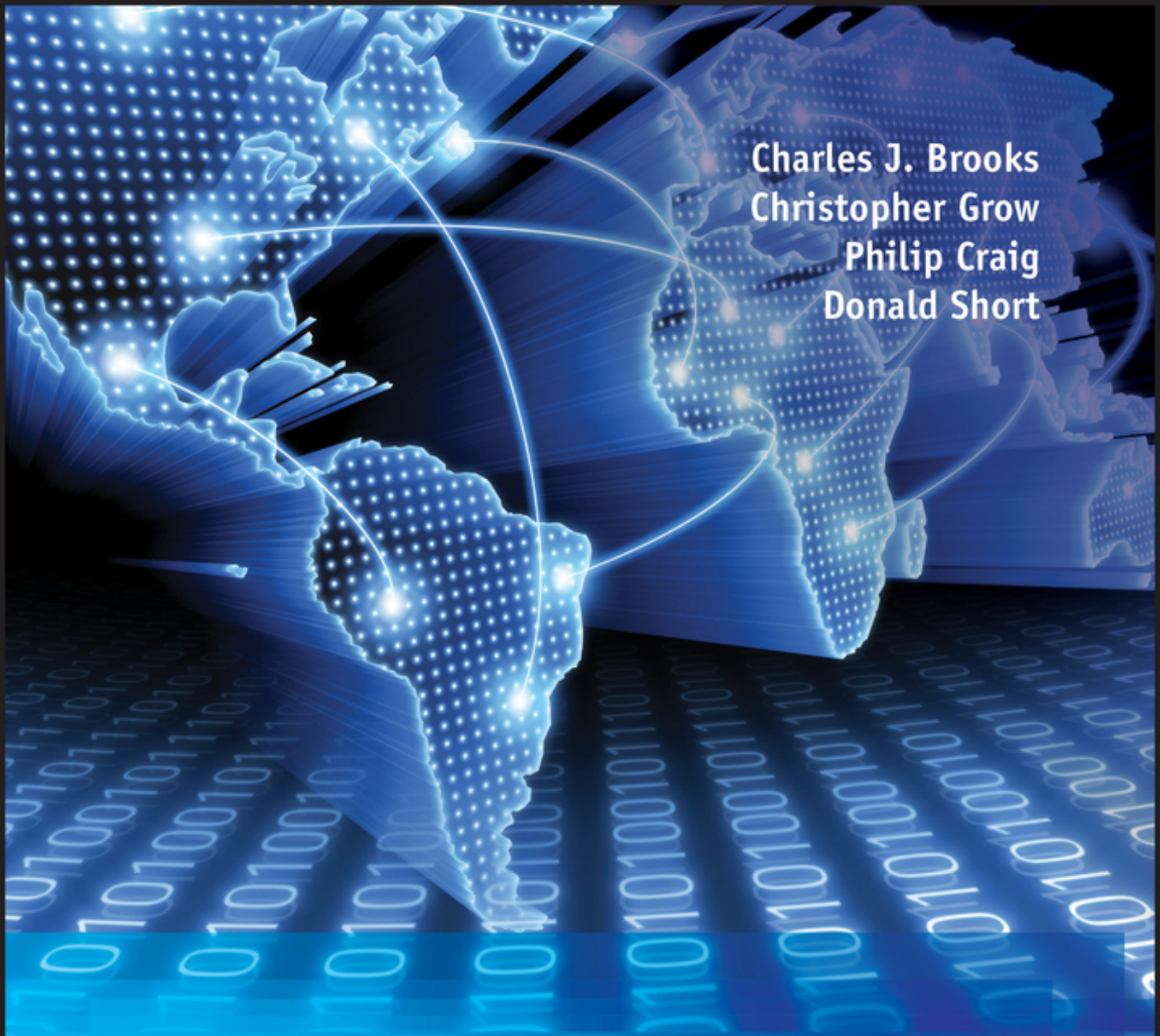


Charles J. Brooks
Christopher Grow
Philip Craig
Donald Short

Cybersecurity

ESSENTIALS

SYBEX
A Wiley Brand

Table of Contents

List of Tables

List of Illustrations

Chapter 15

PART I
Securing the Infrastructure

CHAPTER 1
Infrastructure Security in the Real World

The following challenges will provide contextual reference points for the concepts you will learn in Part I. Because you have not yet read the chapters in Part I, the challenges in this chapter are designed to introduce you to the infrastructure security scenarios you'll face in the real world. In this chapter, you'll learn to:

- **Understand the relevance of infrastructure security**
- **Describe the functions, categories, subcategories, and reference structure of the NIST Cybersecurity Framework**
- **Apply the NIST Framework references to specific cybersecurity scenarios**

Security Challenges

The NIST Cybersecurity Framework was developed by the U.S. National Institute of Standards and Technology (NIST) to provide a set of independent guidelines that organizations can use to implement or upgrade their cybersecurity programs. Because the framework is a product-independent tool, it provides guidelines that any organization can tailor to meet its own cybersecurity needs.

The frameworks are divided into five functions (Identify, Protect, Detect, Respond, and Recover) that provide a top-level description of the cybersecurity development process. Each function is then divided into applicable categories that underpin the stated function. Each category is further divided into subcategories and implementation methodology. Finally, the subcategories are supported by lists of reference documents that contain the nuts and bolt of building the cybersecurity program.

This chapter will kickstart your thought processes for what you are about to learn in Part I. It contains two specific cybersecurity scenarios to which you will be asked to apply the NIST Framework in order to produce a cybersecurity solution that meets the desired objectives. In each case, you will be provided with specific subcategories to research, along with some guidance to help you produce your solutions.

In this first pass through the scenarios, you are expected to generate and record *general observations* about securing the infrastructure described, as you have not yet been introduced to the supporting material. As mentioned earlier, this is activity is designed to get your cybersecurity thought processes started.

In Chapter 5, you will return to these scenarios and use what you have learned in Chapters 2, 3, and 4 to revise your initial assessments. You will also compare your observations to those of professional security specialists who have provided their observations and solutions for these scenarios.

Infrastructure Security Scenario 1

You are in charge of planning and implementing a security system for a new electrical substation that will be built next to a new housing development. The substation is equipped with high-voltage electrical switching gear for the surrounding community. It is not manned on a full-time basis but does have a control building that houses instrumentation and communication equipment, as shown in Figure 1.1.

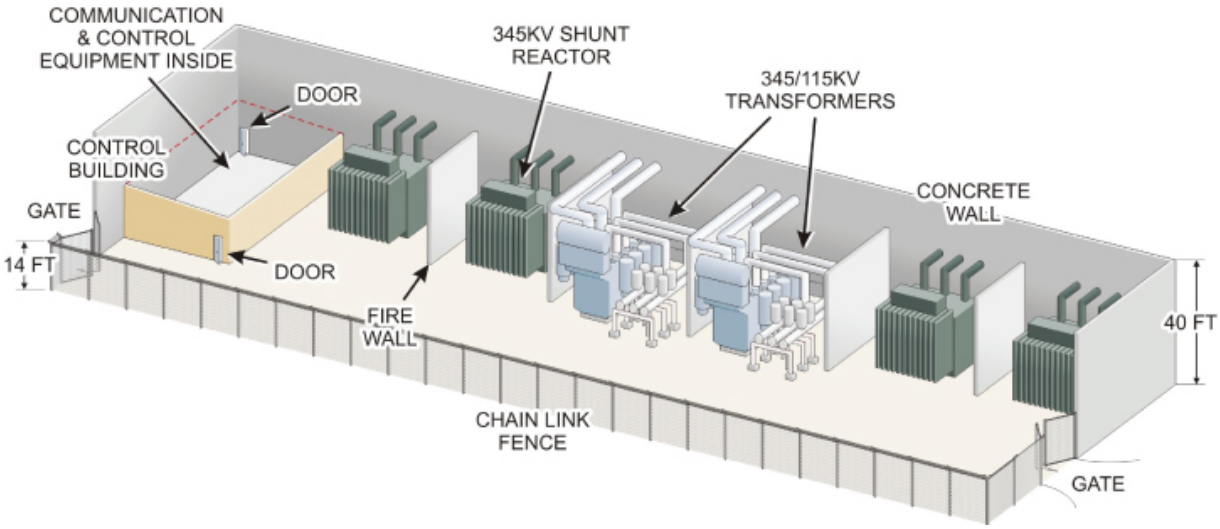


FIGURE 1.1 The Electrical Substation

The high-voltage switch gear accepts electrical power from different sources, which it then conditions and routes to the community users as needed. The energy arrives on a set of different high-voltage supply lines and leaves the facility via different sets of distribution lines.

The monitoring devices and control systems in the substation communicate with different parts of the utility's transmission and distribution system to route electrical power where and when it is needed. These communication channels include wireless radio signals, signals transmitted across the power lines, and traditional network communications media.

Risk Assessment 1

From the information provided in this first scenario, consider the National Institute of Standards and Technology (NIST) functions detailed in this section and then record your observations as they relate to each category.

SEE APPENDIX C FOR THE NIST CYBER SECURITY FRAMEWORK

A copy of the NIST Cyber Security Framework is available in Appendix C. These frameworks were developed by the U.S. National Institute of Standards and Technology to provide cybersecurity guidelines for Improving Critical Infrastructure Cybersecurity under executive order 13636. The ultimate goal of this initiative is to provide guidelines for the nation's critical infrastructure in business, industry, and utility organizations to reduce their cybersecurity risks.

Identify

Create an inventory of physical assets (devices and systems) within the substation (NIST ID.AM-1).

UNDERSTANDING NIST REFERENCES

NIST references include the function, the category, and the subcategory. In the example of ID.AM-1 mentioned earlier, the *function* is Identify (ID); the *category* is Asset Management (AM); and the *subcategory* is 1 (which is "physical devices and systems within the organization are inventoried"). To implement this portion of the Framework for the scenario presented, you may want to refer to an online copy of the designated *Reference* documents listed under this subcategory. The same is true of the following subcategories as well.

Protect

Describe in general how you might go about protecting the physical assets identified in the previous point (NIST PR.AC-2).

Detect

How would you know if someone or something was attempting to access, disable, degrade, or destroy one or more of the devices and/or systems in the substation? How could you detect anomalies and events that might impact the operation of the substation (NIST DE.CM-2, 8)?

Respond

How would you need to respond to the anomalies and events you've identified through the devices, systems, and steps you would implement in the previous point (NIST RS.AN-1, 2, 3)?

Recover

Which steps could be put in place to recover from actions intended to access, disable, degrade, or destroy the assets you previously identified (NIST RC.RP-1)?

Infrastructure Security Scenario 2

Your company is building a new corporate facility, as shown in Figure 1.2, to house its 5,000 headquarters employees. The facility will feature multiple floors. Some management personnel will use traditional offices with doors and windows, but the majority of the employees will work in open cubicles.

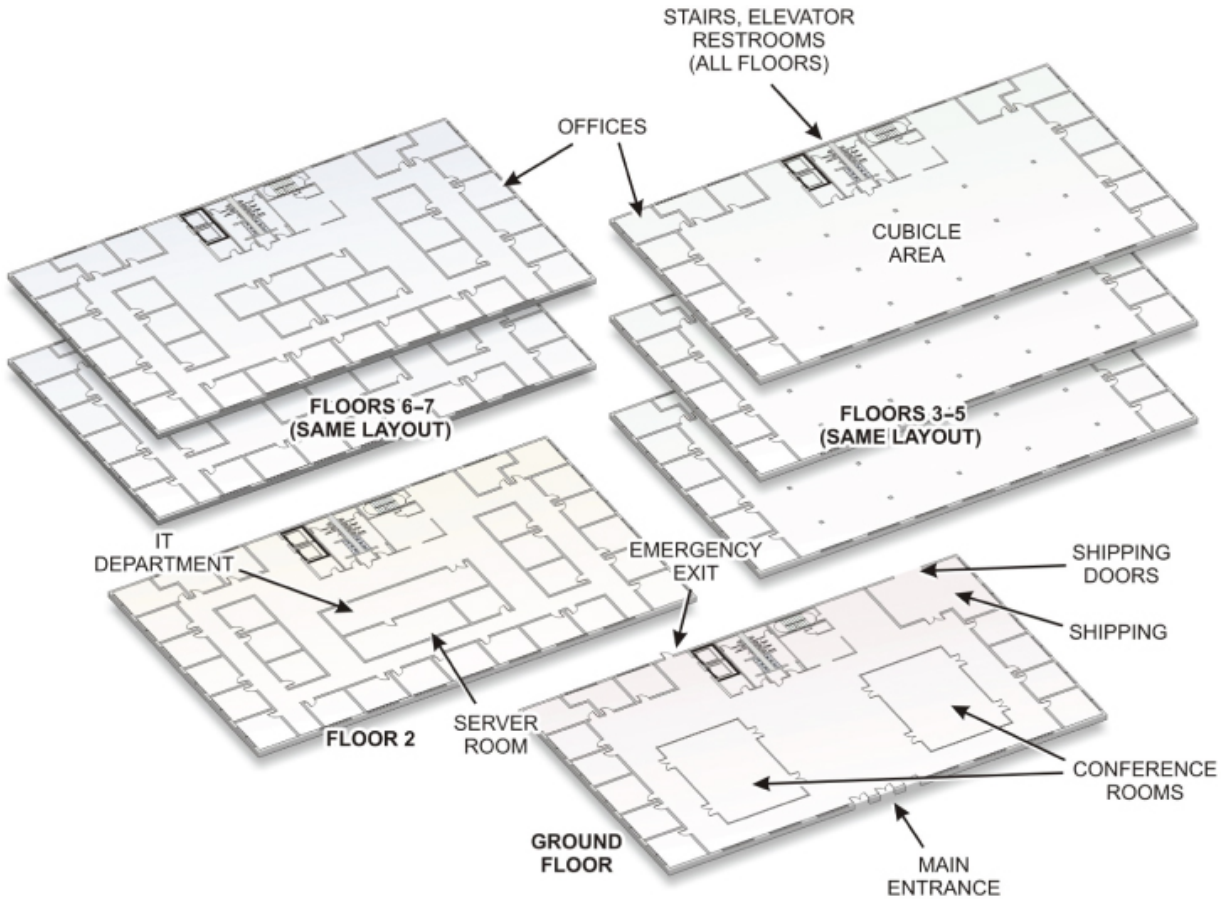


FIGURE 1.2 Headquarters Facility Plans

Each office and cubicle will be equipped with a telephone and network connection. In addition, many of the employees travel as part of their job roles and require portable computers. Other employees work with desktop personal computers.

The facility will house a cluster of computer servers and network devices that provide workflow and communications between all of the managers and employees. This architecture electronically manipulates, stores, and transmits all of the company's important business information and data. This includes product descriptions, accounting information, legal records, customer records, employee records, and the company's intellectual property.

Risk Assessment 2

From the information provided in the second scenario, consider the NIST functions detailed in this section and then write your observations as they relate to each category.

Identify

Create an inventory of physical assets (devices and systems) within the organization (NIST ID.AM-1).

Create an inventory of cyber assets (software platforms and applications) within the organization (NIST ID.AM-2).

Prioritize the organization's assets based on their criticality or value to the business functions of the organization (NIST ID.BE-3).

Identify any assets that produce dependencies or provide critical functions for any of the organization's critical services (NIST ID.BE-4).

Create a risk assessment of asset vulnerabilities identified (NIST ID.RA-1, 3).

Protect

Create a policy for managing access to authorized devices and resources based on the following items (NIST PR.AC-1).

Create a method for controlling physical access to secured assets (NIST PR.AC-2).

Create an action plan for informing and training general employees (NIST PR.AT-1).

Create a plan for helping privileged users understand their job roles and responsibilities (NIST PR.AT-2).

Detect

Which types of systems must be in place to identify occurrences of physical security breaches (NIST DE.CM-2)?

Which types of systems must be in place to monitor personnel activity to detect potential cybersecurity threats (NIST DE.CM-3)?

Respond

Which type of response plan might be necessary when general physical security is breached at the facility (NIST RS.AN-1, 2, 3)?

Considering the information kept on the company's servers, which type of response plan might be necessary when physical security is breached in the server room (NIST RS.CO-4, 5)?

Recover

Which type of recovery plan might be needed for general physical security breaches that occur at one of the cubicles in the facility (NIST RC.RP-1)?

Which items might a recovery plan include if server security is breached at the facility (NIST RC.CO-1, 2)?

Summary

Record your observations for the risk assessments presented in this chapter. In Chapter 5, you will compare these original thoughts and observations with those you will generate after reading Chapters 2, 3, and 4. You'll also be able to compare your answers to those of professional security specialists.

CHAPTER 2
Understanding Access-Control and Monitoring Systems

If you skipped reading the "Introduction," you might wonder why there's an entire Part I devoted to infrastructure security. However, as the "Introduction" pointed out, without physical security there is no security. Infrastructure security operation and management is based on three basic types of subsystems: access-control and monitoring systems (covered in this chapter), video surveillance systems (covered in Chapter 3), and intrusion-detection and reporting systems (covered Chapter 4). In this chapter, you'll learn to:

- **Understand the application of the following concepts of physical security: access control, physical barriers, and biometrics**
- **Differentiate between authentication and authorization**
- **Identify commonly used physical access-control systems/devices including keypads, card readers, biometric readers, proximity readers, electronic deadbolts, and magnetic locks**

A Quick Primer on Infrastructure Security

The overall aim of any security effort is to establish a peace-of-mind condition (a carefree state free from worries) for an individual, a group, or an organization. This condition is ideally achieved by securing exclusive rights to assets (objects and information), access to those assets, and use of those assets. This condition creates value and provides peace of mind to asset owners.

NO TIME FOR RELAXING IN THE CYBERSECURITY WORLD

In the cybersecurity realm, a carefree state is never actually achieved. New types of cyber attacks are constantly being devised, causing cybersecurity specialists and administrators to be constantly on guard against potentially damaging occurrences.

A more modern definition for security is the science, technique, and art of establishing a system of exclusion and inclusion of individuals, systems, media, content, and objects. It also provides increased safety and utilization with physical assets such as machinery or processing equipment.

Physical security is the science, technique, and art of establishing a system of exclusion and inclusion for tangible assets. In practice, this involves policies, practices, and steps aimed at combating theft, preventing physical damage, maintaining system integrity and services, and limiting unauthorized disclosure of information.

Similarly, the term *cybersecurity* involves securing physical access to property, systems, and equipment ports while securing intangible assets including electronic, optical, and informational access to the system's data and controls.

In any modern system, security is a function of the synergies of both the physical and cybersecurity domains. Both entities are necessary to support a strong overall security posture and program.

When physical security initiatives are applied to providing security for the basic physical and organizational structures needed for the operation of an enterprise, an organization, or society, this is known as *infrastructure security*.

Although we may think of infrastructure security in simple physical terms such as a lockable door, a patrolling security guard, or as some other method used to protect our assets; there are several additional

components that go into constructing an effective infrastructure security system. Such systems generally involve a combination of several critical security procedures that have been well planned and tested to meet or exceed operational and organizational security needs.

As shown in Figure 2.1, there are three general layers to designing and implementing a plan to physically secure an infrastructure asset (a property, building, physical space, system, or device):

The Outer Perimeter Securing this space involves controlling who can move (walk, drive, fly) across the legal or physical line that marks this perimeter. Examples of typical physical outer perimeters include property lines or the exterior walls of a building or complex.

The Inner Perimeter This perimeter typically involves physical barriers such as walls, doors, and windows—either exterior or interior, depending on the context of the outer perimeter.

The Interior This is the innermost level of security and consists of the interior of the building, office, cubicle, etc. that is surrounded by the inner and outer perimeters.

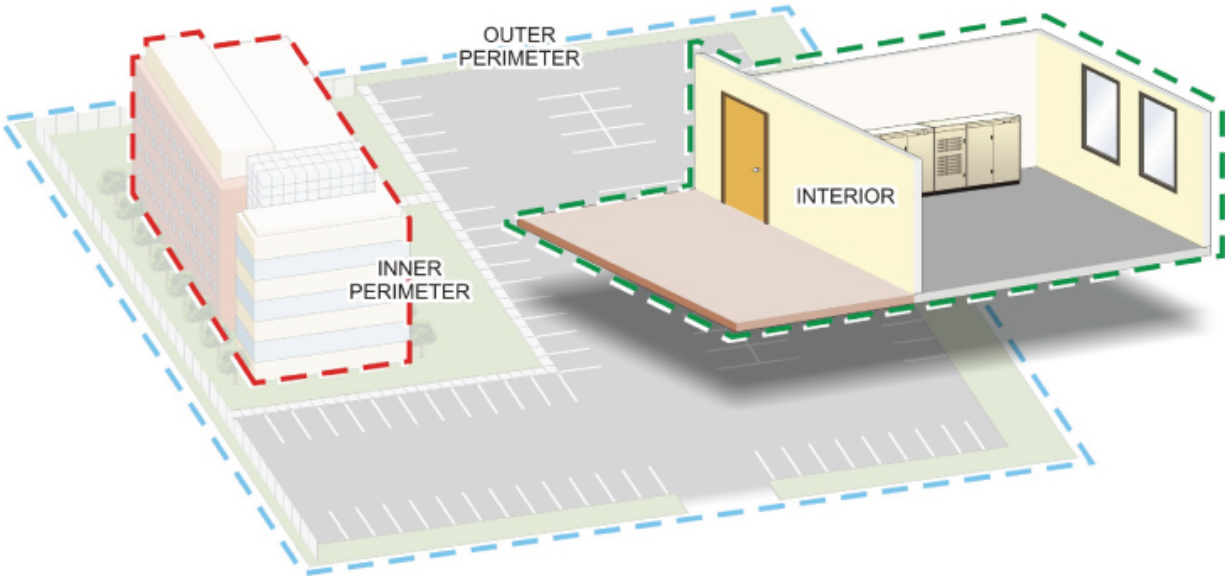


FIGURE 2.1 The Three Perimeters

In a comprehensive security plan, control of all three layers is addressed. Security at each layer typically consists of a formulation of specifically selected devices working together to provide an effective physical security system.

SECURING LOGICAL PERIMETERS

Cybersecurity also deals with securing logical perimeters. They are covered in later chapters having to do with computing and control systems, networks, and the Internet. The same security concepts developed here will be applied to those topics as they are encountered.

At each layer there are two concepts at work:

Natural Access-Control Methods Natural access control involves using natural design elements, such as structures and landscaping, to guide people as they enter and exit spaces.

Territorial Reinforcement Territorial reinforcement employs structures, systems, and devices to prevent unauthorized entry and create a clear difference between what is public and private.

Infrastructure security operation and management is based on three basic types of subsystems:

- Access-control and monitoring systems
- Video surveillance systems
- Intrusion-detection and reporting systems

In this chapter, you will learn about access-control and monitoring systems. However, before reading further, take a couple of minutes to update the security scenarios in Chapter 1 to reflect these introductory ideas.

Access Control

Most security experts agree that the first and most basic objective of any infrastructure security system is to deter potential intruders, as shown in Figure 2.2. This is the goal of access control. You can't damage, destroy, or steal what you can't physically access.

