption technology and digital signature technology (discussed in Chapter 6).

Personnel practices

Keep in mind that personnel are often the weakest links in any security arrangement. One of the most important things an organization can do is integrate security concerns into its human resources practices, especially for employees with access to sensitive information. Some commonly adopted practices include

- Job rotation: Allow individuals to occupy critical positions for only a predetermined period, to limit their opportunity to misuse data and resources.
- Mandatory vacations: Forcing employees to take vacations provides two important security benefits—it reduces their stress levels, which also reduces the likelihood that they will become disgruntled and take malicious action against their employer, and it provides the organization with the opportunity to have someone else take over that person's job for a week or two and identify any potential fraud.
- Background screening: Most organizations now require some sort of background check for all new employees. This practice is important, and you should consider performing more thorough checks on employees occupying sensitive positions. If local laws permit, you might also want to conduct periodic checks on current employees.

Security through Obscurity

In the early days of computer security, when the field was dominated by government and military concerns, a principle known as *security through obscurity* was prevalent. This principle stated that the inner workings of security mechanisms should be kept secret and that the security of the mechanisms could depend on the preservation of those secrets.

Arguably, this concept worked in the day and age when computer security was strictly a military concern. As you learned earlier in this chapter, the military has a strict protocol for data classification and a thorough background screening and reinvestigation process to ensure that only "reliable" individuals receive access to classified information.

However, now that security concerns have become part of mainstream computing, security through obscurity is no longer a viable concept, for several reasons:

- In general, most companies don't have a strict data classification scheme like the one used by the military. If data on the inner workings of the security mechanisms were disclosed to outsiders, the viability of the mechanism itself would be at risk.
- Most companies won't purchase a system that relies on secret details. Security professionals now want to know how mechanisms operate to assure themselves that the mechanisms will provide adequate security for their networks.
- Mechanisms that rely on secret workings cannot be validated by independent authorities. Encryption algorithms and other security mechanisms become generally accepted by the security community only after successful evaluation by one or more independent organizations.
- Patenting a device that relies on secret mechanisms isn't possible. Patent protection requires full public disclosure.

The working details of most modern security mechanisms are publicly available. However, developers engineer these mechanisms so that they depend on some other type of secret information or tamper-resistant device. For example, you can find the details of all accepted encryption algorithms on the Internet. However, it has been shown mathematically that the algorithms are extremely difficult to break without access to the secret keys used to encrypt and decrypt data by individual communicants.

Cross-Reference

You can find out more in Chapter 6 about how encryption algorithms use secret keys.

Information Warfare

The introduction to this chapter mentioned that governments around the world are gearing up for the newest front in war fighting: information warfare (IW). Strategic military thinkers recognize that information drives the militaries, economies, and governments of powerful countries and realize that inattention to security over the years leaves those complex yet critical infrastructures open to attack (like an Achilles's heel).

Note The U.S. military recently discarded the term information warfare in favor of the more neutral-sounding information operations. However, the two terms can generally be used interchangeably.

The major feature of IW that makes it appealing to many nations is its asymmetry. *Asymmetric* types of warfare are highly leveraged — the value of the outcome is much greater than the effort required to cause it. Other examples of asymmetric warfare include terrorism and political upheaval. Most modern militaries aren't prepared to wage this type of warfare. They are, on the other hand, prepared for traditional (or symmetric) warfare involving massive troop movements and bombs on targets.

These same factors make IW extremely appealing to small, radical groups who might lack the budget and manpower to challenge a superpower adversary on a traditional battlefield. A small investment in some computer equipment and training could yield dramatic results.

Offensive Information Warfare

The main objective of offensive information warfare is to interrupt the enemy's decision-making process through the special tools and techniques available to IW practitioners. Here are the main principles of offensive IW, paraphrased from the official U.S. military doctrine:

- Clearly establish objectives and include measures of effectiveness.
- Use specific offensive capabilities that are appropriate and consistent with the overall effort.
- In the terms of a larger conflict, IW can be the main effort, a supporting effort, or a phase of a larger effort.
- All offensive IW operations must be integrated, coordinated, and deconflicted with all other aspects of a military campaign. (For example, you don't want one branch of the military to blow up a computing facility that another branch of the military is mining for valuable intelligence.)