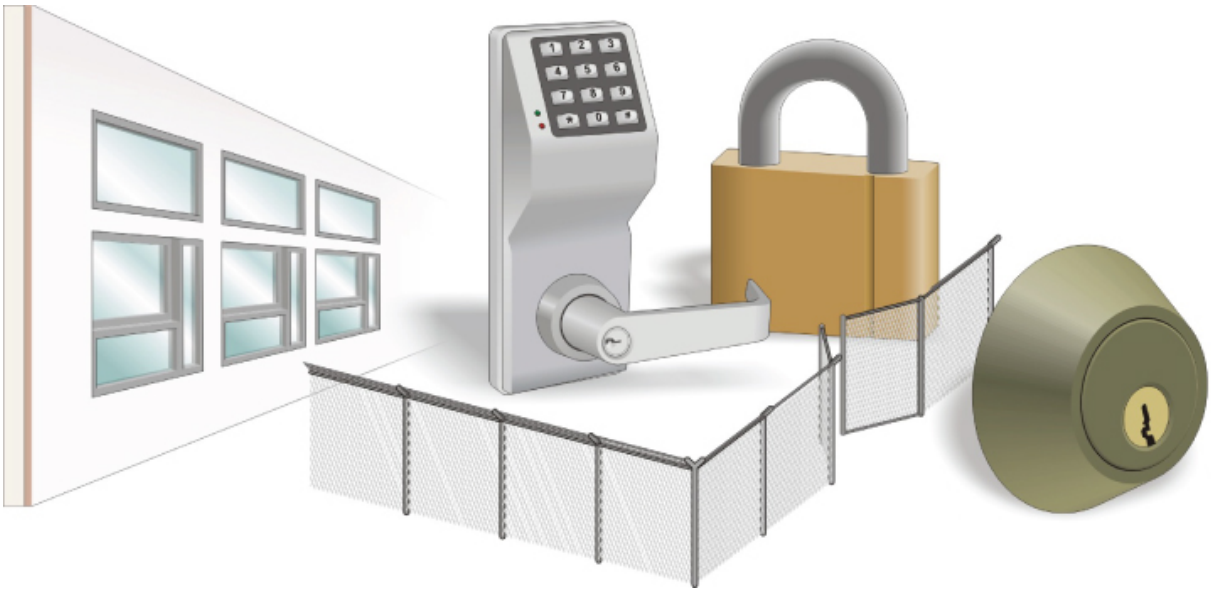


FIGURE 2.2 Access Control

The basis of designing efficient access-control systems involves three terms: ingress, egress, and regress. By definition, *ingress* is the right of an individual to enter a property, while *egress* is the legal right to leave a property. Similarly, *regress* is the term used to describe the legal right to reenter a property.

On a physical security basis, ingress can be defined as the physical path of an individual to properly enter a property, while egress is the physical path to properly leave a property.

In security terms, a *right* is a legal privilege or permission granted to someone, or some group, by some recognized source of authority. This source can be a government, a legally recognized governmental agent, or a legally recognized owner of an asset. By extension, a person who has the right to access an asset is said to be *authorized* (by the recognized authority), while anyone who has not been given this right is labeled as *unauthorized*. When unauthorized people attempt to gain access to an asset they do not have rights to access they become *intruders*.

Therefore, access control involves being able to control the ingress, egress, and regress to an asset based on authorization, as depicted in Figure 2.3. In particular, limiting the access of unauthorized personnel to important assets is the most fundamental security step that you can take.

FIGURE 2.3 Authorization

From the list in the previous section, you can see that access control begins at the outer perimeter. Depending on the specific example being studied, this may be the property line of the organization's physical property or the front door of their facilities.

Recall that the goal at the outer perimeter is to control who can walk or drive across the perimeter. Control at this point can be as simple as planting hedges at the edge of the property or including appropriate visual signs to warn unauthorized people to stay out, or as complex as a barbed-wire fence with gates and armed guards.

Access-control efforts typically extend into the area between the outer and inner perimeters. These efforts can include natural access-control techniques such as strategic placement of employee and guest parking, as well as the use of landscaping features to channel people to selected entrances and exits and inhibit access to other possible entry/exit points. This also extends to clearly marking ingress and egress approaches to facilities and properties.

CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)

CPTED is a set of building and property design principles based on anticipating the thought processes of potential intruders to discourage them from follow through.

Inner perimeter control of a physical infrastructure involves the use of physical structures such as walls, windows, and doors that can act as barriers that impede the ability of an intruder to advance from the outer perimeter to the interior region. Once again, depending on the specific security scenario being discussed, these barriers may be part of the building's external structure that encloses the entire interior environment, or they can be interior structures that control movement into and out of individual work areas.

Interior security is the innermost level of infrastructure security, and it involves monitoring the area inside the inner perimeter. Such monitoring may consist of both human and electronic security systems to observe, track, and detect intruders as well as record evidence of different activities. The mixture of empowered people and electronic devices makes for an effective security tool at the interior security level.

Security Policies

A key component that brings all three levels of security together is a well-designed security policy that states how security is implemented at each level. Businesses and organizations develop comprehensive security policies that define who is authorized to access different assets and what they are allowed to do with those assets when they do access them.

For example, allowing employees and visitors to have free access to all the departments inside the organization provides a variety of security risks. You will want to maintain access control to create an environment that reduces the human nature of temptation. If everyone can move

freely within the interior of the organization, it is much more difficult to implement safeguards to prevent them from accessing or taking physical or cyber assets. You also need to maintain access control to prevent accidents.

For example, you do not want a sales representative accidentally spilling their coffee on one of the production servers in your engineering department.

Instead, develop a cohesive access-control policy at each level that provides authorized people with appropriate levels of access to selected assets, while inhibiting access to assets by people who are not authorized. Then enforce those policies with the correct types and numbers of access-control devices (sensors, barriers, logs, ID badges, or security guards) as deemed appropriate.

A WORD ABOUT SECURITY GUARDS

Although access-control devices may be cheaper than human guards, guards are able to make valuable judgmental decisions based on the actions of a potential intruder. They offer a symbol of security, can initiate human judgment, and they can provide timely intervention during an incident.

Frequently, badges or smartcards are used to control access. Employees may also be identified by a Radio Frequency Identification (RFID) transponder as they move within proximal range of an RFID sensor. Transponders store access codes and use radio receivers and transmitters.

These access-control techniques, systems, and devices are discussed in detail throughout the remainder of this chapter.

Physical Security Controls

Enforcing access-control measures may initially include placing locks on doors that access offices and separating departments or networking

sections with similar physical barriers. Many companies have a front door or an entranceway that includes a receptionist to control access. During business hours, the receptionist acts as a physical barrier, inquiring about the nature of clients' visits, as illustrated in Figure 2.4.

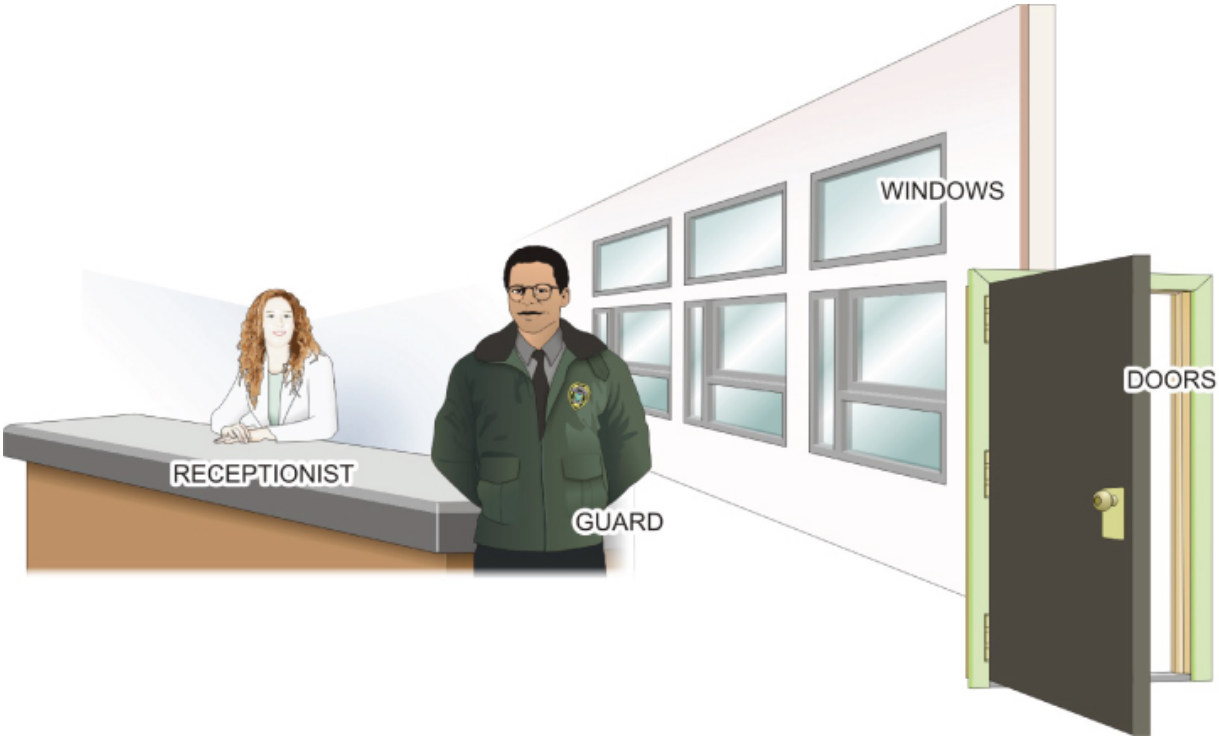


FIGURE 2.4 Physical Barriers

In some institutions, the visitor may be required to be accompanied by an escort to physically limit their movement through the company. For additional access control, a human guard could be employed to control access to specific, restricted interior locations, such as a laboratory, or to an elevator that services a restricted area, such as a basement.

At night, the physical barrier may simply be a locked door. However, the door may also be equipped with a sensor and an alarm. The alarm could be a local annunciator such as a siren, or it could be linked directly to an external monitoring system or to the police department.

Locks and Keys

The primary physical barrier in most security perimeters is the lockable door. The door provides the physical barrier but in itself will only keep honest people out. The lock, on the other hand, provides the

authentication function of the barrier through its key. Having the key signifies that the person either possesses or knows the information required to gain access through the door.

Many different types of locks are used with security barriers. Likewise, many different types of keys are used to disengage the locking mechanism. Depending on the type of lock being used, the key can be either physical or logical.

In most organizations, only select personnel who work in a particular office may possess a key to access their working environment. Maintaining tight key control and using numbered keys that are clearly coded for nonreproduction helps to maintain the locked door as an effective physical barrier.

ENFORCE A STRICT KEY CONTROL POLICY

A strict key control policy is required to successfully protect equipment and ideas behind locked doors.

Standard Key-Locking Deadbolts

Standard key-locking deadbolts have a locking mechanism similar to that of the electronic solenoid-operated deadbolt but are engaged or withdrawn with a key. They provide an added level of security for doors that can be operated manually. A key-locking deadbolt is available with a single or double cylinder, as shown in Figure 2.5.

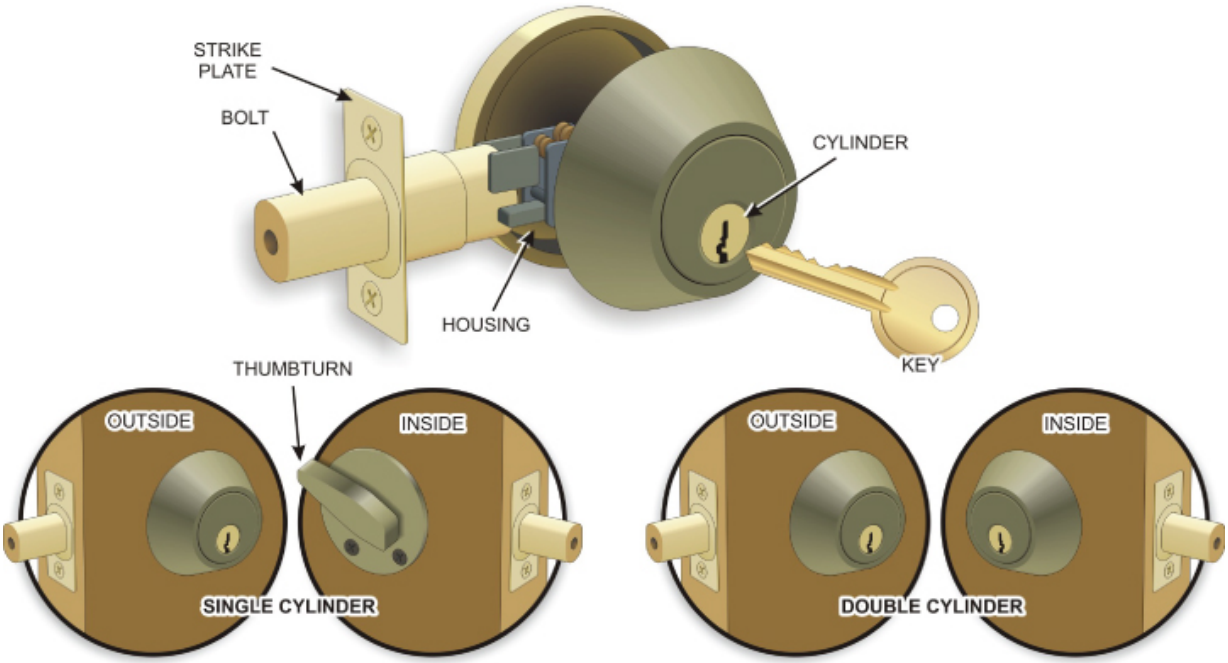


FIGURE 2.5 Key-Locking Deadbolt

Solenoid-Operated Deadbolt Locks

Electronically operated deadbolt locks offer an increased level of security for the perimeter. Adaptable to any security system, electric deadbolts perform well as auxiliary locks on doors where access control is desired.

The main actuation component of solenoid-operated deadbolt locks, like the one displayed in Figure 2.6, are electrically activated solenoids. When electric current is applied to the solenoid's coil, an electromagnetic field is developed around it. The electromagnetic field applies magnetic pressure on the core in the center of the coil, causing it to move. This movement either engages (activates) the physical locking mechanism or it disengages (deactivates) the locking mechanism.

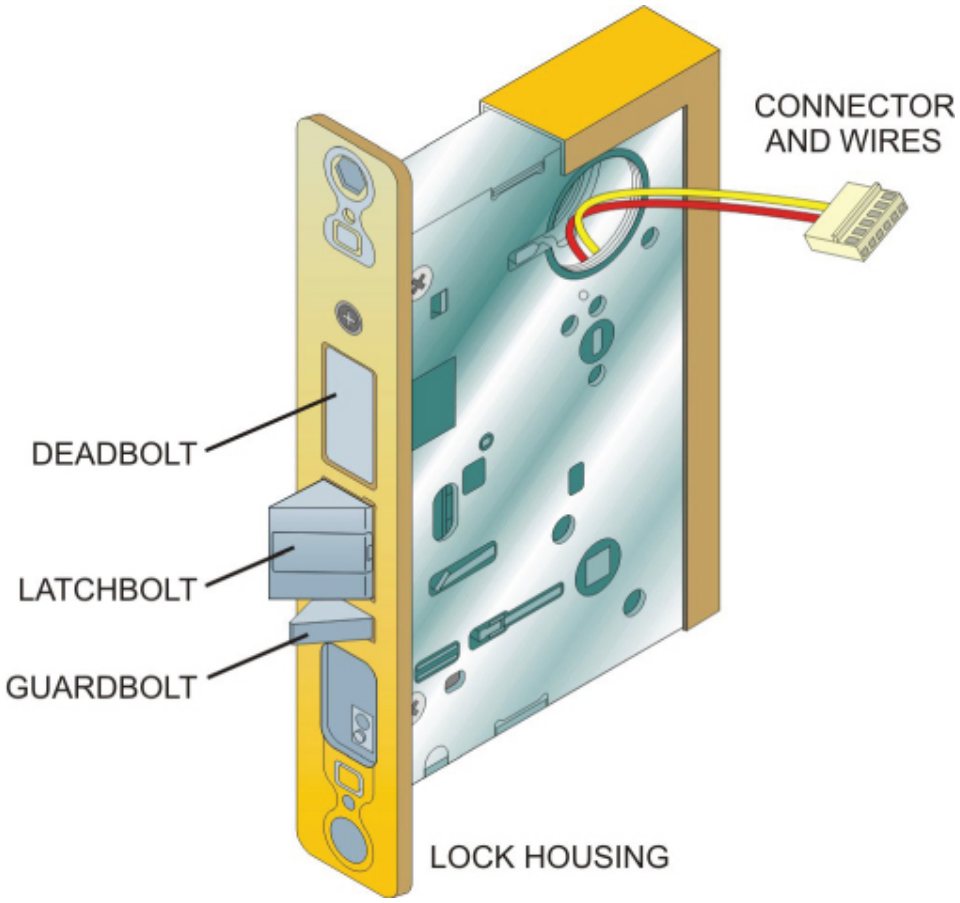


FIGURE 2.6 Electronic Deadbolt

The operation of the solenoid is typically controlled by a remotely located switch or through an electronic access-control system. In the latter case, the system is typically actuated by input from intelligent identification card-access devices.

Solenoid-operated deadbolts can be set to either lock or unlock when energized and are listed by Underwriters Laboratories (UL) as burglary-protection devices. In security applications, the solenoid lock is typically configured so that it automatically moves to the locked position when the door is closed. This helps prevent tailgating, where an unauthorized person slips past the locking door closely behind someone who is authorized to pass through it.

However, some doors that use automatic locks need to be configured to operate in a fail-safe manner (unlocks when power is removed). This type of configuration must be used to enable employees to exit through the door in case of emergency.

A dead-bolted door configured to operate in a fail-secure manner (locks when the power is removed) would not be suitable for use as an emergency exit, because it could not be used to exit the perimeter in an emergency. With a fail-secure lock, the door would default to the locked condition and would not open because of the lack of electricity to operate it.

Electronic deadbolts can be used with swinging, sliding, power-operated, and vertical-lift doors, as well as on fence gates.

Cipher Locks

Cipher locks requiring personal access codes known by the user are often used in access-control and management systems. These locks operate by unlocking magnetic door locks when the correct programmed code is entered by the user on the cipher-lock keypad. They provide an added level of security for perimeter entry areas. An example of a cipher lock is shown in Figure 2.7.

FIGURE 2.7 Cipher Lock

While electronic door pads may offer a more secure physical barrier, their entry codes need to be periodically changed for such pads to be effective over time.

Access-Control Gates

Like a door, a gate is a type of physical barrier that can be swung, drawn, or lowered to control ingress and egress through a wall or fence. Access-control gates can be classified into two main types:

- Sliding gates
- Swinging gates

Both types can be opened or closed through the use of a motorized operator. The size of the gate operator is determined by the width of the pathway and the weight of the selected gate.

Sliding Gates

Sliding gates, such as the one shown in Figure 2.8, are used where high levels of operational safety and security are needed.

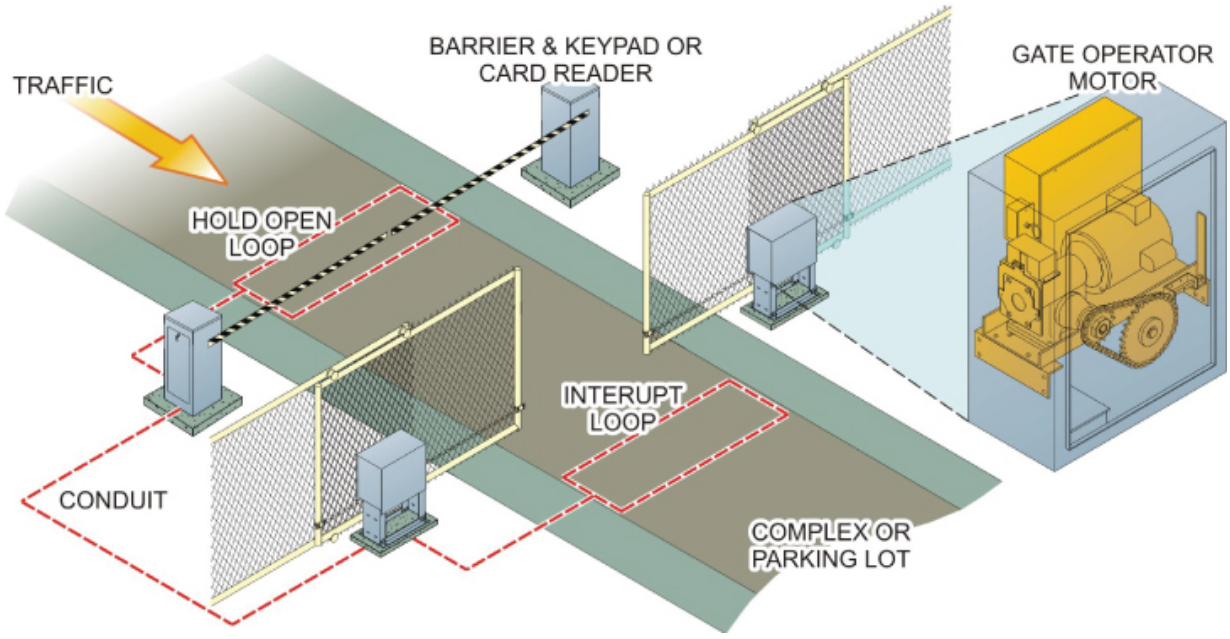


FIGURE 2.8 Sliding Gate

Swinging Gates

Swinging gates, like the one depicted in Figure 2.9, are equipped with fully adjustable hinges that allow the gate to swing through 180 degrees. An articulated arm, which runs from the operator to the gate, pulls or pushes the gate open and closed. Manufacturers sometimes use a piston/cylinder configuration as the actuator for the arm.

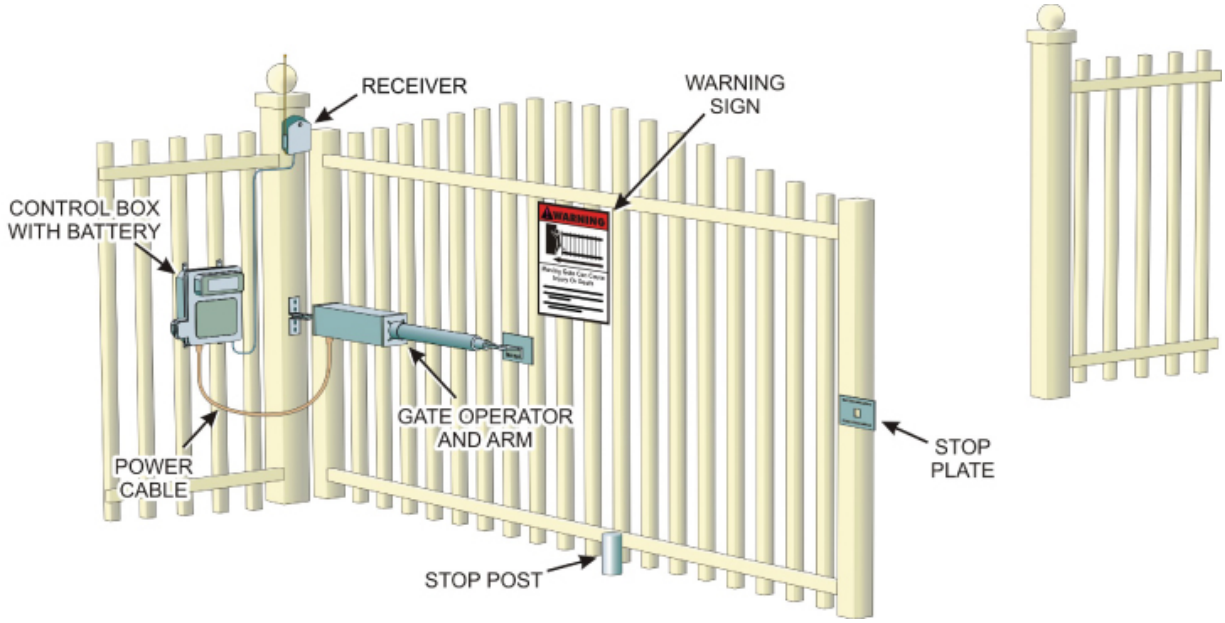


FIGURE 2.9 Swinging Gate

Control Relays

Relays are electromechanical devices that employ safer, low-voltage/low-current control signals to be used to control higher-voltage/higher-current devices. In access-control settings, relays are commonly used to control the operation of electric gates and door locks, garage door openers, and other remote devices.

Figure 2.10 shows a schematic diagram of a simple single-pole, single-throw (SPST) relay. As the diagram illustrates, the relay consists of a coil with two external connections, a Common connection, and two output connections.

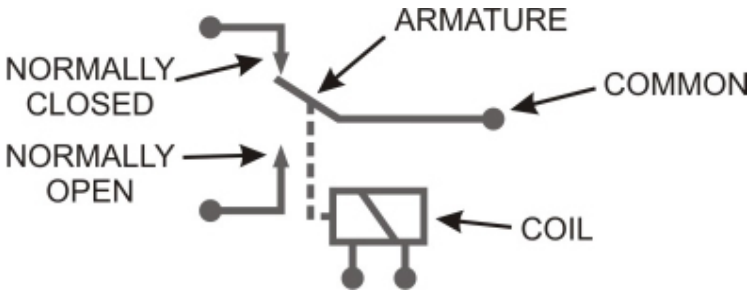


FIGURE 2.10 SPST Relay Schematic

The output connections are specified by their relationship to the Common connection when no energy is applied to the coil. One output is called the Normally Open (NO) contact and the other is the Normally Closed (NC) contact.

When no signal is applied to the coil, the relay is at rest, and there is a physical connection from the Common terminal to the NC terminal. Conversely, there is no physical connection between the Common and NO terminals. In this state, any signal (current) applied to the Common terminal will pass through to the NC terminal, but no signal (or current) can pass through to the NO terminal.

When an electrical current is passed between the two Coil terminals, the coil is energized, and everything changes. The magnetic field developed by the coil causes the electromagnetic core to move (in this illustration the core would move to the right).

The mechanical linkage from the core to the relay switch (shown as a dotted line) also moves. This opens the path between the Common and NC terminals and closes the path between the Common and NO terminals. Therefore, current can flow between the Common and NO terminals, but no current can flow between the Common and NC contacts.

Relay Operations

The decision to use the NO or NC output is typically based on the application the relay is being used to control. In many cases, control circuits are designed so that they provide either fail-safe or fail-secure performance. A fail-safe circuit is designed so that in the event of a power or component failure, the system being controlled will remain in its safe condition (either on or off).

The fail-secure circuit is one that fails in a most secure condition. For instance, if the power fails to an automated security gate, the system should fail in a manner that keeps the operation of the gate secure (it should remain closed unless it is opened manually from a secure location).

Activating relays are frequently built into the keypads, key fobs, door locks, or gate actuators. The relay kit shown in Figure 2.11 is designed for use as a gate controller and provides a view of the relay and associated components. The accompanying key fob is typically used to operate the controller.

FIGURE 2.11 Gate Controller Relay and Associated Components

Authentication Systems

Authentication is the process of determining that someone is who they say they are. Recall that effective access control involves being able to control the ingress, egress, and regress to an asset based on authorization. In particular, limiting the access of unauthorized personnel to important assets is the most fundamental security step that you can take. Therefore, authorization is based on authentication.

Multiple factors are involved in authentication:

- *Knowledge:* Something you know or something that only the designated person should know
- *Possession:* Something you have or something that only the designated person should have
- *Inheritance*: Something you are or something that only the designated person is
- *Location:* Somewhere you are or somewhere that only the designated person is

Many physical authentication systems are based on single authentication factors that depend on possession, such as possessing a key device that opens a lock. The key can be a physical or virtual key as needed to open physical or virtual locking mechanisms.

More intelligent and effective authentication methods involve two-factor authentication (a process that requires two of the factors to grant authorization) based on *knowledge* (something you know) and *possession* (something you have).

Advanced authorization and authentication methods include multifactor authorize and authenticate systems. In these systems, information must be presented to an authentication device that, in turn, passes it to the security controller's authentication system. A number of different authentication devices are used routinely in access-control systems. The major device types are covered in the following sections of the chapter.

Magnetic Stripe Readers

A *magnetic stripe card* is a physical credit-card-like device that contains authentication information in the form of magnetically coded spots on a magnetic stripe, as illustrated in Figure 2.12. The cardholder uses the information on the card to access physical spaces or assets by passing the stripe on the card through a magnetic card reader.

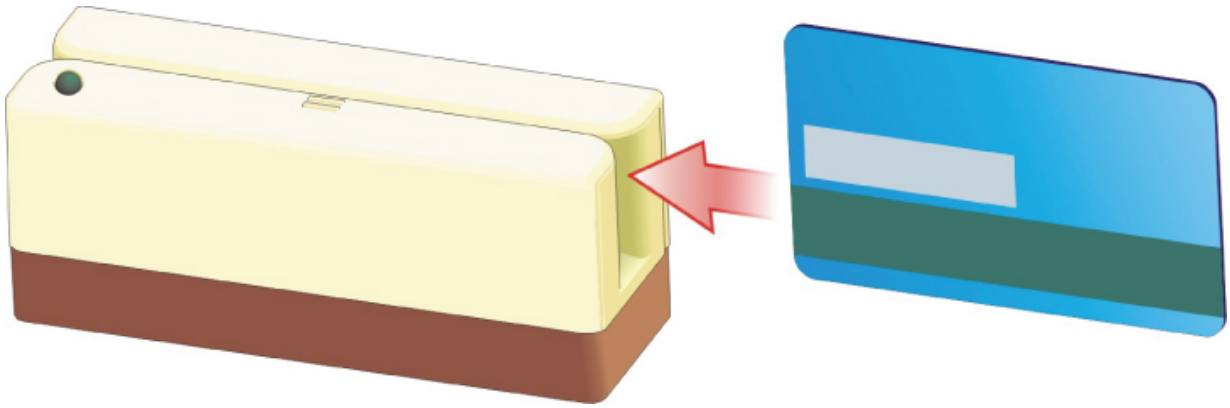


FIGURE 2.12 Magnetic Stripe Card System

The card reader reads the magnetically encoded information as it passes through the reader's magnetic sensor and translates it into digital data that it passes to a host system. The programming of the host system determines whether the information on the card is relevant to provide authorization and access for the cardholder.

Smart Cards

Smart cards are also credit-card-like devices that often resemble magnetic stripe cards, as shown in Figure 2.13. However, they offer improved data security due to the presence of intelligent circuitry that can be used to hide the user's data until an authentication process has been performed. They typically contain information about their owners, such as their passwords, personal identification numbers (PINs), network keys, digital certificates, and other Personally Identifiable Information (PII) that can be used in the authentication process.

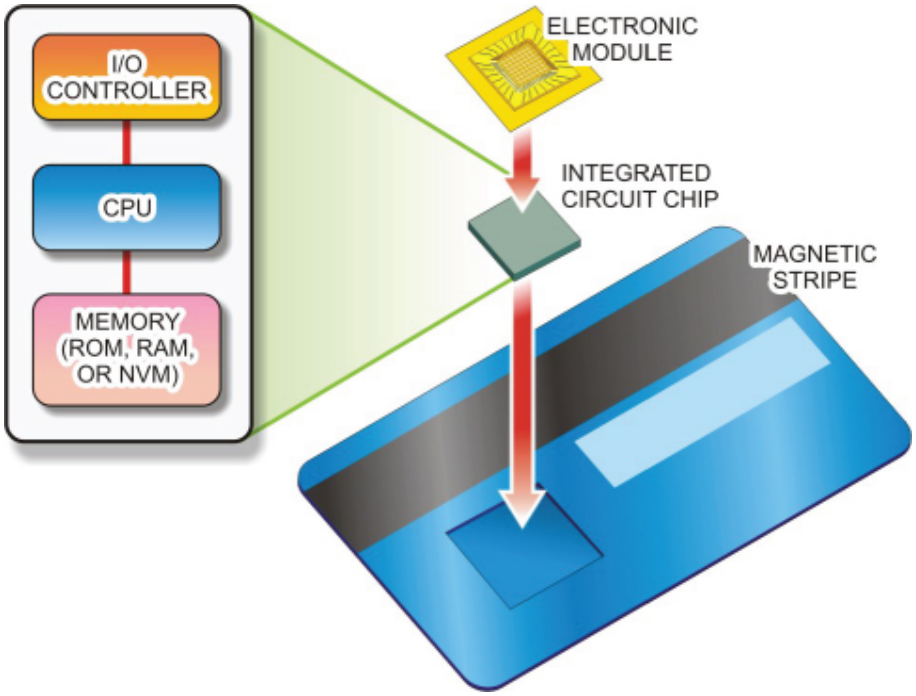


FIGURE 2.13 Smart Cards

A WORD ABOUT PII

PII is considered any information that has the ability to identify an individual. Examples of PII include: first and last name, home address, Social Security number, date of birth, fingerprints, and other information that may distinguish one individual from another.

Physically, smart cards are intelligent, credit-card-like devices, ID badges, and plug-in devices that communicate with a smart card reader.

Internally, all smart card designs contain a microprocessor and a memory device that are embedded in the card's structure. The smart-card memory section holds user-specific identification information, as well as all the programming the card needs to communicate with the host security system.

Some organizations that use smart cards issue their employees single cards that they can use to get into their buildings, log on to their

computers, and access appropriate applications.

Smart cards are designed to be resistant to tampering. Tampering with a smart card generally disables it. In addition, some care must be taken with smart cards as even bending one may render it unusable.

RFID Badges

Radio Frequency Identification (RFID) badges provide hands-free access-control tools that improve on the bar code, magnetic stripe, and proximity reader technologies. The RFID system employs radio signals to identify unique items using an RFID reader device and RFID tags, as illustrated in Figure 2.14.

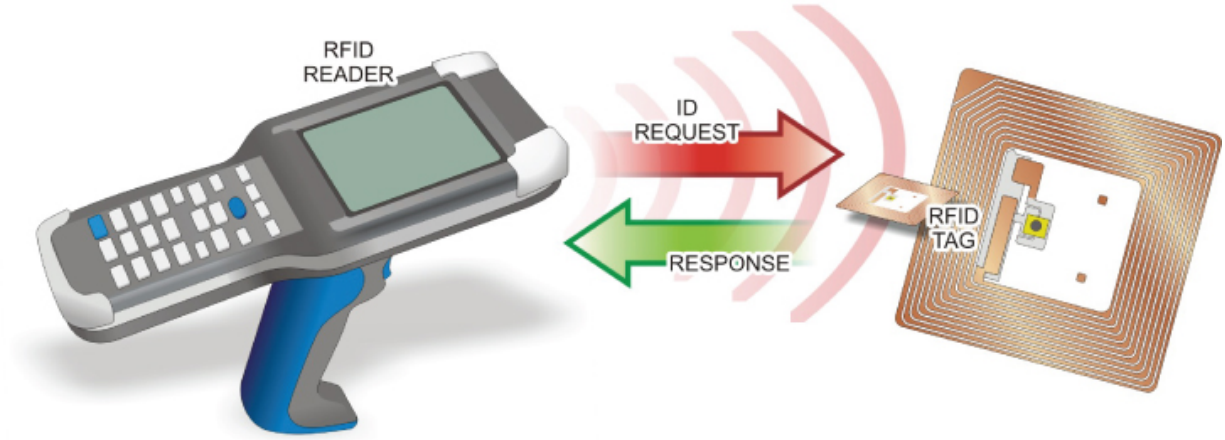


FIGURE 2.14 RFID System

The reader sends and receives radio frequency data to and from the RFID tags. Each tag stores the data sent to it on an embedded integrated circuit (IC) device. While the specific information stored on the RFID tag is determined by the RFID system programmer, it generally consists of a serial number that identifies it, along with information about the item with which the tag is associated.

When the system wants to know something associated with the tag, such as what (or who) it is associated with or where it is at, it simply sends out a request which causes the addressed RFID tag to radiate its information from its built-in antenna. The reader receives the data from the tag and relays it to its host computer for processing. The most interesting part of this technology is that the passive RFID tags are able to perform their task without the presence of an external power source.

Biometric Scanners

Biometrics is the term used to describe access-control mechanisms that use human physical characteristics to verify individual identities. Biometric authentication involves using uniquely personal physiological characteristics to verify people are who they say they are.

Every human possesses unique physical characteristics that differentiate them from other humans. Even identical twins have separate and distinctive voice patterns, fingerprints, eye features, and other characteristics. The qualities most often involved in biometric authentication include voice patterns, fingerprints, palm prints, signatures, facial features, and retinal and iris scans, as shown in Figure 2.15.

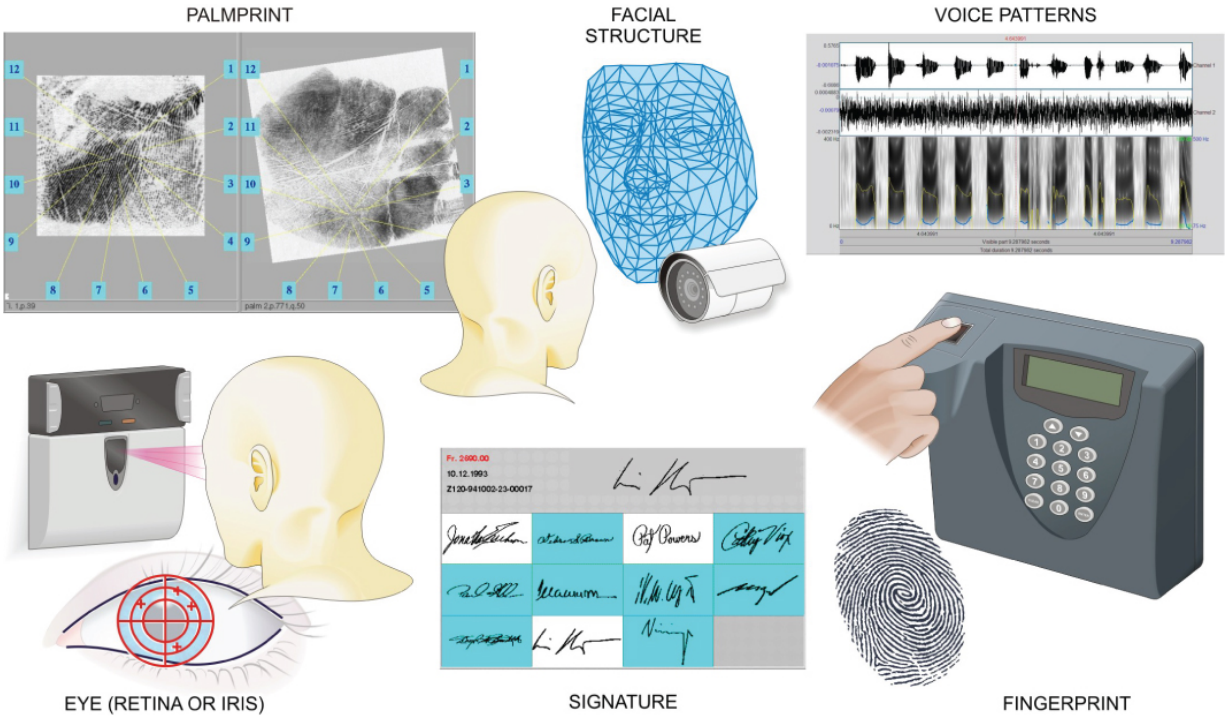


FIGURE 2.15 Typical Biometric Authentication Methods

In each case, a biometric scanning device is required to convert the physiological quantity into a digital representation. The results are stored in a database where they can be used in an authentication process. The underlying application will use the truly unique qualities of the data as a basis to compare with future access requests. If the data

from a future authentication request matches the key points of the stored version, then access will be granted.

However, not all biometric scanning devices are equally accurate at authenticating users. In Table 2.1, U.S. government data shows how different biometric scanning devices rate in terms of their abilities to accurately authenticate people.

TABLE 2.1 Biometric Device Comparisons

	False Positive Rate	False Negative Rate
Palm Print	**1.43%**	**4%**
Facial Structure	**0.1%**	**0.8 – 1.6%**
Voice Patterns	**2 – 5%**	**5 – 10%**
Eye (Retina or Iris)	**0.1%**	**1.1 – 1.4%**
Signature	**0.49%**	**7.05%**
Fingerprint	**2.2%**	**2.2%**

In general, the characteristics of the human eye—iris and retinal scans—tend to make it the most reliable source of authentication. Of the remaining biometric variables in the list, fingerprint readings tend to be more accurate than voice scans. However, fingerprints can be stored on a clear surface and used later. On the other hand, illnesses and user stress levels can affect voiceprints.

As shown in Table 2.1, there are two basic types of authentication failure:

Type 1 – False Rejection or False Negative Failures This is a report that produces an incorrect rejection of the individual, thereby locking them out of a facility or security area that they should have been able to access.

Type 2 – False Acceptance or False Positive Failures This is a report that incorrectly authenticates the individual, which could lead to providing access to equipment or data that this person should not be able to access. Of the two types of authentication failures, this is the most significant in that it could grant access to malicious people.

Because of the potential for false reporting and inaccuracies, a second method of access control may need to be used in conjunction with biometric devices. In areas requiring higher security, a passport, additional fingerprints, or some other type of verification could be used to ensure that the individual was not mistakenly authenticated.

Remote-Access Monitoring

Remote monitoring refers to monitoring or measuring devices from a remote location or control room. In the security realm, this involves having external access to the security system through a communication system.

Remote-access monitoring systems are used to notify supervisory security personnel when an unauthorized access is attempted. In these systems, the controller monitors the open/close conditions of the infrastructure's sensors. When a sensor such as a magnetic switch or a motion detector is activated, the system automatically identifies it as an intrusion and notifies specified security personnel of the occurrence.

The notification can come in the form of a visual notification on a security control panel, a call via telephone, an instant messenger notice, or a text message to a smart phone. The notification can also involve activating strobe lights and high intensity sirens to call attention to the intrusion attempt. Figure 2.16 shows different options for remotely accessing a typical security system.

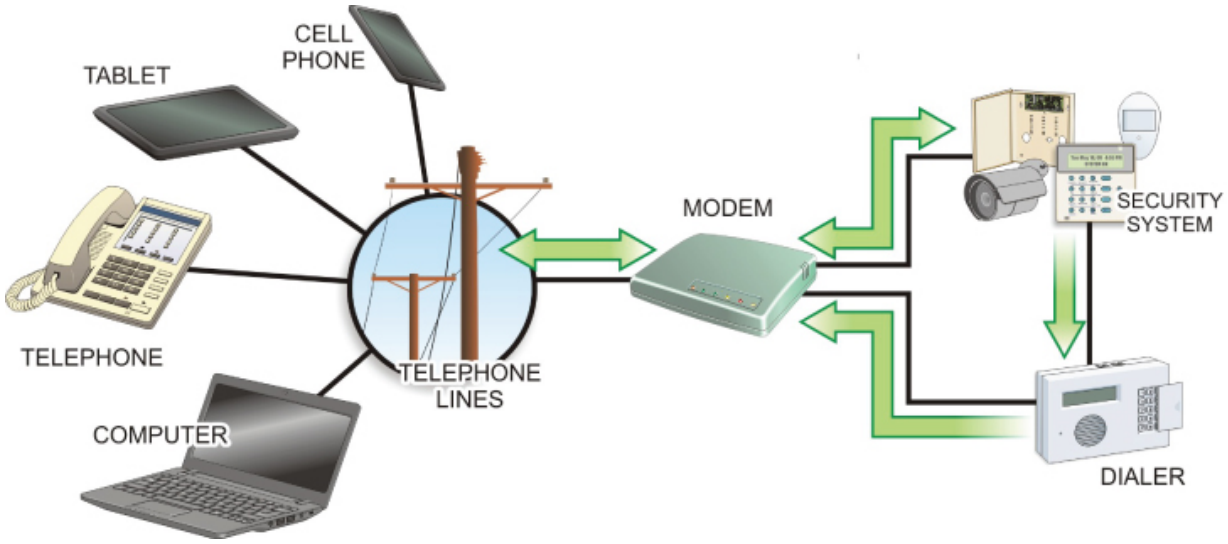


FIGURE 2.16 Remote-Access Communication Options

Opened- and Closed-Condition Monitoring

Various sensors can be used to detect the opened, closed, locked, or unlocked condition of an automated door or gate. They can also be configured to initiate an opened, closed, locked, or unlocked condition at a specified door or gate.

A WORD ABOUT SENSORS

Because open and closed conditions are not the same as locked and unlocked conditions, a single sensor cannot differentiate between these two sets of conditions. A second or different type of sensor needs to be installed and monitored to perform this differentiation.

A simple magnetic sensor and a matching set of contacts for a movable barrier (door, gate, or window) are shown in Figure 2.17. The sensor's transmitter sends a signal either to a control panel or to an emergency dialer when the magnetic switch contacts are broken as the door is opened.

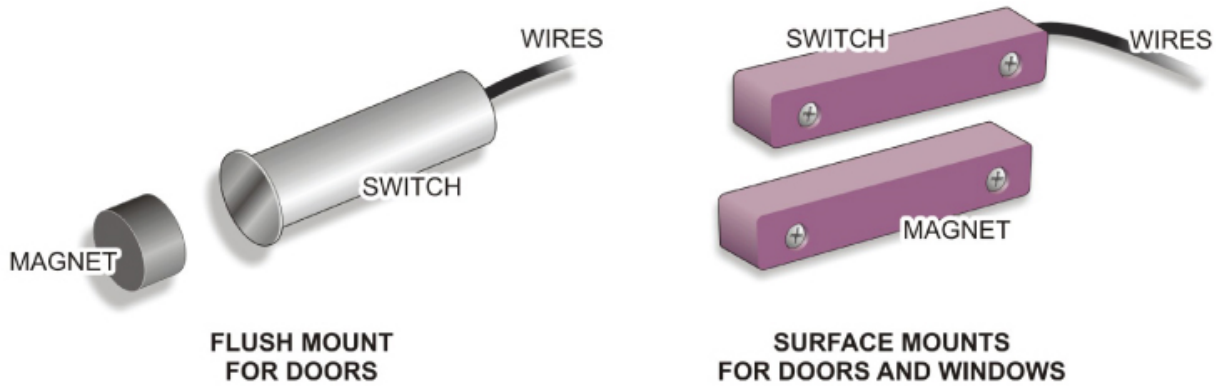


FIGURE 2.17 Window Sensor with Magnetic Switch Contacts

Signaling and reporting between the sensor and the controller is continuous during the elapsed time between the opening and closing of the barrier. If the barrier is left open for a specified time, that information is also noted and recorded by the system. The condition-monitoring system includes an event log, detailing the times and dates of various events. For example:

Locked-Condition Monitoring Locked monitoring is a feature that allows the security supervisor to confirm that a door is locked. In addition to monitoring the locked status of a door or gate, the condition-monitoring system can also provide details as to how long and during what time periods the door or gate has remained locked.

Unlocked-Condition Monitoring The condition-monitoring system can record and signal each time a specific gate or door is unlocked (granting access) and what type of access was granted. Unlocked monitoring can also identify who was granted access.