While studying IW, keep in mind that the military might not be the only target of offensive operations. In fact, the asymmetrical nature of IW lends itself to attacking portions of the civilian infrastructure. It pays for security professionals in all kinds of organizations to be familiar with the basic concepts of IW, at least at a level where they might recognize the early signs of an attack and alert the appropriate authorities.

Information warfare is more than just hacking

When most people think of information warfare or information operations, they imagine a room full of computers manned by geeky soldiers attempting to wreak havoc on an enemy's information infrastructure. However, from the military point of view, information operations are a much broader concept. The military lumps together hacking and computer security with psychological operations (such as deception and propaganda), electronic warfare (such as jamming enemy radar systems), and even physical destruction when it involves attacks aimed at an enemy's information infrastructure (such as blowing up a supercomputing center). To learn more about the U.S. military's thinking on this issue, download the Joint Doctrine for Information Operations at www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf.

Defensive Information Warfare

Just as military thinkers must adapt their mindsets to successfully embrace offensive forms of IW, those responsible for defending our nation's critical information infrastructure must be flexible in their defensive mechanisms.

U.S. military thinkers have outlined a strategy for waging an appropriate defense that counters each facet of offensive IW individually. Some of those components include

✦ Operations security (OPSEC): Minimizes the amount of critical information an enemy can infer by studying unclassified information and monitoring activity levels. The classic example of an OPSEC violation occurred when the news media determined that an attack on Iraq was imminent when they noticed a huge increase in the number of pizzas being delivered to the Pentagon late at night.

✦ Electronic warfare: Can be defended against by employing technical safeguards and secure operational techniques such as regularly changing call signs and frequencies.

✦ Education, training, and awareness: Elements that are critical to the success of any defensive operation. If those involved in the day-to-day operations of an organization aren't tuned in to the threat posed by IW, a real attack is likely to go undetected.

The Joint Doctrine for Information Operations (see the earlier sidebar "Information warfare is more than just hacking" for further information) outlines a number of other areas where defensive IW plays a critical role, such as intelligence support, counterdeception, counterintelligence, and counterpropaganda operations. If you want to learn more, the full doctrine document is freely available on the Internet.

✦ ✦ ✦

SAMPLE QUESTIONS

1. Which one of the following is *not* one of the three fundamental principles of computer security?

a. Confidentiality

b. Disclosure

c. Availability

d. Integrity

Answer: b

Disclosure isn't one of the three fundamental principles that make up the CIA triad — confidentiality, integrity, and availability. In fact, it is the opposite of confidentiality and should be avoided.

2. Which one of the following is the technique hackers use to attempt to defeat availability mechanisms?

a. Destruction

b. Integrity

c. Alteration

d. Disclosure

Answer: a

Destruction is the opposite of availability. It attempts to remove data from a system to prevent legitimate users from accessing it.

3. What security level would include private information about an individual held by a government agency?

a. Unclassified

b. Sensitive But Unclassified

c. Confidential

d. Secret

Answer: b

Private information about individuals is protected at the Sensitive But Unclassified (SBU) or For Official Use Only (FOUO) level. Disclosure of this information might not adversely affect national security but is prohibited under the terms of the Freedom of Information Act.

4. What is the lowest level at which information is considered classified by the defense establishment?
   - **a.** Unclassified
   - **b.** Sensitive But Unclassified
   - **c.** Confidential
   - **d.** Secret

Answer: c

Confidential information is the lowest level of information officially considered classified. Disclosure of this information outside authorized channels would cause some type of damage to the national security.