Time-of-Day Settings Most automated access-control systems base decisions about valid or invalid entry requests, also called *transactions,* on preconfigured time-of-day settings. This is normal because any entry request that does not fit the predefined time profile or time schedule of an identified user is subject to suspicion.

Such a situation might occur for a daily delivery that arrives later than normally expected. The user, in this case a recognized delivery agent, has been identified but is seeking entry at an unauthorized time. An authorized human supervisor will need to intervene to accept the delivery.

Automated Access-Control Systems

Automated access-control capabilities add another dimension to standard security monitoring and reporting functions. Although automated access control is not an integral part of the typical intrusion-detection and monitoring system, it adds to the safety and convenience of perimeter-access control. Automated access-control systems come in two flavors: remote-access-control systems and remote-control access systems.

Remote-access control is a design feature that manages entry to protected areas by authenticating the identity of persons entering a secured area (security zone or computer system) using an authentication system located in a different location than the access point.

This can be accomplished by a number of methods including password readers, magnetic key cards, and secret-cipher lock codes.

Although the differences are minor, the design considerations for remote-control access systems are different from those for remote-access systems. Remote-control access is a design feature that works with remote monitoring systems to monitor, control, and supervise doors, gates, and conveyances from a distance. Figure 2.18 shows the typical components involved in a remote-access-control system.

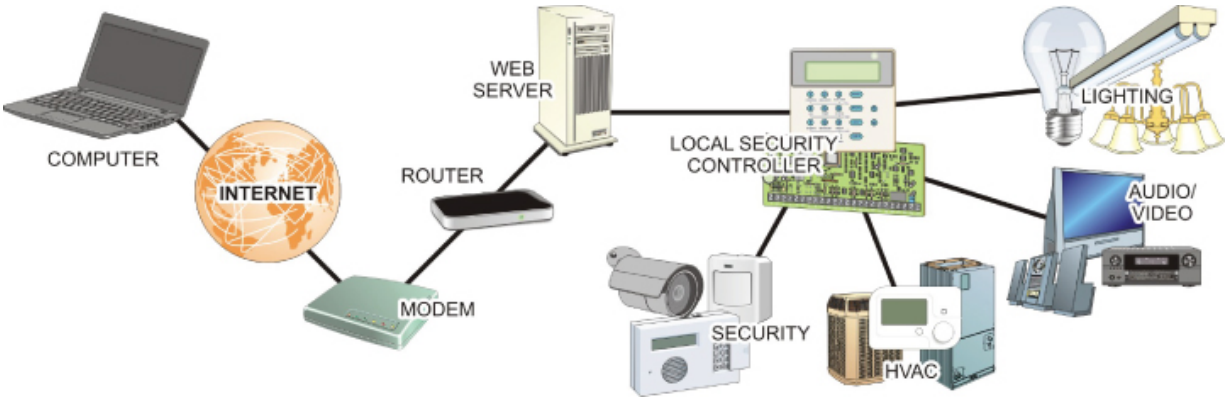


FIGURE 2.18 Remote-Control Operations

The Remote Control function enables the security specialist to initiate communications with a remote site, enter an access code, obtain current conditions, and set system parameters. A closed-circuit television (CCTV) system may be added to the security system to provide visual

recognition functions to the remote-control options. Some remote-monitoring and control systems, such as the one depicted in Figure 2.19, can also be used or obtain status messages concerning any sensor that has detected a value outside of programmed values such as heat, cold, water leakage, loud noises, alarm history, or other custom features.

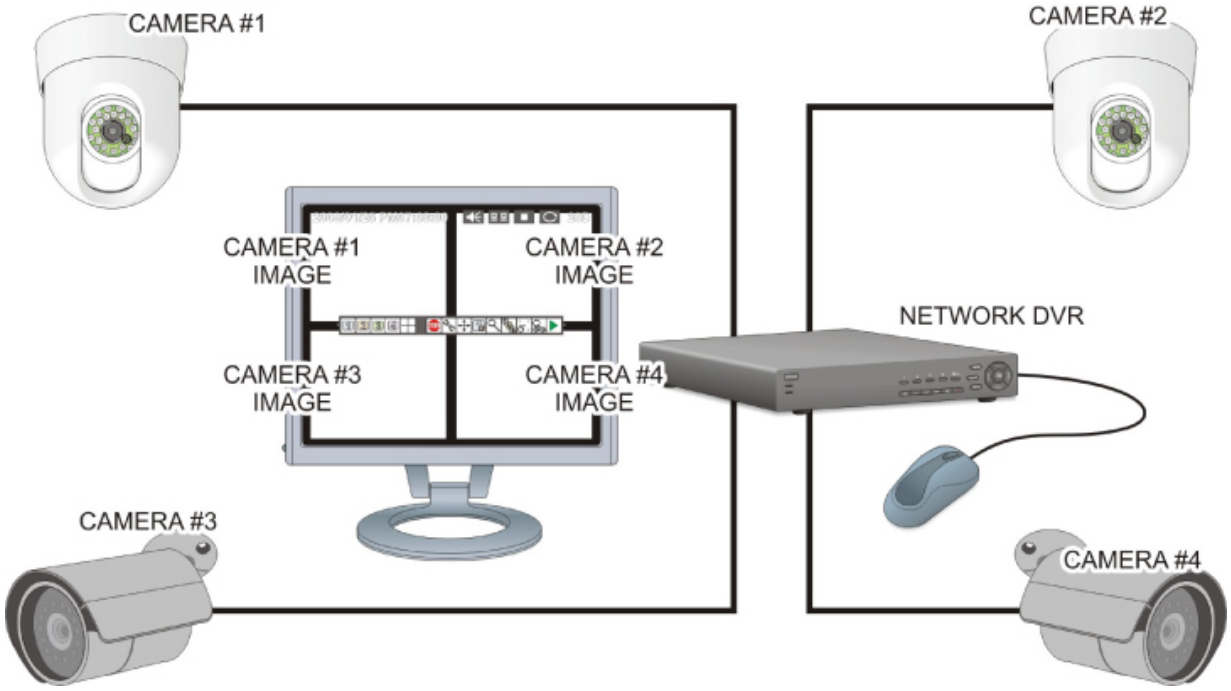


FIGURE 2.19 Remote-Monitoring Systems

Wireless communications devices are often used to connect the components of an automated access-control system. This type of connectivity is an economical solution that eliminates the need for new wiring between control devices, intercoms, and electrically operated security gates and doors.

Hands-On Exercises

In this exercise, you will learn how to secure the outer perimeter. The objectives include:

- For a given facility, define its outer perimeter, inner perimeter, and interior areas, and determine key vulnerabilities associated with each layer.

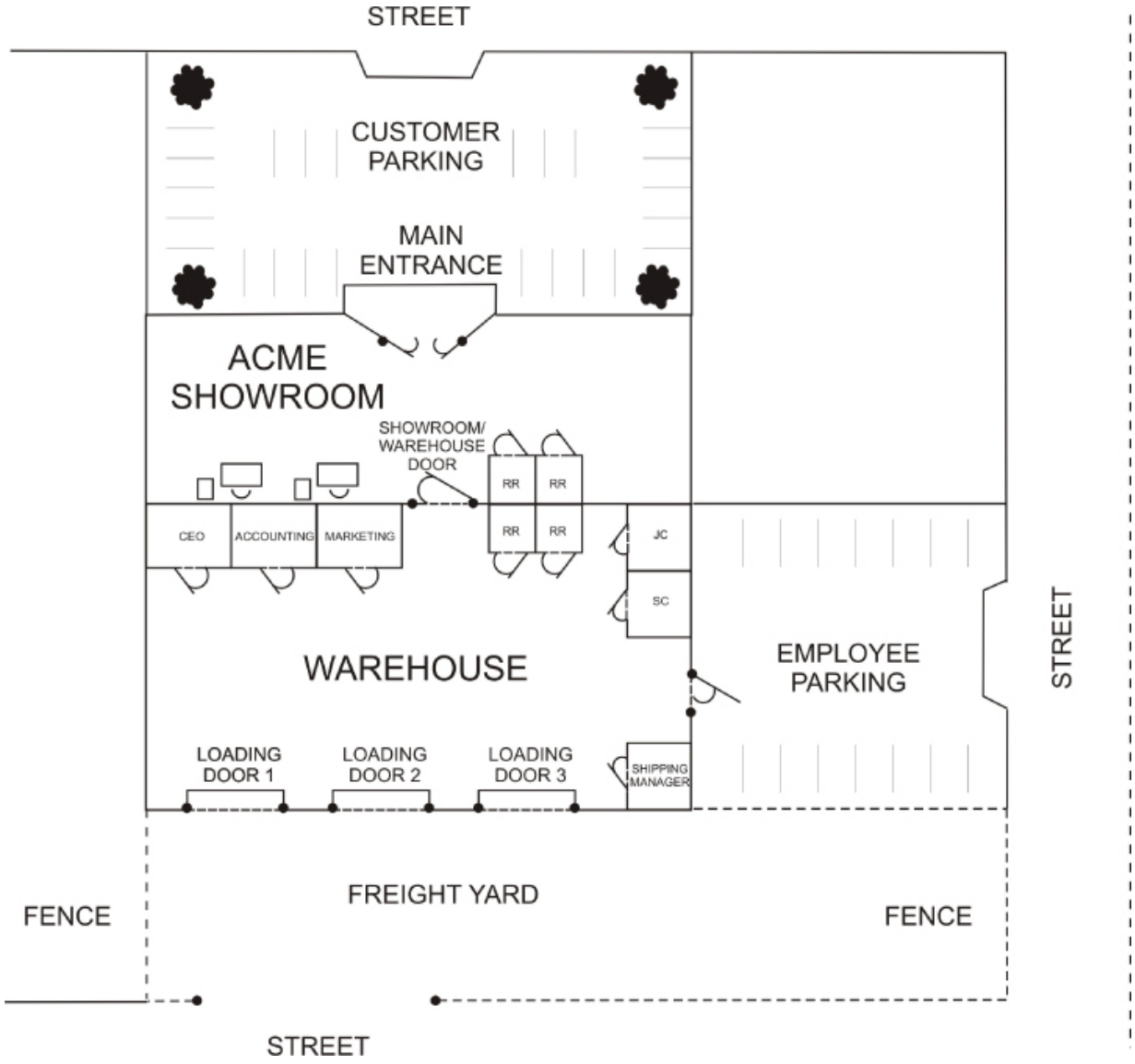
- For the specified facility and its vulnerabilities, perform research to determine what components (devices and systems) are available to secure these points and what the cost options are for the components you find.
- Design an access-monitoring and control system for the outer perimeter of the facility that will enable the customer to implement the security system required to monitor and control access to their facility.

The resources necessary for this exercise are as follows:

- Internet access
- Pencil/pen and paper

Discussion

Figure 2.20 depicts the ACME warehouse facility. This facility is used to store ACME products that are ready for shipment. Its loading docks handle tractor trailer trucks, as well as smaller delivery trucks, through three roll-up doors. The trucks pass in and out of the warehouse loading yard located at the rear of the building through a 30-foot-wide opening in the fence that surrounds the yard. The fence attaches to the building at each corner of its back wall, as shown in the figure. The truck opening in the fence provides access to the street that runs behind the warehouse.



[FIGURE 2.20](#) The Facility

Customers enter the building from the front where there is an open parking area and an attractive customer entrance featuring double glass doors. This parking area is open to the street and has no fencing around it. The customer showroom and sale staff desk areas occupy the front of the building, while the warehouse and management offices are in the rear of the building. Employees can transition between the warehouse and the showroom through an interior pedestrian door between the two portions of the building.

ACME personnel park in an employee parking area along the side of the building. They enter the facility through an employee pedestrian door

that faces their parking area. The employee parking area is open and also has no fencing around it. Each ACME employee (warehouse, showroom, and management) will be issued a company ID device. The access-monitoring and control system should be capable of determining which employees have authorization to enter the warehouse portion of the facility.

The warehouse also houses the management offices and a pair of supply closets. Each office has a single window that faces the showroom and a door that opens into the warehouse area. The supply closets are equipped with a solid door and no windows.

The facility is nearing completion, and the ACME Company has asked you to research and recommend security and surveillance systems that will enable them to monitor and control the flow of people into and out of their warehouse.

Procedure

In this procedure, you will use whatever resources you have available to research physical security devices and systems that can be used to secure the outer perimeter of the ACME facility in preparation for developing a comprehensive physical-security proposal.

1. Examine Figure 2.21 and create/label a three-perimeter, multilayer security topology for the ACME facility.

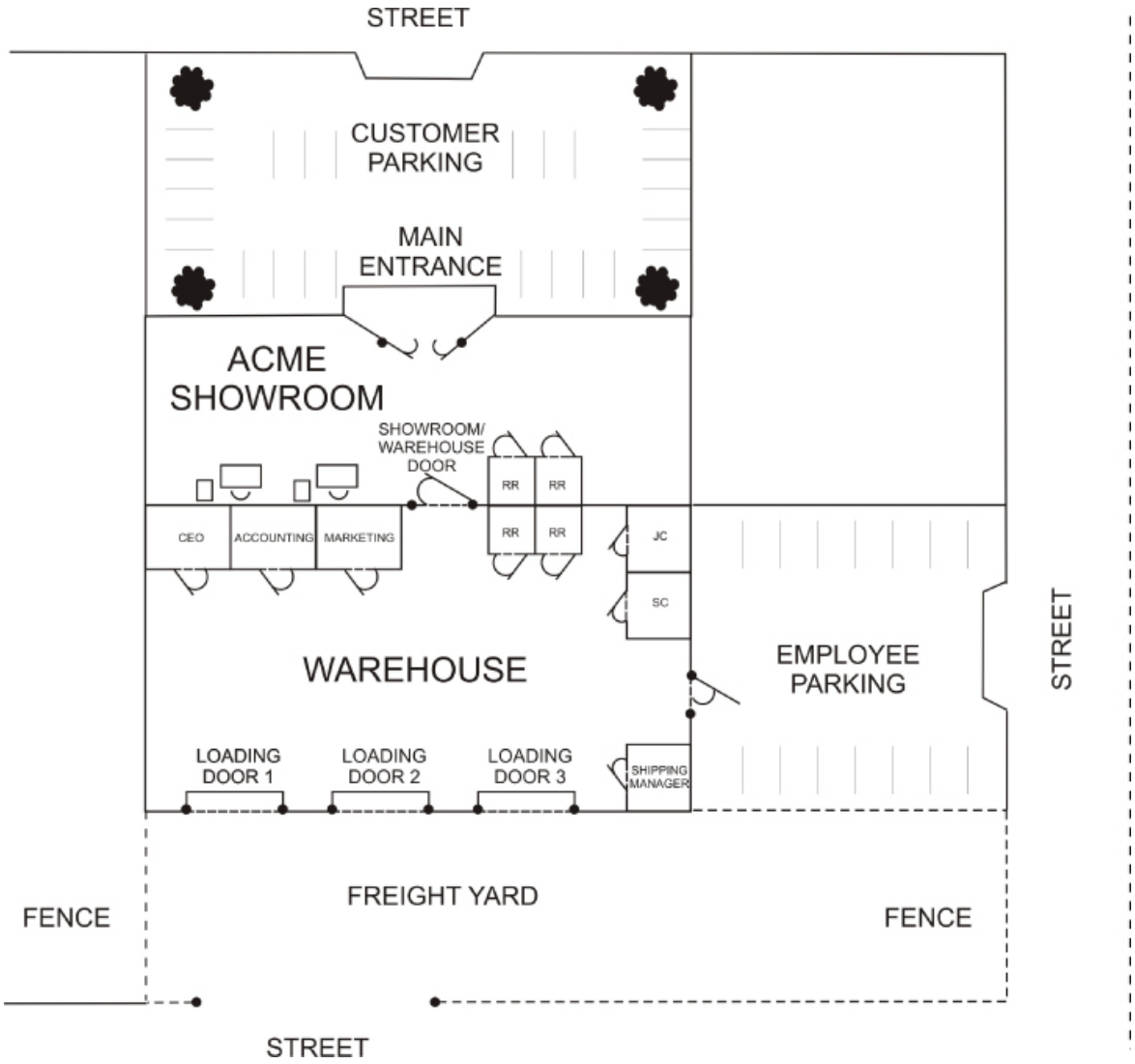


FIGURE 2.21 Security Perimeters

2. After establishing the three perimeters of the security topology, return to the figure to identify and mark the physical access points associated with the facility's outer perimeter.
3. Use the Internet or other available research tools to research access-monitoring and control devices and systems that can be used to secure the access points you've identified in Step 2. Use Table 2.2 through Table 2.10 to organize the specified details about the access-monitoring and control products you find there. For each item, try to locate at least two vendors.

TABLE 2.2 Access-Control Gates

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Slide Gate Op.	DoorKing	1	$889.00	$889.00
B	Slide Gate Op.	Viking	1	$1,048.00	$1,048.00
C	Slide Gate Op.	LiftMaster	1	$1,499.00	$1,499.00

TABLE 2.3 Access-Control Doors

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Electronic Keyless Door Lock	Gino Development	1	$89.99	$89.99
B	Mag Door Lock Kit	Entry Vision	1	$274.99	$274.99
C	Cobra Controls Lock Kit	Maglocks.com	1	$1,699.99	$1,699.99

TABLE 2.4 Door/Gate Actuators

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Chain Drive	Genie	3	$185.88	$557.64
B	Jackshaft	LiftMaster	3	$273.39	$820.17
C	Screw Drive	Genie	3	$229.00	$687.00

TABLE 2.5 Security Controllers

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	HAI OmniPro II	Leviton	1	$1,094.90	$1,094.90
B	Honeywell Intrusion	Ademco	1	$345.53	$345.53
C	Mercury Security EP4502	Mercury Security	1	$1,495.90	$1,495.90

TABLE 2.6 Security Keypads

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Omni 33A00-4	Leviton	1	$192.00	$192.00
B	Honeywell Lynx 7000	Alarm Liquidators	1	$204.95	$204.95
C	Interlogix CaddX Keypad	Home Security Store	1	$94.65	$94.65

TABLE 2.7 Door Contacts/Sensors

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Door Sensor Wired	SensaPhone	8	$9.00	$72.00
B	Gate & Com. Door Sensor	Gogogate	8	$35.00	$280.00
C	SDC MC-4	Grainger Industrial	8	$53.95	$431.60

TABLE 2.8 Driveway Sensors

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Driveway Sensor	Mighty Mule	1	$180.78	$180.78
B	Direct Burial Sensor	CarSense	1	$208.46	$208.46
C	WPA 3000 Magnetic Probe	Absolute Automation	1	$249.00	$249.00

TABLE 2.9 Authentication Devices/Systems

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Mag Door Lock Kit	Entry Vision	1	$274.99	$274.99
B	Electronic Keyless Door Lock	Gino Development	1	$89.99	$89.99
C	Cobra Controls Lock Kit	Maglocks.com	1	$1,699.99	$1,699.99

TABLE 2.10 Door Locks

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Mag Door Lock Kit	Entry Vision	1	$274.99	$274.99
B	Electronic Keyless Door Lock	Gino Development	1	$89.99	$89.99
C	Schlage B581	Doorware.com	2	$52.00	$104.00

4. List your selection for the access-control gate/gates you think should be recommended to ACME to secure the entrance to the truck-loading yard.

   _____

   Answer: Viking meets the desired specifications for length and anticipated weight requirements to open a 30-foot sliding gate for the best price point. Vendors can be given access through RFID card or programmable access code.

5. List your selection for the access-control doors that you think should be recommended to ACME for controlling their outer perimeter.

   For the Warehouse Pedestrian Door:_____

   Answer: The Entry Vision unit can use programmable keycards to allow all employees access to enter the building at the beginning of their work day. Manual deadbolt locks can secure the door at night.

   For the Showroom Entry Doors:_____

   Answer: Manual deadbolt with actuation to inside of showroom only.

6. List your selections for the any access door/gate actuators you think should be recommended to ACME.

   _____

   Answer: The LiftMaster model can be configured to meet the needs of business, can be tied into security system to trigger if activated after an alarm is set or bypassed, and can be remotely operated by management or CEO if tied into network for after hours or weekend deliveries.

7. List your selection for a security controller you think should be recommended to ACME to monitor and control the access points in their outer perimeter.

   _____

   Answer: Leviton HAI OmniPro II. It offers the best price point for the features. The OmniPro II is Leviton's flagship security and

automation control system. Boasting the largest feature set, it can control the maximum number of devices and is designed to provide security and automation for large residences and small commercial installations such as restaurants, offices, and franchise locations. This allows all security considerations to be tied into one controller with multiple zone configurations for varying perimeter requirements. It can cover up to 176 zones so you can segregate or integrate as needed.

8. List your selection for the security keypad you think should be recommended to ACME to enable and disable functions of the security system controller.

   _____

   Answer: Omni 33A00-4 is the best selection because it can be expanded for increased control over loading-bay doors and a slide gate in the freight yard, and it is guaranteed to be compatible with the selected controller.

9. List your selection for the door sensor types you think should be recommended to ACME for their outer perimeter access points.

   _____

   Answer: The Gogogate sensors with an integrated indoor and outdoor sensor system utilizing magnetic contact sensors should be used for eight units. There is a wide enough gap for commercial and residential applications, so they should work well with delivery bay and pedestrian doors as well as the freight gate to monitor access.

10. List your selection (if any) for driveway sensors that you think should be recommended to ACME for the truck gate.

    _____

    Answer: The CarSense unit can be used to automate the opening of the gate for delivery trucks leaving, and it can be tied into/bypassed from the security system to trigger an alarm if activated by a vehicle leaving after hours.

11. List your selection for any authentication devices/systems you think should be recommended to ACME for controlling personnel access through their outer perimeter.

_____

Answer: RFID passcards should be used to enter through the pedestrian door to the warehouse from outside. The Mag Door Lock Kit already has this feature integrated as part of its design.

Also specify where you would employ the authentication devices/systems.

_____

Answer: They should be used to enter through the pedestrian door to warehouse from employee parking outside.

12. List your selection for the access-control door locks you think should be recommended to ACME. Also specify where you would employ the door locks you are recommending.

_____

Answer: The Mag Door Lock Kit should be applied to the outside warehouse pedestrian door for entry authentication and control. The Electronic Keyless Door Lock should be applied to the pedestrian door between the warehouse and showroom. It can be actuated without any authentication steps from inside the warehouse, but it requires a key or passcode to operate the door from inside the showroom. Schlage B581 should be used outside the showroom and outside the warehouse pedestrian door to secure the perimeter during closed hours.

13. On Figure 2.22, record the types of devices and deployment locations you would recommend to ACME's management to secure the outer perimeter of their new warehouse facility. Explain the reasoning for your recommendations on the lines provided.

_____

_____

_____

_____

Answer: Apply the Mag Door Lock Kit to the outside warehouse pedestrian door for entry authentication and control. Apply the Schlage B581 to the outside showroom and outside warehouse pedestrian door to secure the perimeter during closed hours. The

CarSense unit can be used to automate the opening of the gate for delivery trucks leaving, and it can be tied into/bypassed from the security system to trigger an alarm if activated by a vehicle leaving after hours. Use seven Gogogate sensors as an integrated indoor and outdoor sensor system utilizing magnetic contact sensors. The gap is wide enough for commercial and residential applications, so they should work well with the delivery bay and pedestrian doors, as well as the freight gate to monitor access. The Leviton HAI OmniPro II has the best price point for its features. The OmniPro II is Leviton's flagship security and automation control system. Boasting the largest feature set, it can control the maximum number of devices and is designed to provide security and automation for large residences and small commercial installations such as restaurants, offices, and franchise locations. This allows all security considerations to be tied into one controller with multiple zone configurations for varying perimeter requirements. It can cover up to 176 zones, so you can segregate or integrate as needed. The Liftmaster model can be configured to meet the needs of the business. It can be tied into a security system to trigger if activated after an alarm is set or bypassed. It can be remotely operated by management for after hours or weekend deliveries if tied into the network. Viking meets the desired specifications for length and anticipated weight requirements for opening a 30-foot sliding gate for the best price point. Vendors can be given access through an RFID card or a programmable access code.

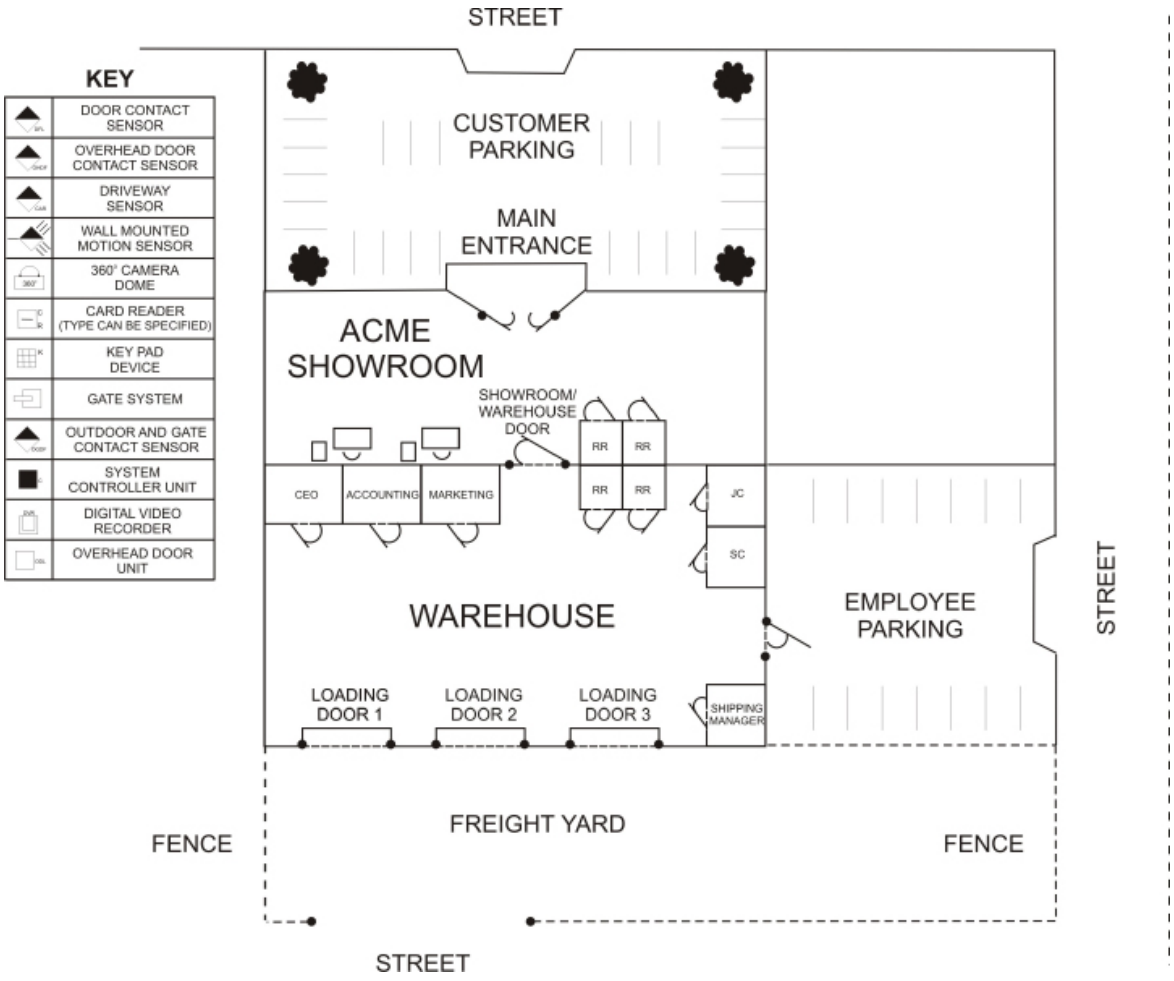


FIGURE 2.22 Device Locations

Review Questions

1. **Which access points are associated with the outer perimeter of the facility?**

   Answer: The street access opening in the fence for trucks to come and go, the warehouse employees' entrance door, and the main entrance door to the showroom

2. **The access door between the showroom and the warehouse are considered to be part of which security perimeter?**

   Answer: The inner perimeter

3. **Which access points are associated with the inner perimeter?**

Answer: The access door between the warehouse and the showroom, the loading dock doors, and the pedestrian door into the warehouse from employee parking

4. **In this exercise, which structure represents the interior security zone?**

   Answer: The warehouse

5. **The showroom should be considered to be a part of which security layer in this scenario?**

   Answer: The outer perimeter

CHAPTER 3
Understanding Video Surveillance Systems

Video surveillance systems—the second of the three basic types of subsystems introduced in Chapter 2—are important elements of most commercial security systems. Many organizations include visible cameras in their infrastructure security systems to inhibit unlawful activity and to record events that occur at the perimeter or key interior levels. In this chapter, you'll learn to:

- **Identify strengths and weaknesses of different types of security and surveillance systems and devices**
- **Select appropriate camera types when given specific scenarios**

Video Surveillance Systems

Video surveillance systems are based on closed-circuit television (CCTV) systems. The name is derived from the type of the system that transmits signals over a "closed circuit" or private transmission circuit rather than over a standard television broadcast system. Figure 3.1 shows the major components of a basic video surveillance system. Common components include:

- One or more video cameras
- A time-lapse video recorder
- A switcher (optional)
- A video display monitor

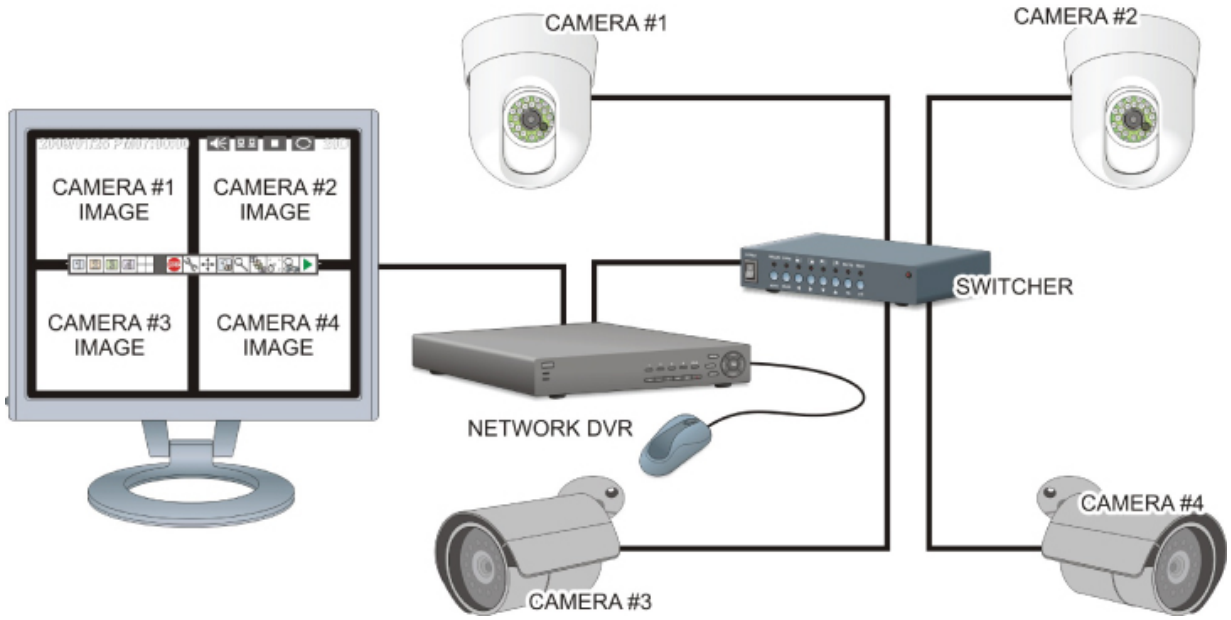


FIGURE 3.1 A Basic Video Surveillance System

In this basic system, the cameras monitor their fields of vision and pass the information to the video-processing equipment. In most cases, this equipment consists of a digital video recorder of some type.

In some cases, the flow of video information from the cameras is controlled by passive infrared (PIR) detectors. If there is no PIR signature (created by body heat) in the PIR detector's field of view, the video information is not transmitted. However, during event periods of motion detection, the video information flows from the camera to the video recorder. In such events, the cameras can be instructed to speed up the number of frames recorded per second to provide finer detail.

Some systems are based on coaxial cable for component connectivity, while others are IP-based and rely on wireless Wi-Fi communications or traditional network cabling.

The digital video-processing equipment can provide video output directly to a video display, or the video output can be channeled to a video switcher. In some cases, the video-processing component may offer its own integrated switcher.

These components are covered in greater detail in the following sections.

Cameras

Surveillance systems use video cameras that convert a viewed image into standard video-transmission formats (composite video, component video, S-Video, or HDMI signals) for display on a video output device, such as a monitor, television display, or personal computing device.

The best surveillance cameras employ Charged Coupled Device (CCD) technology. They have high-resolution, low-operating light requirements, less temperature dependence, and high reliability. A typical CCD camera used in video surveillance systems is illustrated in Figure 3.2.

FIGURE 3.2 Video Surveillance Camera

Surveillance cameras are available that use digital or analog interface technologies. Digital cameras convert the images they detect directly into digital signals that can easily be transmitted to and manipulated by digital computing devices. Analog cameras are based on older analog television signal and resolution standards. Cameras of this type require a separate coaxial cable to connect to a monitor or recording device.

Digital cameras generally offer superior performance over analog cameras. Analog cameras are more susceptible to quality degradation of the information being transmitted.

IP Cameras

IP cameras are actually digital IP (Internet Protocol) devices that have IP addresses that can be connected directly to a network, or to the

Internet, rather than directly to a host controller or computer. The advantage of using an IP camera, like the one depicted in Figure 3.3, is that it can be viewed from anywhere in the world where Internet access is available.

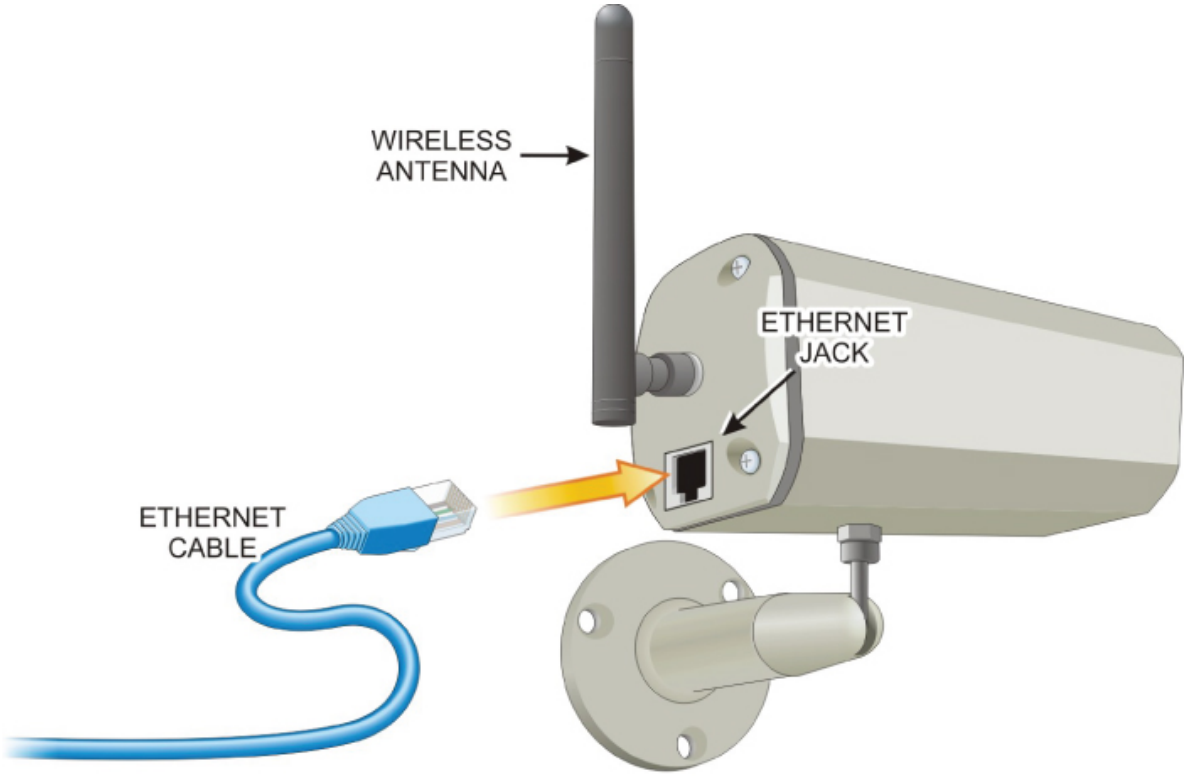


FIGURE 3.3 IP Camera

What sets IP systems apart from other video technologies are the abilities to email notification of motion sensing, process simultaneous user logins, and conduct FTP upload operations. An additional benefit of these cameras is that they can be powered by Power over Ethernet (PoE), whereby power is provided through the network cable rather than from a dedicated power supply for each camera.

Pan-Tilt-Zoom Cameras

A network IP camera with Pan-Tilt-Zoom (PTZ) capabilities, like the one depicted in Figure 3.4, is a standalone device that permits users to view live full-motion video from anywhere. This type of camera is designed for use either on a proprietary computer network or over the Internet using only a standard web browser as its display unit.

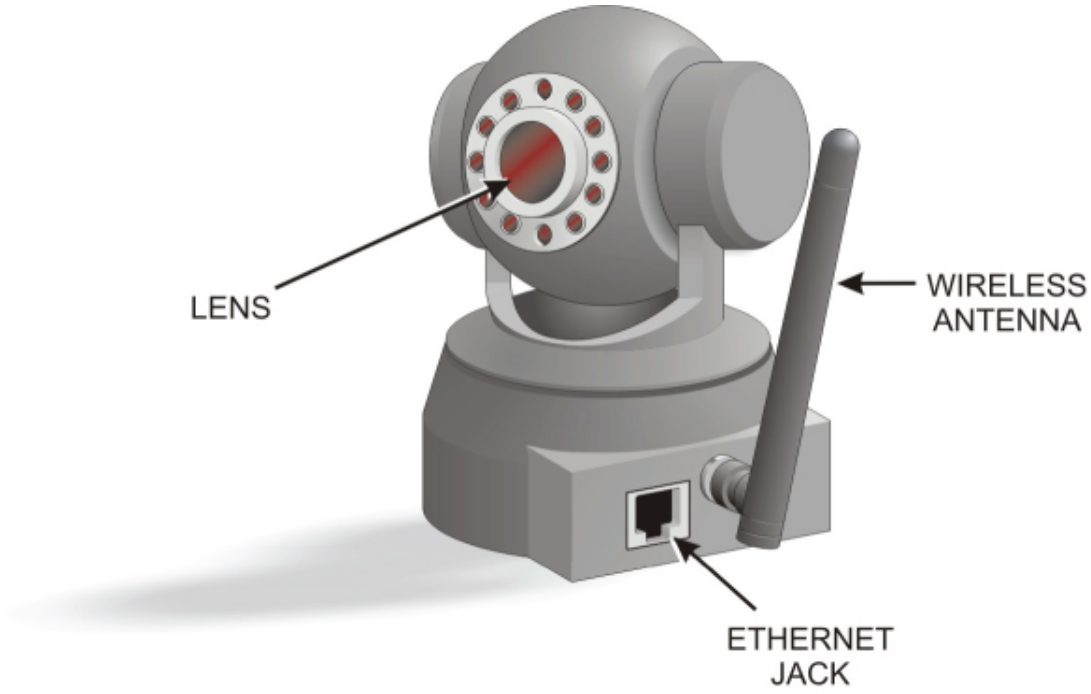


FIGURE 3.4 Pan-Tilt-Zoom Camera

Not only is manual Pan-Tilt-Zoom control provided, the ability to remotely direct dozens of positions for each PTZ-capable camera is also possible.

Camera Specifications

The two important specifications that influence the cost of cameras are light-sensitivity rating and resolution. The camera's resolution-specification method depends on whether it is an analog camera or a digital camera.

Resolution for an analog camera is specified as the number of horizontal lines it is capable of generating from top to bottom of the display. With digital cameras, the resolution is expressed in terms of the X-by-Y (horizontal-to-vertical) dot (picture elements or pixels) matrix format it produces. Figure 3.5 illustrates the meanings of the different camera-resolution specifications.

FIGURE 3.5 Analog and Digital Camera Resolution

The amount of light required to obtain a reasonable video camera image is called the *lux rating*. Lux is a measure of the amount of light that falls on an object. One lux is approximately the amount of light falling on one square meter from one candle measured from one meter away. Typical camera ratings range between 0.5 and 1.0 lux.

The lower the stated lux rating of the camera, the better the camera is able to differentiate objects at lower light levels. Conversely, the higher the number of lines of resolution, or the greater the number of pixels for a given surveillance camera, the better it will display the fine details of the view.

Lens Types

Surveillance cameras come in a variety of lens specifications. The lens size determines the camera's field of view and zoom capabilities. In general, the larger the lens, the narrower and more highly focused the field of view will be.

For example, a fixed lens rated at a 3.6 mm focal length is designed to provide a field of view of approximately 72 degrees, while a 6 mm focal length lens should provide a 44-degree field of view. As a general rule, the shorter the focal length of the lens, the wider the field of view.

On the other hand, a lens with a shorter focal length will also produce a view that provides less image detail. At a distance of 16 feet (5 meters), a 3.6 mm fixed lens may only provide a general description of the objects in a parking facility, while the same camera with a 12 mm lens would

provide sharper details of objects in the field of view (such as faces and license plate numbers) but might only cover a fraction of the facility.

You must also determine the objectives of having surveillance cameras. Are they to provide a visible deterrence? Are they to be used for gathering legal evidence? It is always important to select surveillance cameras with lens specifications that will capture the desired viewing area. Common security-camera-lens types include:

Varifocal Lens These are optical assemblies containing several movable elements that permit the effective focal length (EFL) to be changed. Unlike a zoom lens, a varifocal lens needs to be refocused with each change. If a surveillance camera has a fixed lens, it can see only one fixed position. If it has a varifocal lens, it can focus at multiple mm settings based on the user's preference.

Fixed Focal Length Lens Lens that can't be refocused regardless of the distance to the subject.

Wide-Angle Lens Lens that provides the ability to see a wider image in confined areas than standard lens types.

Telephoto Lens The best type of lens for seeing details at long ranges.

Fish Eye Lens A type of lens that allows you to see an entire room, but with some distortion of the image.

Pinhole Lens Lens used for applications where the camera/lens must be hidden. The front of the lens has a small opening to allow the lens to view an entire room through a small hole in a wall.

Black and White versus Color

There is a common misconception that color CCTV cameras offer better pictures than black-and-white (B&W) CCTV cameras. The reality is that although color cameras are more enjoyable to view, both types of cameras are fully capable of providing quality pictures. The real question is what type of camera is better suited for a particular situation.

The most important practical difference between color and black-and-white cameras is that only color cameras can offer a full and accurate clothing and vehicle description. Law enforcement relies heavily on the reported colors of clothing and suspect vehicle when responding to calls

for service. Being able to look for specified colors greatly increases the likelihood of catching a suspect.

IR Illumination

Cameras with infrared illumination of the image area permit viewing in low-light conditions. This also provides the ability to maintain a degree of secrecy by using illumination that is outside of the visible light spectrum.

An infrared security camera has infrared LED lighting (light from a region of the electromagnetic spectrum than humans cannot see) installed around the outside of the camera lens. This lighting allows the camera to capture a good image in no-light settings. With a small amount of light (a low-light setting), the infrared camera can capture a picture that looks just like daytime. A typical IR camera is shown in Figure 3.6.

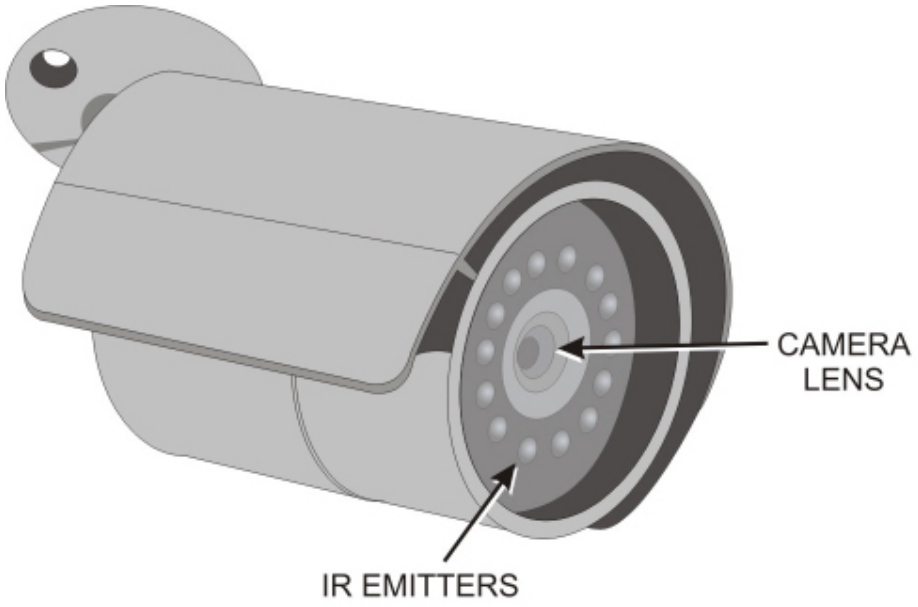


FIGURE 3.6 IR Camera

Camera Applications

Surveillance cameras can be mounted outside the facility to provide the ability to recognize someone wishing to enter the security perimeter area such as a front door or driveway gate. The cameras should be located where no blind spots exist or where it is not practical to use

other types of sensors. Cameras can be mounted on any surface area of the facility where coverage is required, as long as the area is illuminated sufficiently at all times after dark.

There are certain legal implications involved in using video surveillance cameras. In particular, there are privacy concerns that must be taken into account when deploying surveillance cameras. They should not be used where there is a reasonable expectation of privacy by individuals, such as in a restroom. This obviously does not apply to a person breaking into a facility.

Other applications for cameras are discussed in the following sections.

Indoor/Outdoor

Indoor cameras are usually less expensive than outdoor types because outdoor cameras must be housed in weatherproof enclosures. The cabling for outdoor cameras must also be suitable for temperature extremes and seasonal weather conditions.

Day/Night

Cameras are available that can switch from color imaging in the daytime and black-and-white for night operation when the illumination is too low for color. This provides the best tradeoff between good color resolution during daytime monitoring and black-and-white during night hours when the light levels are not sufficient for color imaging.

Fixed versus Animated

Cameras that are mounted in a fixed configuration always show the same areas. They are useful for monitoring important areas such as high-risk areas like parking areas and door entrances. Animated cameras provide the ability to move. They are mounted on a gimballed assembly where the viewing area can be changed, and they support zooming, tilt, and pan.