5. Bob received an e-mail message from Alice, and he wants to be sure that the contents of the message weren't altered between the time Alice sent the message and the time he received it. What security goal is Bob attempting to achieve?
   - **a.** Confidentiality
   - **b.** Availability
   - **c.** Integrity
   - **d.** Disclosure

Answer: c

Integrity provides assurances that data wasn't modified in an unauthorized manner. Bob and Alice could use a digital signature mechanism to achieve this goal in their e-mail communications.

6. Which one of these security mechanisms provides the strongest degree of authentication to a system?
   - **a.** Token-based authentication
   - **b.** Password authentication
   - **c.** Biometric authentication
   - **d.** Multifactor authentication

Answer: d

Multifactor authentication provides the strongest degree of authentication assurance by combining techniques from two or three of the authentication mechanism categories (something the user knows, something the user is, and something the user has).

7. Which one of these categories of security mechanisms provides a means for a system to objectively confirm the identity of a user?

a. Authorization

b. Authentication

c. Verification

d. Identification

Answer: b

Systems use authentication techniques to confirm the professed identity of users. An example of an authentication scheme is using a password to confirm the claim made by a username.

8. Mal is a malicious former employee seeking to gain access to a system. Her goal is to find sensitive documents and disseminate them to competitors in an effort to harm the company. Which leg of the CIA triad is she most directly targeting with this objective?

a. Confidentiality

b. Integrity

c. Authorization

d. Availability

Answer: a

Mal is seeking to violate the confidentiality of corporate secrets by disseminating them to outsiders.

9. What is the formula commonly used to describe when a risk is posed to a computing system?

a. Risk = Threat – Vulnerability

b. Risk = Threat × Vulnerability

c. Risk = Compromise + Vulnerability

d. Risk = Compromise – Vulnerability

Answer: b

Risk = Threat × Vulnerability is the cornerstone of risk assessment and risk management programs.

10. Which one of the following is *not* a recommended source of threat prioritization information?

- **a.** Business goals
- **b.** Vendor information
- **c.** Validated data
- **d.** Industry best practice

Answer: b

The three recommended sources of threat prioritization data are business goals, validated data, and industry best practice. You might also gain prioritization information from vendors but must recognize that this comes from an inherently biased point of view and might not be applicable to your situation.

11. Which one of these metrics measures the detail with which a security administrator can control access to a system?

- **a.** Multifactorality
- **b.** Concurrency
- **c.** Granularity
- **d.** Obscurity

Answer: c

The granularity of a resource is the level at which a security administrator can control access to the resource. Systems with high granularity allow a great deal of detailed control whereas low-granularity systems are often all-or-nothing access propositions.

12. Which one of these combinations of circumstances poses a significant risk?

- **a.** Low threat, low vulnerability
- **b.** Low threat, high vulnerability
- **c.** High threat, low vulnerability
- **d.** High threat, high vulnerability

Answer: d

Significant risks occur when a high threat combines with a related high vulnerability.

13. What security term was coined by the SANS Institute to represent the optimal information security strategy?

a. Separation of privilege

b. Least privilege

c. Defense in depth

d. Security through obscurity

Answer: c

Defense in depth is the term used by the SANS Institute to describe the optimal security architecture achieved by enforcing a strong security policy through the use of multiple redundant mechanisms at various levels.

14. Which one of these security principles was once popular but has been shown to be ineffective?

a. Separation of privilege

b. Least privilege

c. Defense in depth

d. Security through obscurity

Answer: d

Security through obscurity practitioners attempt to achieve secure computing environments by hiding the details of their security mechanisms. This strategy leads to weak, unproven security mechanisms while achieving debatable security benefits.

15. Perimeter protection is an example of a mechanism that might be used as part of a defense in depth strategy to protect resources at the ________ level.

a. Data

b. System

c. Network

d. Internet

Answer: c

Perimeter-protection devices, such as firewalls and packet-filtering routers, are used to protect resources at the network level. These devices generally form the boundary between a protected network and an unprotected network (such as a WAN or Internet connection).