Recording and External/Interior Triggers

Digital Video Recorders (DVRs) are the preferred type of recording systems rather than older VCRs for surveillance cameras. Cameras can

be configured to record only when a trigger is generated to initiate recording.

Triggers can be internal types where recording is started when the scene changes. External triggers can be programmed to start recording when an alarm condition exists or when a motion detector triggers the recorder to begin recording.

Sequencing versus Multiplexing

Sequencing allows several cameras to be used with a single monitor. A switcher can be programmed to cycle through all of the cameras in a surveillance system or to dwell on each camera for a specified length of time, usually in the range of 1 to 60 seconds.

Multiplexers route the images from the surveillance system to a specific display device and are capable of recording all of the camera images at the same time by tiling them on the monitor.

Camera Deployment Strategies

The purpose for investing in security cameras is to be able to view activity in critical areas or where critical assets are located. In addition to determining what specifications security cameras must possess for a given role, it is equally important to map out a camera deployment strategy to maximize the surveillance investment.

To accomplish this, cameras should be positioned to capture important events in all critical security areas. In particular, they should be installed in passageways and in locations where their field of vision covers important assets (physical equipment and/or personnel).

Passageways include chokepoints in the physical facility where people or other traffic must pass through a portal, such as a gate, doorway, hallway, or access street/road. Cameras in passageways are typically placed there to document entry, exit, and movement through a facility, as illustrated in Figure 3.7.

FIGURE 3.7 Monitoring Passageways

Security cameras are routinely installed in positions that cover important assets and activities within the facility. This enables management to monitor activities around and associated with those important assets.

Bank lobbies are great examples of both placement strategies. Cameras are positioned to record activities around the bank's parking area and exterior, as well as in hallways that lead to the vault and offices, as illustrated in Figure 3.8. In addition, most banks have cameras arranged so they can focus on each teller station to monitor the handling of money and transactions.

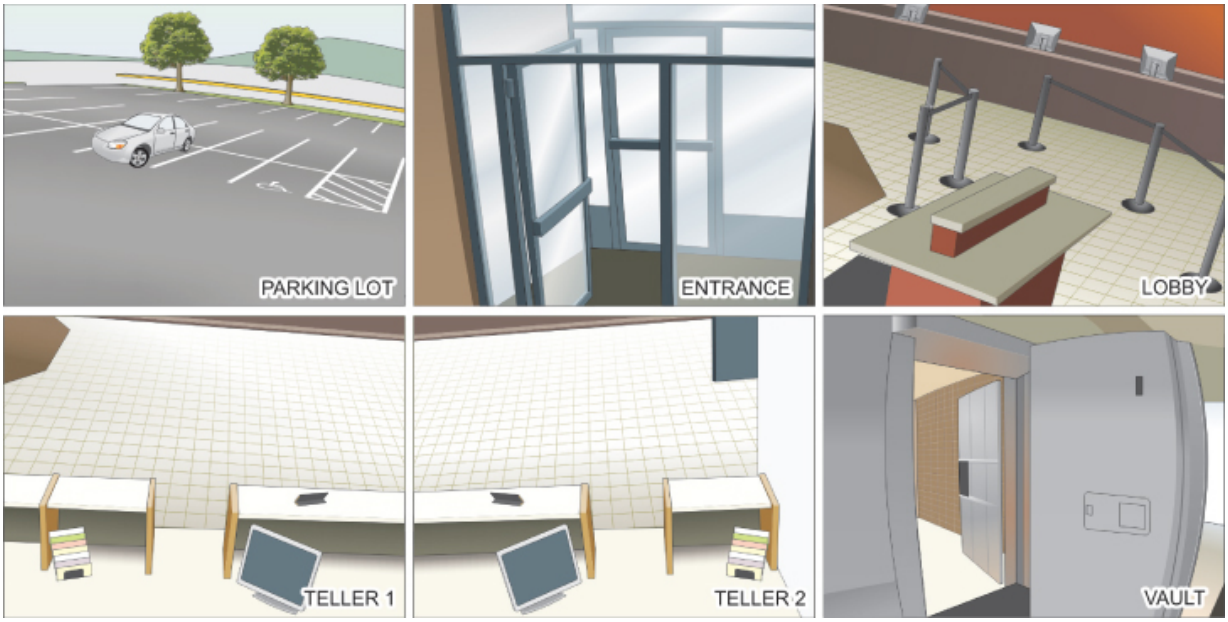


FIGURE 3.8 Asset Monitoring

Determining actual camera placement is a matter of first deciding whether the camera is required to provide an overview or detailed view. An overview generally covers a wide field of view, such as over a parking lot or warehouse floor. Conversely, a detailed view is required for targeting relatively narrow fields of view featuring specific areas of interest, such as the bank teller stations mentioned earlier.

The number of cameras involved in the installation depends on the number of passageways and assets that have been identified for viewing/monitoring. In some cases, this depends on the size of the organization; in others, it depends on the value of the assets and physical geography involved.

For example, a small operation may only need to install a single camera to provide surveillance of their key assets. For medium-sized operations, it is far more common for installations to involve dozens of cameras. In large organizations, hundreds of cameras may be deployed to meet their security and surveillance needs. The goal is to effectively cover the areas and assets identified through risk-analysis procedures.

After the installation points have been determined, the next step in the deployment strategy is to determine the specifications for the cameras to be used at each installation point. In general, the following four questions should be answered:

- Is a fixed or movable field of view required?
- Which type of image display is required?
- Which level of display definition is required?
- Which type of signal processing and transmission is best suited for the installation?

Fixed or Movable Field

Fixed cameras are typically employed for overview functions. They provide a fixed field of view, so they must be set up to effectively cover the desired passageway or asset. Therefore, they must have the desired focal length and angle to cover these items.

A remotely controlled PTZ camera is generally used where a detailed view is required. However, in some cases, it may be more economical to install several fixed cameras in different locations than to mount a single PTZ camera that requires an attendant to operate it effectively.

Image Display

From the previous discussion in Chapter 2, you should recall that common image display options include:

Color Color cameras are the default, general-purpose cameras in video surveillance applications today. The one application where color cameras lag behind other camera technologies is in low-light situations. In such cases, infrared or thermal cameras are generally advised.

Infrared Infrared cameras provide clear black-and-white images in very low-light settings. However, they tend to be significantly more expensive than color cameras.

Thermal Thermal cameras tend to be very expensive and produce only silhouettes. However, they also require no light to work.

Display Definition Levels

Is a standard video display acceptable for the view being addressed or is something with a higher definition required? One of the biggest complaints associated with standard definition systems is their inability

to deliver a signal that enables law enforcement and the courts to positively identify criminal suspects after a crime.

Signal Processing and Transmission

As described earlier in the chapter, the choices here include analog, digital, and IP cameras. IP cameras continue to gain acceptance over other types of cameras due to their ability to capture and transmit data electronically.

IP cameras also provide more robust connectivity options than traditional analog and digital cameras. They can work directly with a host computer without additional hardware. They are also more compatible with wireless networking options than other camera technologies.

Video Recorders

CCTV has traditionally been recorded using Videocassette Recorders (VCRs); however, such systems tend to be highly labor-intensive. The wear and tear on tapes is a constant problem, along with the need to perform periodic system maintenance.

The introduction of Digital Video Recorders (DVRs) has greatly reduced the dependence on storage media quality and operator intervention. The migration of video recording to digital media has permitted the storage of images to disk and has provided additional advantages such as:

- Ease of use
- Advanced search capabilities
- Simultaneous record/playback functions
- No image degradation
- Improved compression storage techniques
- Integration with other digital systems
- Remote system-management capabilities

Some video-processing systems feature built-in web server functions that provide remote access to either live images or recently recorded

ones. These web interfaces are capable of permitting viewing from one or multiple remote locations.

An example of a video-processing unit with built-in web access capabilities is shown in Figure 3.9. Units like this are capable of conducting Internet monitoring activities from remote locations.

FIGURE 3.9 A Video Recorder

Saved recordings can be searched according to date and time or according to activity/alarm mode options using real-time Video Motion Detection (VMD) technology. Active alerting can also be provided through email transmissions from the observing location.

Two of the most important considerations when recording video for security purposes are how much video needs to be stored and for how long. The answers to these questions enable the organization to determine its storage capacity needs.

Security video by its nature requires a substantial amount of storage space. As such, there is always a tradeoff between storage costs and the risk the organization faces. A single video surveillance camera can consume multiple gigabytes of storage capacity in a single day. With this in mind, the requirement for how long the organization needs to store surveillance video becomes a major decision point. Depending on the nature of the organization and the types of risks they face, the storage requirements may require that several weeks or months of video be stored for each camera they install.

As mentioned earlier, most organizations do not employ a single camera for their surveillance needs—they may employ dozens or hundreds of cameras. To store video data coming from so many cameras can easily require hundreds of terabytes of data storage.

Three common video-storage types can be employed to meet such needs:

Internal Storage Video information can be stored on the internal disk drive (or drives) in the DVR. This solution is practical only for small organizations that use few cameras and store the video information only for a short time.

Peripheral Storage or Direct-Attached Storage (DAS) This technique employs additional disk-drive storage devices that are attached directly to the DVR via USB or eSATA connections, as depicted in Figure 3.10. Direct-Attached Storage does not involve using an IP address to offload the video to the external device.

FIGURE 3.10 DAS Video Storage

Networked Storage This storage method uses networking techniques to store IP-based video on remote computers or video servers. The most common techniques for doing this include Network Attached Storage (NAS) and Storage Area Network (SAN) technologies, as shown in Figure 3.11.

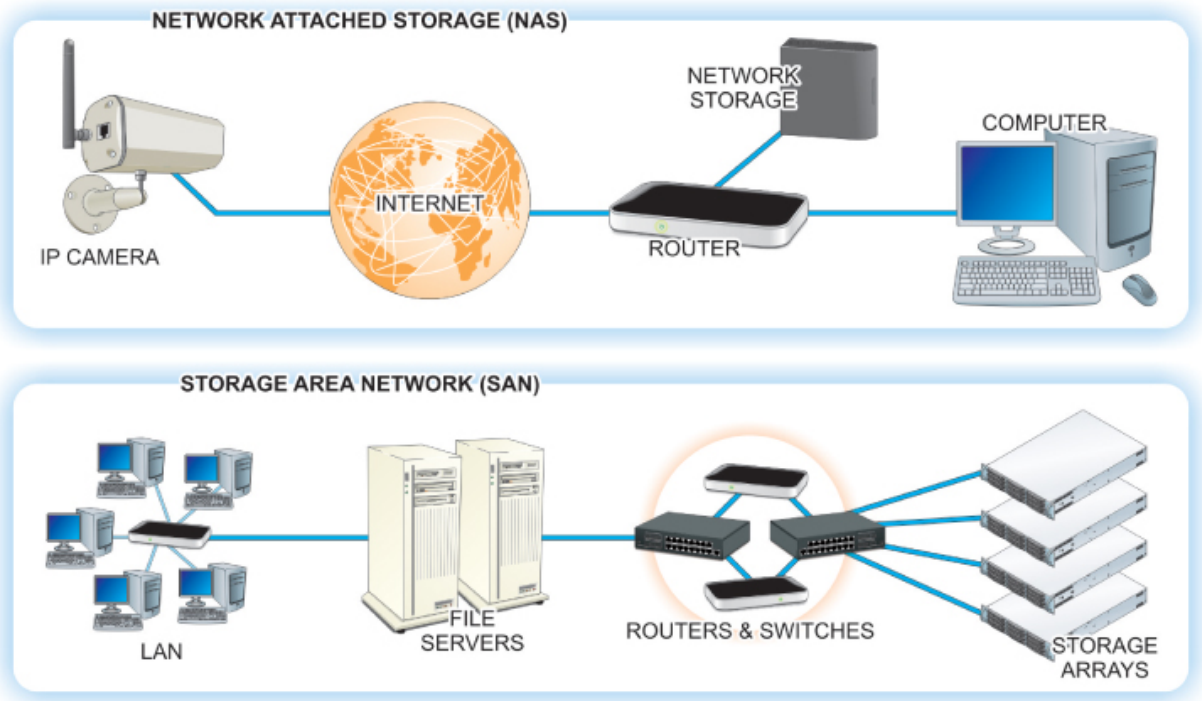


FIGURE 3.11 NAS and SAN Storage Systems

Switchers

Switchers are devices used with multiple-camera surveillance systems. They allow several cameras to be used with a single monitor. A switcher can be programmed to cycle through all of the cameras in a surveillance system or to dwell on each camera for a specified length of time, usually in the range of 1 to 60 seconds. Exterior sensors can detect movement and cause cameras to start recording on a video recorder.

A WORD ABOUT SWITCHERS

Four images can be displayed by a "quad" switcher. More advanced systems often provide simultaneous video recording, viewing, and playback activities using 4-, 9-, 16-, or 25-camera capacities.

A *quad* is a switcher that allows the viewer to simultaneously record and monitor four cameras at a time. It does this by splitting the monitor

screen into four sections. The normal configuration for connecting a quad switcher with a sensor and a video recorder is shown in Figure 3.12, which illustrates the connections between a quad switcher, a monitor, and four surveillance cameras. The monitor can view all four images at the same time. The sensor detects movement that triggers the video recorder to capture a recording of the event.

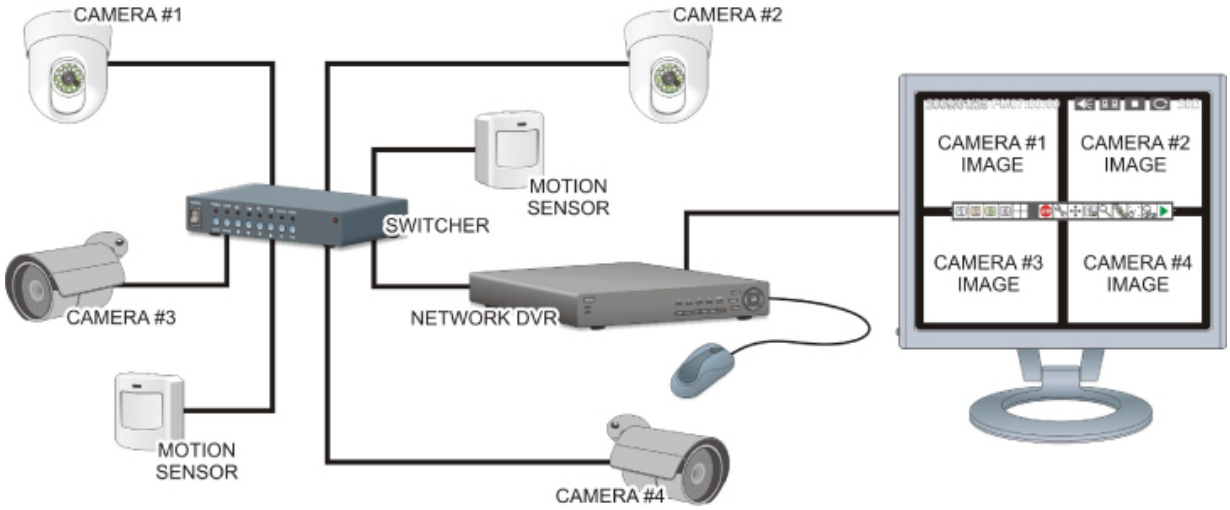


FIGURE 3.12 Quad Camera Switcher with a Sensor and Video Recorder

Typically, live images can be observed from one camera at a time or from multiple cameras simultaneously. Security personnel can use the interface to browse through and play back recordings from a specified camera, using fully adjustable built-in VMD.

Security Monitors

Monitors are video display systems similar to computer displays or televisions. They display video information that is obtained from the cameras and processed by video processing devices, such as the DVR. They may also be connected to programmable switchers that receive inputs from several cameras so as to show multiple images on a single screen.

The quality of the image produced on the screen is a function of two factors: the *refresh rate* (the speed at which the image is retraced on the screen) and the number of pixels (picture elements) on the screen. The more pixels on a given screen size, the higher the image quality.

As with cameras, this quantity is referred to as the display's *resolution,* and is often expressed in an X-by-Y format. Using this format, the quality of the image is still determined by how big the viewing area is (for example, an 800 □ 600 resolution on a 14-inch-wide display will produce much better quality than the same number of pixels spread across a 27-inch display).

CCTV monitors are available for black-and-white or color display, depending on the resolution and camera selection. Black-and-white monitors have resolutions in the range of 700 to 1,000 lines. Color monitors are available with 350 to 400 lines. They are designed for extended 24-hour operation.

Hands-On Exercises

In this exercise, you will learn how to secure the inner perimeter. The objectives include:

BUT FIRST

Before you can complete this exercise, you must complete the exercise in Chapter 2.

- For the ACME facility, define its inner perimeter and determine the vulnerabilities associated with that perimeter.
- For the specified perimeter and its vulnerabilities, perform research to determine what components or systems are available to secure the inner perimeter and what the cost options are for the components you find.
- Design a video surveillance and notification system that ACME can implement to secure this portion of their facility in the most cost-effective manner.
- Design an access-monitoring and control system for the inner perimeter of the facility.

The resources necessary for this exercise are as follows:

- Internet access
- Pencil/pen and paper
- Completion of the exercise in Chapter 2

Discussion

After the outer perimeter has been established and designed, the next step in a multilayer physical-security topology is to define the inner perimeter. Often, this involves monitoring the spaces between the outer and inner perimeters using video surveillance equipment. When properly designed and implemented, the surveillance system provides detection and notification capabilities that will cover specific passageways and key assets, as well as any areas requiring wide areas of view.

The other major component of securing the inner perimeter is to monitor and control its access points that lead to the interior. This process is similar to the one you performed in the previous procedure for the outer perimeter.

Procedure

1. Review Figure 3.13 and identify/label the inner perimeter of the warehouse facility. Hint: Do not include the showroom as part of the inner perimeter.

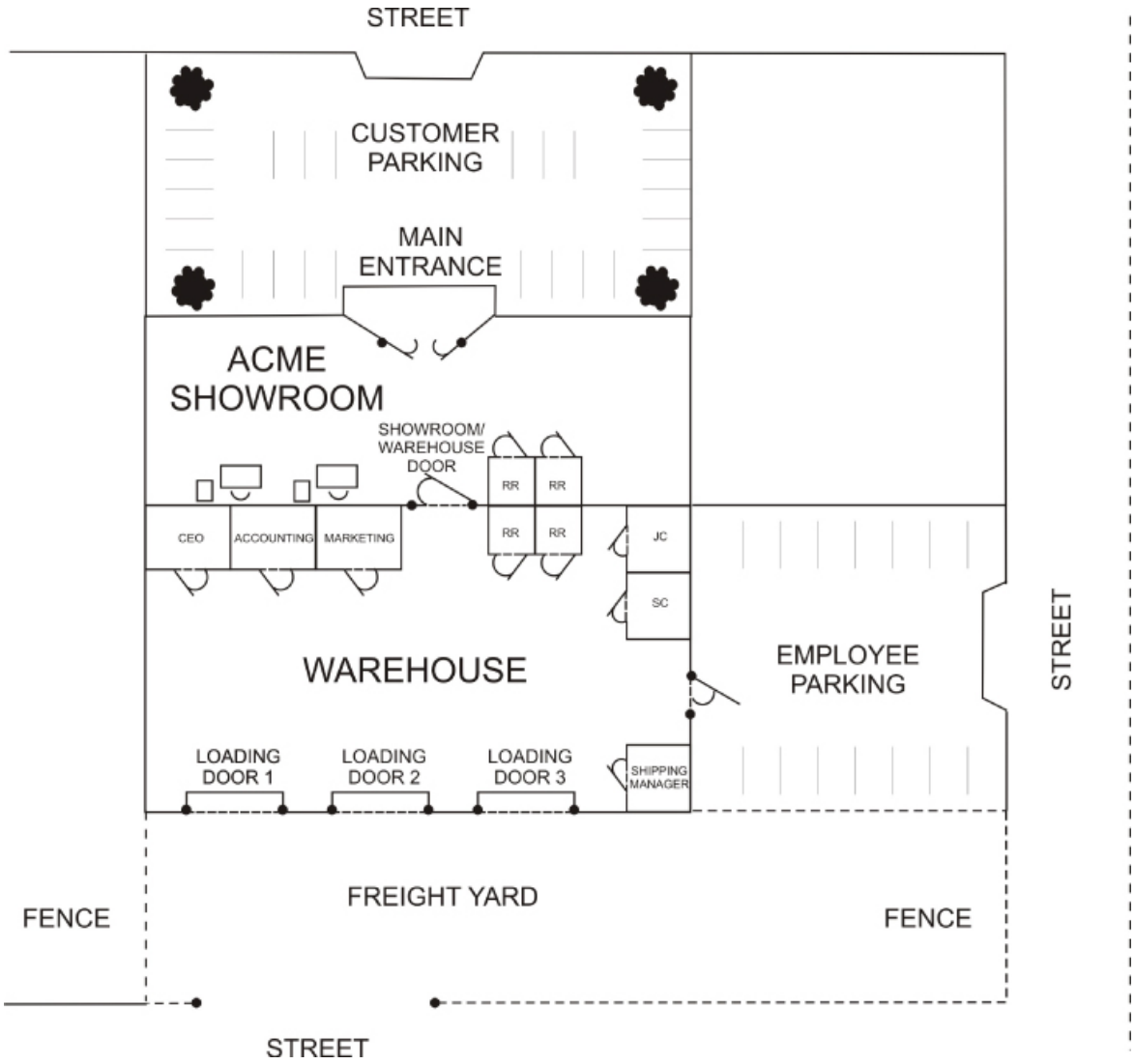


FIGURE 3.13 The Inner Perimeter

2. After examining the layout, identify at least two security areas between the outer and inner perimeters that would be suitable candidates for video surveillance. Highlight these areas on the drawing and record your reasons for selecting these areas on the following lines:

_____

_____

_____

_____

Answer: There are at least three areas: the loading bay doors into the warehouse, the pedestrian door into the warehouse from

outside, the pedestrian door between the showroom and warehouse, and any possible windows. These are all conventional means of entry and likely sources of intrusion.

3. Identify and mark the physical access points associated with the interior perimeter of the facility on the figure.
4. On the diagram, identify and mark the locations where surveillance cameras might be mounted for maximum effectiveness in monitoring these areas between perimeters.

Video Monitoring

1. Use the Internet to research video surveillance/monitoring devices and systems that can be used to effectively secure the *areas* and *access points* you identified in the previous section. Use Table 3.1 through Table 3.3 to organize the specified details about the video surveillance products listed there. For each item, try to locate at least two vendors.

TABLE 3.1 Video Cameras

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	360-Degree Panoramic Camera 20MP	Arecont Vision	3	$1,468.00	$4,004.00
B	Home Network Surveillance Dome 360 Degree	Digital Watchdog	3	$425.00	
C					

TABLE 3.2 Digital Video Recorders

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	4 CH DVR	TW Vision	1	$51.99	$51.99
B	4 CH DVR	Lorex	1	$89.99	$89.99
C	4 CH HD DVR	Samsung	1	$475.00	$475.00

TABLE 3.3 Additional Video Monitoring Software

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Android APP	Samsung	Dependent on number of authorized users	$0.00	$0.00
B	Apple APP	Samsung	Dependent on number of authorized users	$0.00	$0.00
C	Windows/Mac Browser	Native to operating system of workstation	Dependent on number of authorized users	$0.00	$0.00

Use caution when you're selecting cameras. Make certain to differentiate between camera types and the specifications that best fit the different locations you've noted.

2. List your selections for any video surveillance cameras you think should be recommended to ACME for controlling access to their inner perimeter.

Answer: Arecont Vision for the truck- loading- yard cameras.

Answer: Arecont Vision for the showroom cameras, also covers warehouse/showroom pedestrian door.

Answer: Arecont Vision for the inside warehouse space covering both the warehouse/outside pedestrian door and the loading bay doors.

3. Specify where you would deploy the cameras.

Answer: Centered inside warehouse to cover warehouse/outside man door, warehouse/showroom pedestrian door, and all three loading bay doors.

Answer: Central ceiling inside showroom to cover warehouse/showroom pedestrian door and for the showroom areas including the front, public entryway, and showroom floor.

Answer: Outside corner of building in truck yard to cover outside of loading bay doors and truck yard.

4. Specify the power and connectivity requirements for the different camera types you select.

Answer: Utilizing 360-degree indoor/outdoor cameras all with POE capability (Power over Ethernet), a powered switch will be required on the network hosting the DVR and cameras.

Answer: (Optional answer if student is using dissimilar cameras in their design.)

A WORD ABOUT COMPATIBILITY

Make certain the video recorder you select is compatible with the camera types you've already specified.

5. List the DVR that you would recommend to ACME for recording and storing the video surveillance data related to their inner perimeter.

Answer: The Samsung unit. It is compatible with IP cameras and its remote-access capabilities meet the desired specifications. This unit has a reasonably large hard-drive capacity for data storage, and it has the ability to use a USB device to burn video for evidentiary purposes.

BE AWARE OF ACME SPECIFICATIONS

Make certain the video monitoring software associated with the camera types and video recorder you've already specified meets the requirements laid out by the ACME specification. In particular, make certain that it will enable all of the ACME managers to access the current camera views as well as review past activities captured by the system.

6. List your recommendations for any video monitoring software you think should be recommended to ACME in addition to the native software offered by the DVR manufacturer.

Answer: For remote access via website or smartphone app, no additional software should be needed.

7. As part of your video surveillance research, investigate the local and remote notification capabilities associated with each surveillance system you list. Use the following lines to describe the capabilities of the system you would recommend to ACME.

Answer: Remote access via website or smartphone app. Record and playback. Camera-view auto sequencing. Capability to manage

and set permissions for multiple users/groups. Camera privacy settings. PTZ control. Tamper detection.

Inner Perimeter Access Controls

In addition to the surveillance system, you must also determine what types of access controls (if any) are required between the area inside the outer perimeter and the interior zone of the facility (the warehouse). The major access point between these two zones in the ACME warehouse is the showroom/warehouse door.

The movement of personnel between the showroom and the warehouse needs to be monitored and controlled. Only warehouse management personnel should be able to move freely between the two areas. Sales and customer service personnel should not be allowed in the warehouse area.

1. Use the Internet to research access control devices and systems that can be used to secure the access points you've associated with the inner perimeter. Use Table 3.4 through Table 3.6 to organize the specified details about the intrusion-detection products listed there. For each item, try to locate at least two vendors.

TABLE 3.4 Authentication/Access-Control Devices and Systems

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Electronic Keyless Door Lock	Gino Development	1	$89.99	$89.99
B	Mag Door Lock Kit	Entry Vision	1	$274.99	$274.99
C	Cobra Controls Lock Kit	Maglocks.com	1	$1,699.99	$1,699.99

TABLE 3.5 Door Contacts/Sensors

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Door Sensor Wired	SensaPhone	7	$9.00	$54.00
B	Gate & Com. Door Sensor	Gogogate	7	$35.00	$210.00
C	SDC MC-4	Grainger Industrial	7	$53.95	$377.65

TABLE 3.6 Door Locks

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Jackshaft	LiftMaster	3	$273.39	$820.17
B	Electronic Keyless Door Lock	Gino Development	1	$89.99	$89.99
C	Mag Door Lock Kit	Entry Vision	1	$274.99	$274.99

2. What authentication devices/systems would you recommend to ACME to control access through their inner perimeter?

_____

Answer: An RFID pass card to enter through the pedestrian door to the warehouse from outside. The Mag Door Lock Kit has this feature integrated as part of its design. The Electronic Keyless Door Lock to be applied to the pedestrian door between the warehouse and the showroom can be actuated without any authentication steps from inside the warehouse, but it requires a key or passcode to operate the door from inside the showroom.

3. Specify where you would employ the authentication devices/systems.

_____

Answer: Authentication devices should be at both inner-perimeter pedestrian doors; they should require different levels of authentication for the different departmental levels of employees.

4. List your selections for the door sensor you would recommend to ACME for their inner-perimeter access points.

Answer: Gogogate Magnetic contact sensors for the pedestrian doors and roll-up loading-bay doors.

Answer: (An optional secondary sensor package if using dissimilar sensors for roll-up doors or pedestrian doors.)

5. List the door locks you would recommend to ACME for their inner-perimeter access points.

Answer: The Electronic Keyless Door Lock to be applied to the pedestrian door between the warehouse and showroom. It can be actuated without any authentication steps from inside the warehouse, but a key or passcode is needed to operate the door from inside of showroom.

Answer: The Jackshaft LiftMaster for the three roll-up doors. The devices will keep the doors secure in a fail-safe design unless manually disengaged from inside the warehouse.

Answer: An RFID pass card to enter through the pedestrian door to the warehouse from outside. The Mag Door Lock Kit already has this feature integrated as part of its design.

Review Questions

1. **Which two areas of the ACME facility are good candidates for video monitoring?**

   Answer: The loading yard and the showroom. The loading yard provides direct access to the warehouse through the three roll-up

doors, while the showroom provides direct inside access to the showroom/warehouse pedestrian door.

2. **Which access points are associated with the inner perimeter of the facility?**

   Answer: The three loading dock doors and the showroom/warehouse door.

3. **Which type of camera is best suited for monitoring the area inside the fence of the truck loading yard and the gate at the driveway entrance?**

   Answer: Any outdoor-rated camera with an adequate zoom/focus/frame rate that is compatible with the surveillance system desired by the client.

4. **Which type of camera is best suited for monitoring the showroom and the pedestrian door that leads to the warehouse?**

   Answer: Any indoor-rated camera with an adequate zoom/focus/frame rate that is compatible with the surveillance system desired by the client.

5. **ACME wants to include a hardware device that will enable all the members of their management staff to simultaneously display the output from the video cameras on the PCs located at their desks. Which type of hardware should you install to provide this level of functionality?**

   Answer: A DVR that offers network access and a web interface for remote access.

CHAPTER 4
Understanding Intrusion-Detection and Reporting Systems

While preventing unauthorized access is the first line of defense in physical security, layers of additional security measures are crucial to preventing intrusions from escalating into serious events. A closely related second tier of defense is intrusion detection, which enables potential intruders to be detected and removed before they can cause problems. This level of security involves detection devices that are monitored or that can create an alarm. In this chapter, you'll learn to:

- **Describe components of a typical, physical intrusion-detection and reporting system**
- **Explain the purpose for creating physical security zones and common techniques for defining them**
- **Identify common sensor types employed in a physical intrusion-detection system**.

Intrusion-Detection and Reporting Systems

The components of a basic commercial security system, as depicted in Figure 4.1, come together to provide a functional intrusion-detection and reporting system. This system includes an intelligent control panel connected by wires (or radio signals) to sensors at various locations throughout the facility.

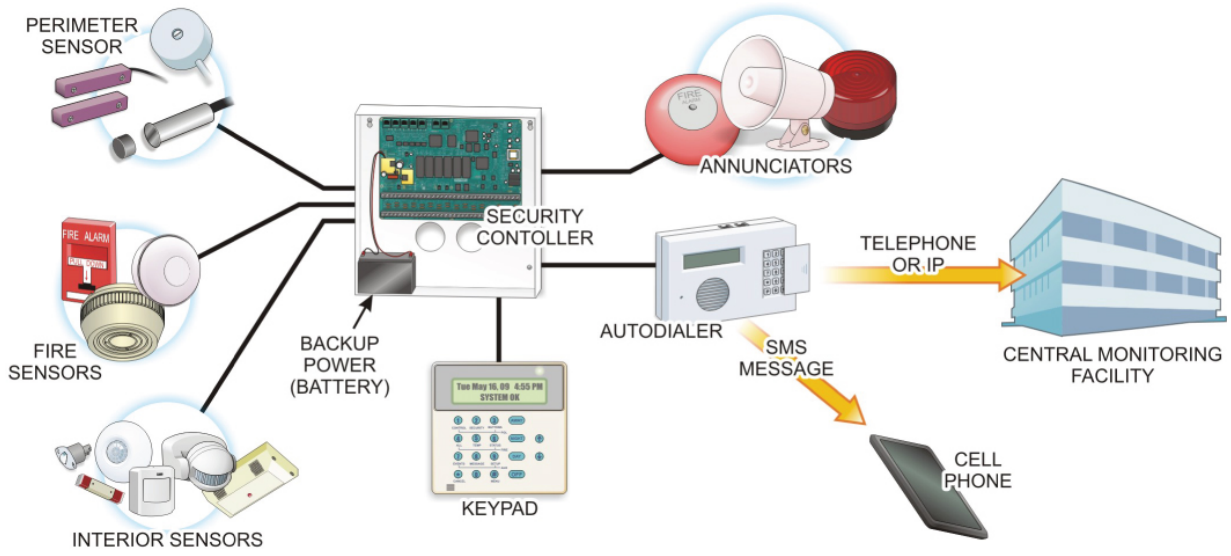


FIGURE 4.1 Basic Intrusion-Detection and Reporting System

The control panel includes the electronic components and central processor, which monitors and controls the entire system. The processor accepts input information from the various sensors attached to it. In a basic security system, these inputs can be divided into three distinct types: perimeter, interior, and fire.

Perimeter area inputs to the control panel typically include sensors at every perimeter opening including doors, windows, garage doors and windows, and doors to crawl spaces. Additional perimeter protection may include using sound, vibration, and motion-detector sensors to guard against entry through broken windows.

Some interior areas may also be protected with various types of sensors, such as motion detectors and interior door sensors. Most security systems also include inputs capable of handling adequate smoke and fire sensors.

When the controller receives an active input signal from one of its input sensors, it evaluates the conditions presented according to its programming (and the type of emergency response required), and if necessary, sends the appropriate output signals to annunciators (sirens or bells). It may also communicate with designated security

contacts (security supervisors, monitoring services, or law enforcement/fire agencies) as directed by its programming.

Commercial security systems may use any of several notification methods to notify designated security personnel when an alarm condition is triggered. Some alarm systems use a telephone dialer to alert the remote security contacts that an alarm condition exists. These systems are designed to react when no one is present by placing the call over a standard telephone line or cell phone. Special digital codes are used to inform the security contacts as to what type of condition caused the alarm.

It is also possible to have a prepared text-messaging system, such as SMS, relayed by a cell phone to the designated security contacts. Another option is IP-based notification, which is used to notify the monitoring station via an IP network, such as the Internet, concerning an alarm condition.

Most security systems typically employ some type of keypad to provide the control interface for supervisors to arm and disarm the system using a programmed access code. The keypad may be designed to provide some level of visual and audible output signals to help monitor the status of the system.

Finally, most security systems include some type of emergency backup power (a backup battery or uninterruptable power supply) to provide emergency power to the security system when commercial power outages occur.

The choices for access-control and management system components and subsystems are extensive. The following sections of this chapter will explain the various subsystems typically found in the intrusion-detection and reporting portion of a typical infrastructure security system.

Security Controllers

The center of any intelligent security system is the *controller*. The security controller, shown in Figure 4.2, is typically installed in an

enclosure that contains the security controller board, all of the electronic components, wire termination points, backup battery packs, and telephone termination wiring.

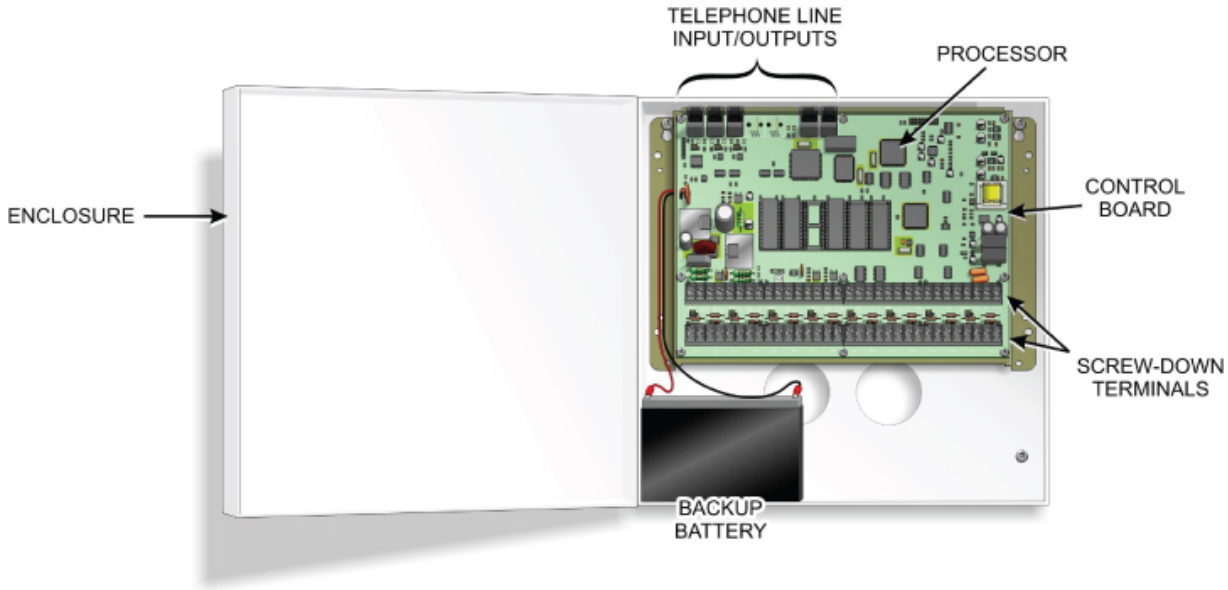


FIGURE 4.2 Control Box with Panel and Battery

A given security controller model will be designed to handle a specific number of programmable zones. A *zone* can be a single point of protection such as a motion detector, or multiple points can be combined into a single zone. For example, two hallway motion detectors could be connected to form a zone, or a stairway motion detector could be combined with the hallway sensors to form a single zone.

The security controller is the command center and distribution point of the intrusion-detection and reporting portion of the security system to which all input and output devices are connected. Each sensor receives power and is managed from the security controller.

The controller must have enough capacity and functionality to connect to and manage all the security devices that will be part of the security system, in addition to providing remote access capability for remote monitoring and control.

The controller's enclosure should be mounted out of plain view and near a 120-volt AC outlet, where a plug-in transformer can supply

low-voltage power to the total system.

Security Zones

As mentioned earlier, security controllers possess a fixed number of detection circuits that can be used to create physical security zones. For instance, a typical, commercial security controller may possess as few as eight zones and up to 250 zones or more. Typically, one of these inputs is dedicated to the fire detection system. Figure 4.3 shows a typical eight-zone security controller connection scheme.

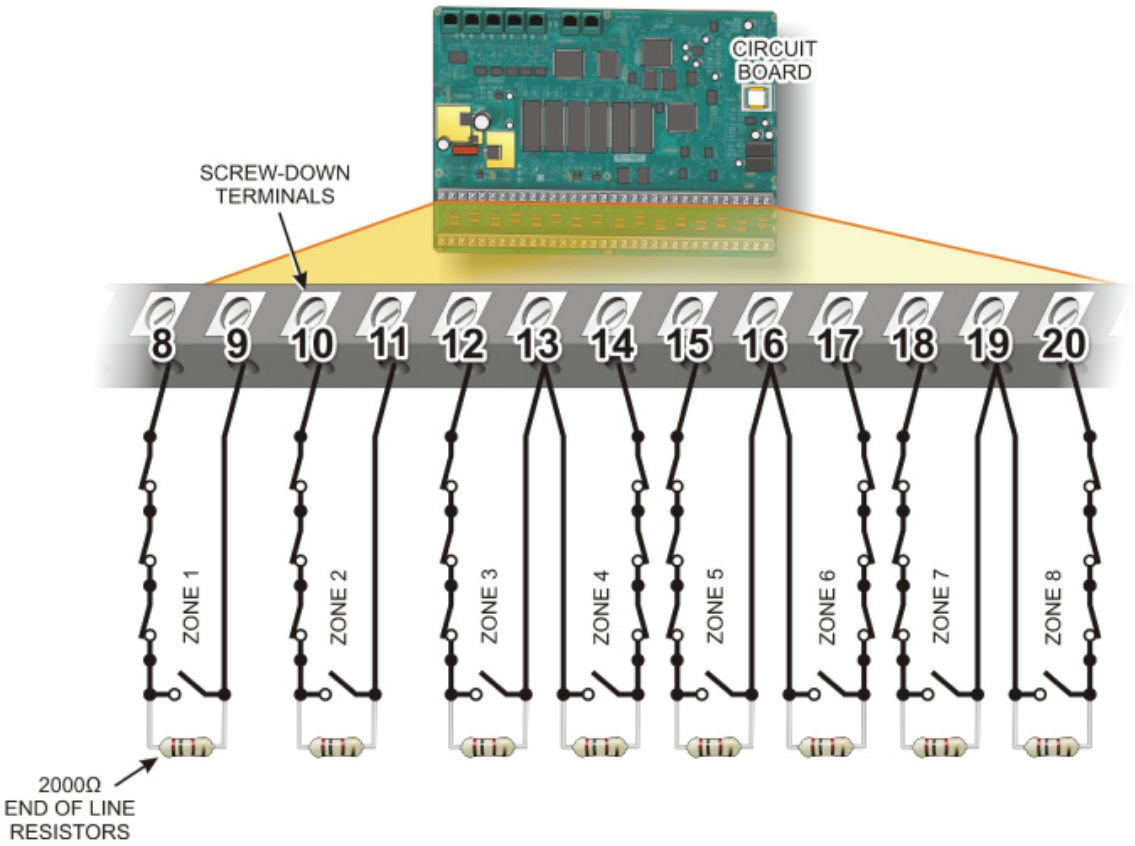


FIGURE 4.3 Security Panel Zone Inputs

Suppose that the facility in which you are installing the security system has fourteen windows, two personnel entrance doors, and a roll-up receiving door for the warehouse. In addition, it has two major hallways to monitor and an integrated fire-detection system.

How should you physically install and configure the controller so that it provides full protection for the facility? The answer is to

logically group related sensors together to create a security zone. This is accomplished by connecting all of the related sensor switches (all sensors appear as switches to the security controller) together in a serial format as illustrated in Figure 4.4.

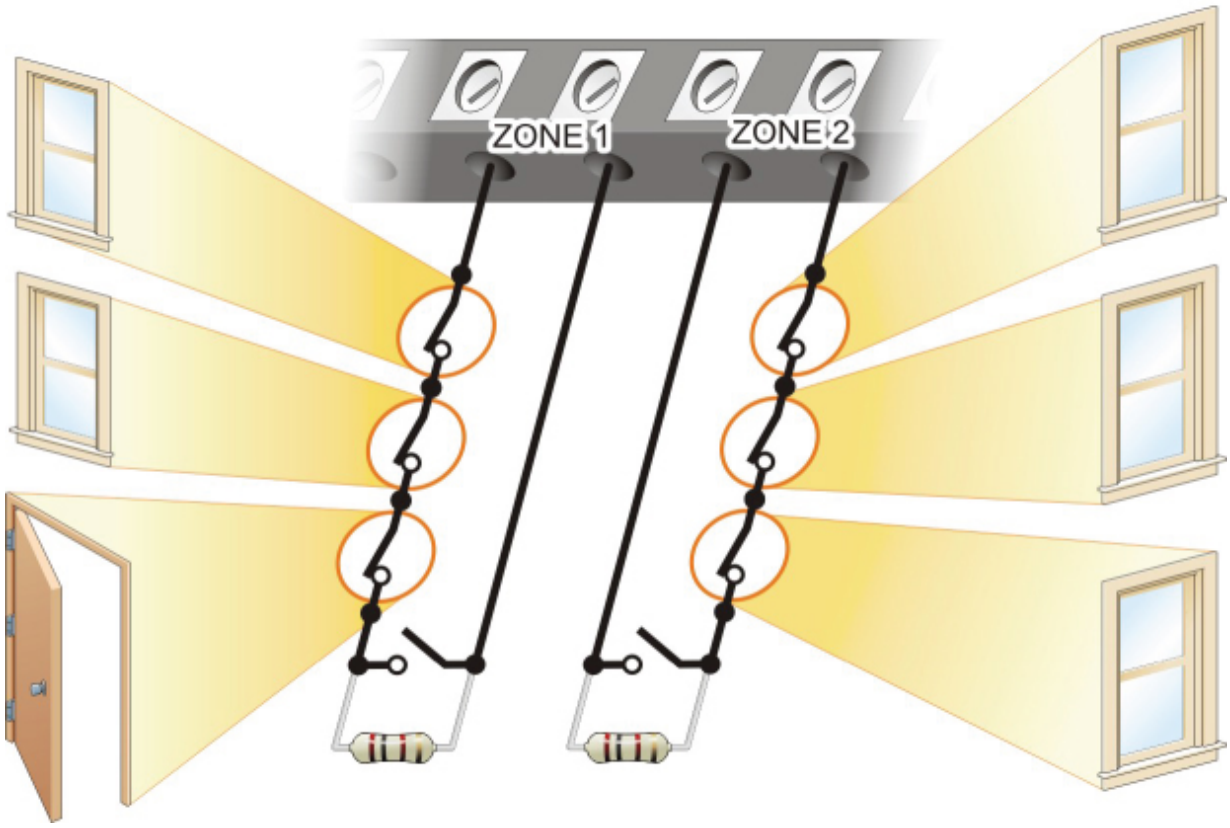


FIGURE 4.4 Creating a Physical Zone

The controller monitors the amount of electrical current flowing between the zone's two connection points (referred to as a *current loop*). The loop requires that a resistor be placed within the loop to regulate the current flow to the correct level for the controller being used (different controller models typically require different resistance levels).

If one of the sensors is activated, its switch moves into an open condition and current flow through the loop stops. The controller detects the lack of current flow and processes the input according to its configuration programming.

The fact that a certain level of current must be flowing helps to make tampering with the loop more difficult. If the system used normally opens switches that close when activated, the system could be circumvented by simply cutting a wire in the loop; no signal would ever be presented to the controller.

For the sample installation presented earlier, it might be logical to wire all of the west-side window sensors into one input that could be reported as the West Side Windows. Likewise, the two personnel entry doors can be configured together because they will require special settings to allow exit and entry times for setting and disarming the system when leaving or entering the structure. Conversely, the other door may be connected into a different door zone or incorporated into one of the window zones since it has no timing requirement.

Zoning also enables the system to instantly sound an alarm for intrusion detection in a specific area, while other sensor alerts in a specific zone (such as the main front door) may require a short delay before sounding the alarm. This enables security personnel to arm the system by entering a secret code on a keypad when exiting the facility (exit delay).

It also allows them to enter a protected area when arriving at the facility and disarm the system through the entry area keypad within a specified entry-delay interval (usually 30 to 45 seconds). This feature allows keypads to be installed inside the facility near the exit door to avoid vandalism and tampering with keypads from the outside area.

Interior motion sensors that guard the hallways may be integrated into a window or a door zone. However, they are more likely to be configured separate from the exterior sensors so that they can be disabled at night when people may need to move around during the night but want the perimeter to be protected from outside intruders. Figure 4.5 describes a possible zoning solution for this example.

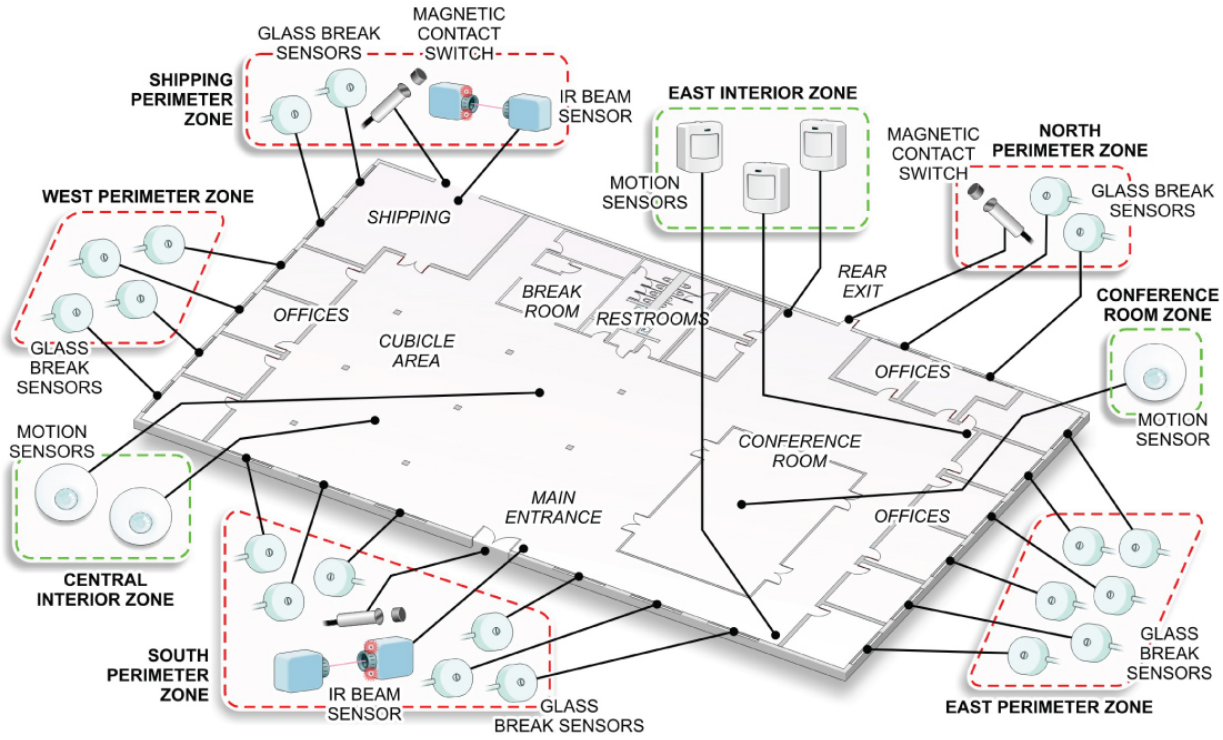


FIGURE 4.5 Zoning Concepts

The use of zoning also enables security personnel to arm only portions of the system, such as the perimeter doors and windows, while bypassing interior motion detectors in a specific zone. A bypass mode setting is normally accomplished by entering a predetermined numerical code through the keypad. When personnel leave the facility, all zones including the interior detectors can be armed as required.

A zoned security-system layout can also be used by an external monitoring service to know which sensor in a designated zone is causing an alarm. If a sensor is reported as just Sensor 3, Zone 5, this could mean that the event occurred just about anywhere. If the sensor was reported as Sensor 3, Zone 5 perimeter, this would inform the operator that the violated area is on the outside of the premises.

Zones also provide ease of troubleshooting. For example, if a sensor in the Zone 3 perimeter is reporting a problem, there is no need to troubleshoot sensors that are located in the interior of the system.

Sensors

Sensors are a class of input devices that convert physical activity into a signal that can be presented to the security controller. They are available in a variety of configurations including magnetic switches for doors and windows, acoustic detectors, vibration detectors, motion detectors, and glass-break detectors. Sensors protect the perimeter, selected outside areas, and the open spaces inside the facility.

As mentioned earlier, perimeter devices primarily protect doors and windows. The most common perimeter sensors are magnetic door switches, window vibration, and window acoustical detectors to detect breaking-glass sounds.

Open-space-protection sensors called *motion detectors* cover interior rooms and hallways. Outside motion detectors activate security lights when movement is detected. Indoor motion detectors can detect an intruder who has been able to defeat a perimeter device. Exterior motion detectors and motion-activated security lights are also used. The following paragraphs describe the sensors included in basic security and surveillance systems.

Magnetic Contact Switches

Magnetic contact switches basically consist of a two-part magnetic switch. One piece of the sensor is a magnet, while the other side is a switching mechanism, called a *reed switch,* that is sensitive to a magnetic field. The switch portion is mounted on the fixed structure (frame) of the barrier, as shown in Figure 4.6. Wires from the switch are routed to the security system's control panel.

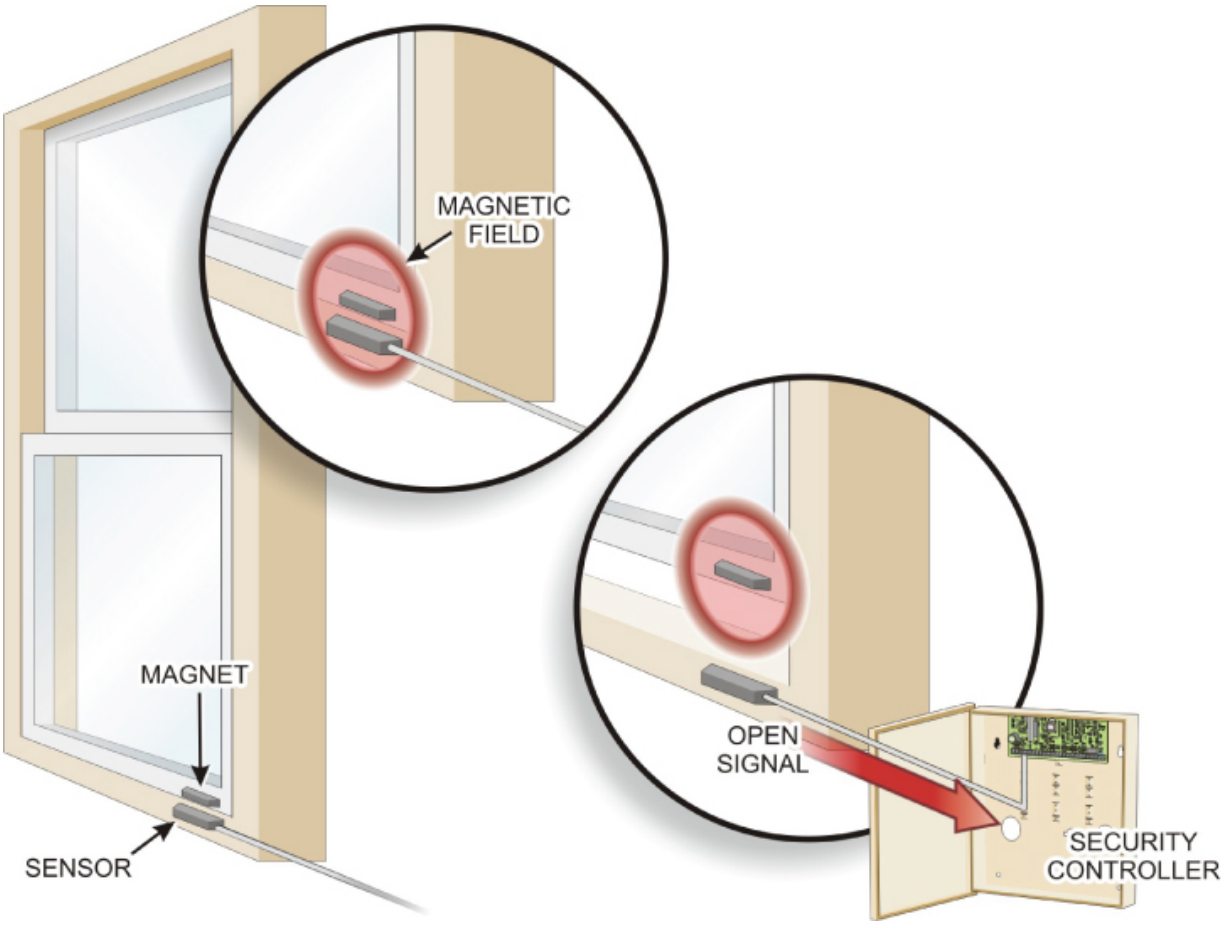


FIGURE 4.6 Sensor Mounting

The magnet portion of the sensor is mounted on the movable barrier so that it is in close proximity to the switch when the barrier is closed. This also keeps the switch closed. Opening the barrier moves the magnet away from the switch and opens the switch, which is sensed by the central control panel, and activates an alarm.

This simple magnetic-switch sensor can be used to protect doors and windows or any other moving barrier. It alerts security managers when someone attempts to gain entry through a passageway through illegal or unauthorized means. Its magnet and reed-switch mechanism detects any intrusion and signals an alarm.

This type of sensor can be used to indicate the open/closed condition of a movable barrier, but it cannot determine whether the barrier's locking mechanism is locked or unlocked. As mentioned earlier, some types of electrically operated door locks are equipped with

sensors for determining whether the locking mechanism is locked or unlocked.

Even though up to 70 varieties of barrier sensors are available, a sensor alone cannot offer true control other than detection and warning. Its signal, however, can be used by other access-control system components to provide automated responses.

Glass-Breakage Sensors

As mentioned earlier, a perimeter security system may include a glass-breakage detection system. Magnetic switches do not protect against an intruder entering through a broken window. Two types of glass-breakage detection systems are available. The vibration type is mounted on the glass or on a nearby wall. Acoustical or sound discriminators sense the sound of breaking glass.

The unit may be tuned to react only to the specific frequency of glass breaking, typically 4 to 6 kHz, or to any loud noise. Some sensor manufacturers have combined vibration and sound detectors into one unit that will not activate unless both are detected. These units may be used where the normal conditions would cause a single technology detector to generate false alarms.

Vibration detectors are mounted on the glass, and the acoustical window sensors are normally mounted on an adjacent wall, as illustrated in Figure 4.7.

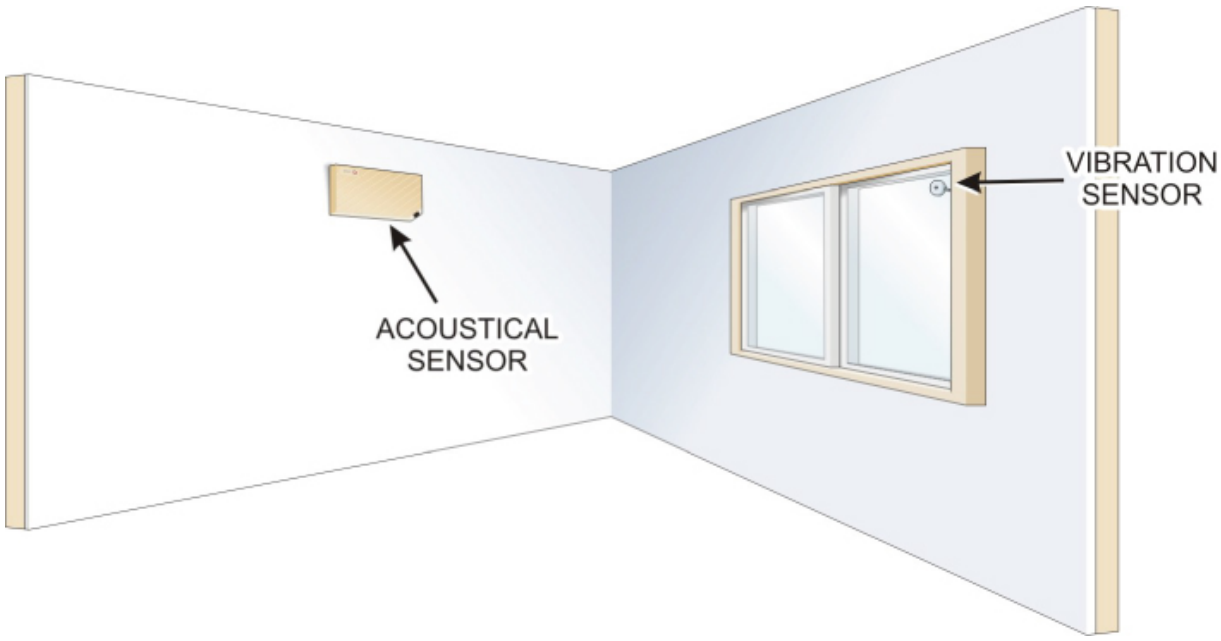


FIGURE 4.7 Glass-Breakage Sensors

Motion Detectors

Motion detectors work by detecting the changes in the infrared energy in an area. Because these devices do not emit any energy, they are called *passive infrared (PIR) detectors*.

PIR detectors use a lens mechanism in the sensor housing to detect any change in infrared energy across the horizontal sectors covered by the sensor. This type of detector is insensitive to stationary objects but reacts to rapid changes that occur laterally across the field of view. PIR detectors are the most common and economical type of motion detectors.

Motion detectors should be installed in open areas that cannot be protected by window or door sensors. An example of a PIR motion detector for interior use is shown in Figure 4.8.

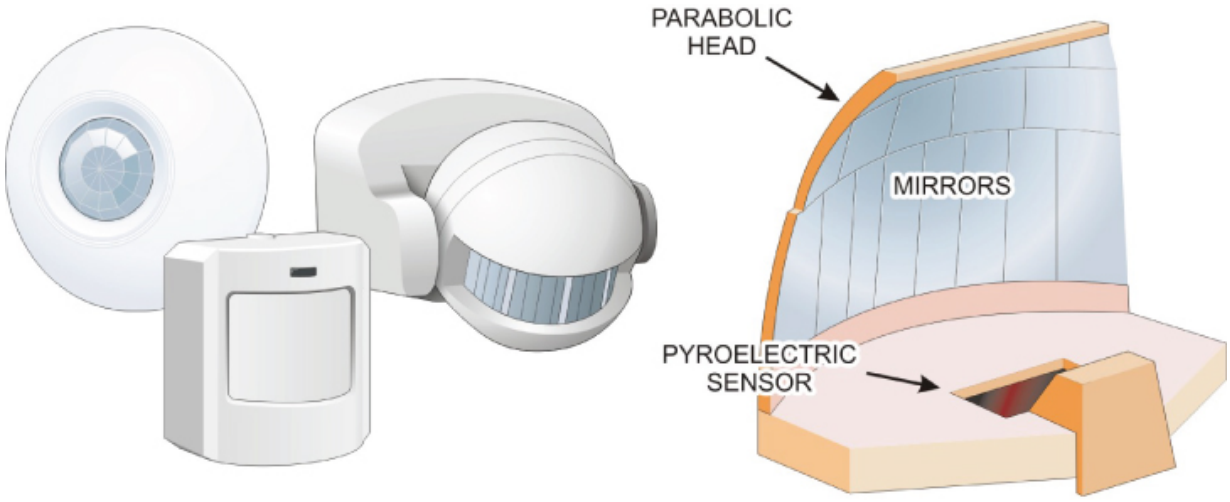


FIGURE 4.8 A PIR Motion Detector

Motion Detector Locations

Motion detectors are normally mounted in the corner of a room. This allows the detector to cover a 90-degree field, as illustrated in Figure 4.9. Motion detectors are sensitive to movement across the sensor's field of view.

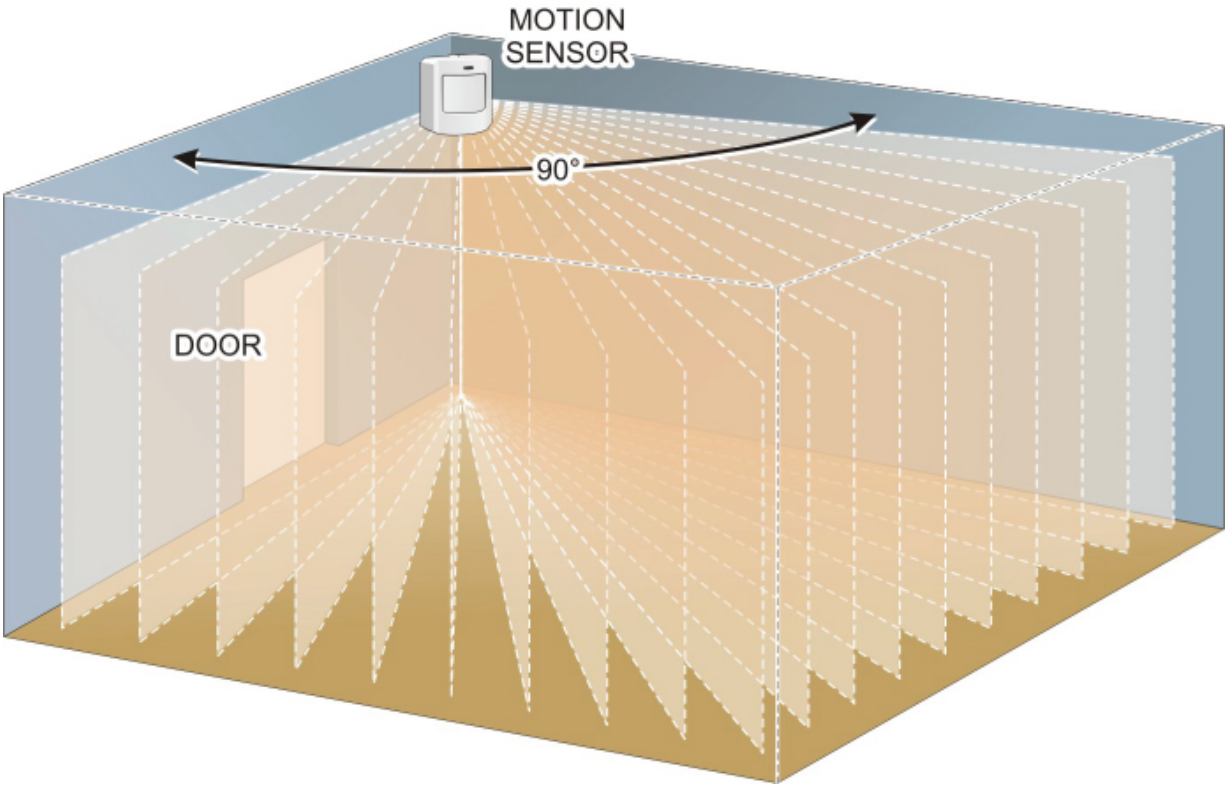


FIGURE 4.9 PIR Field of View

Exterior lighting is often used to illuminate dark areas or areas to be protected using motion-detection sensors that activate security lighting to deter an intruder. Outside lighting is used solely as a deterrent and safety feature, so it is not normally connected to the security controller.

Dark areas surrounding the facility with trees or shrubs need to be illuminated with security lighting systems. Security lighting systems used during dark hours prevent intruders from entering the area surrounding a facility and attempting entry under the cover of darkness. Motion-detector-activated lights are also popular for exterior lighting.

Vehicle-Detection Sensors

Several methods are used to detect the presence of an automobile entering an area near a facility. The most common type of sensor used for this purpose is a motion detector placed above the entrance

to the garage. Pressure sensors can also be employed to detect a vehicle on a driveway or garage area.

Photoelectric Beam Devices A photoelectric sensor is an optical control that detects a visible or invisible beam of light and responds to a change in the received light intensity. Photoelectric beam devices use this feature by having a narrow beam of light aimed through an area of interest such as a parking lot gate, as shown in Figure 4.10. When the light beam is interrupted, the photoelectric device is used to sound an alarm, or in the case of garage door safety system, to stop or reverse an automatic garage door's lifter motor.

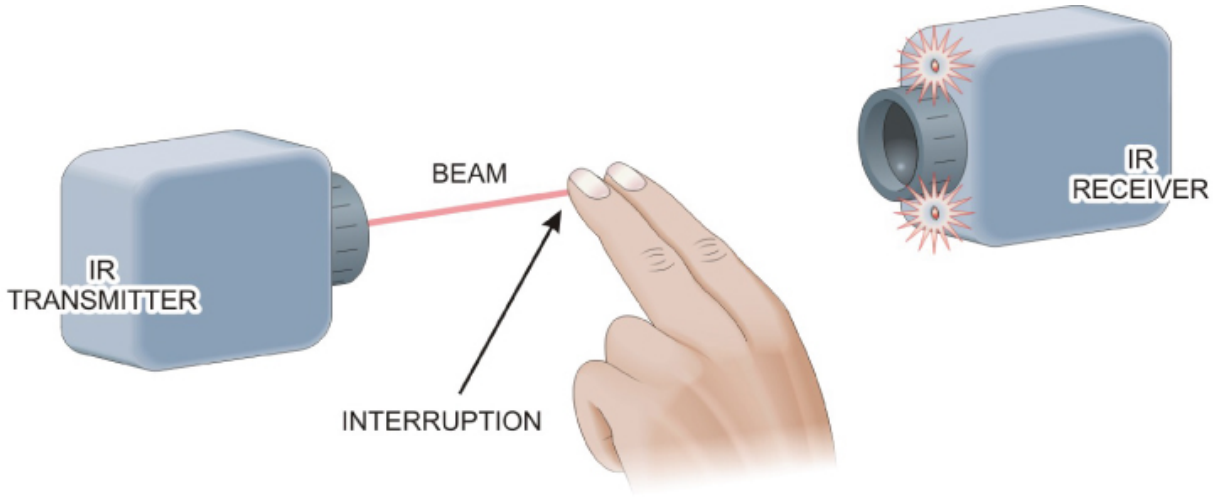


FIGURE 4.10 Photoelectric Beam System

Microwave Beam Devices This device emits microwaves from a transmitter and detects microwaves at a receiver, either through reflection or reduction in beam intensity. The transmitter and receiver are usually combined inside a single housing for indoor applications and separate housings for outdoor applications. By generating energy in the microwave region of the electromagnetic spectrum, the detector operates as an active device that responds to:

- A Doppler shift frequency change. These devices are based on the Doppler Effect phenomenon, which observes frequency changes in energy waves (in this case, microwaves) in motion relative to a

listener or receiver. These detectors emit microwaves of a specific frequency into a given environment and then analyze the frequencies of any waves reflected to it. Changes from its normal frequency reception cause the sensor to signal an alarm condition.

- A frequency phase shift. These devices also rely on changes in reflected energy waves caused by motion. Like the Doppler sensors, these sensors emit specific microwave frequencies into an area and measure phase shift of reflected waves, which are directly proportional to the velocity of the moving object.
- A motion causing reduction in received energy. These devices respond to changes in the level of energy between a transmitter and a receiver caused by some or all of the transmitted energy wave being blocked by an obstacle moving into its path.

Pressure Sensors Pressure mats are a type of sensor that can be placed under rugs in hallways or on stair treads. They react and alarm due to pressure from footsteps activating the alarm. Pressure sensors typically use normally open switch contacts. When pressure is applied to the pressure mat, the switch closes, which alerts the control panel that the pressure switch has been activated.

Keypads

Most intrusion-detection and reporting systems employ a keypad device for programming, controlling, and operating various access-control and management devices.

Keypads are input devices that are typically equipped with a set of numerical pushbuttons that are similar to a telephone touchtone keypad, as illustrated in Figure 4.11. Security personnel typically use keypads to initiate commands for control options such as arming and disarming the system or bypassing a zone.

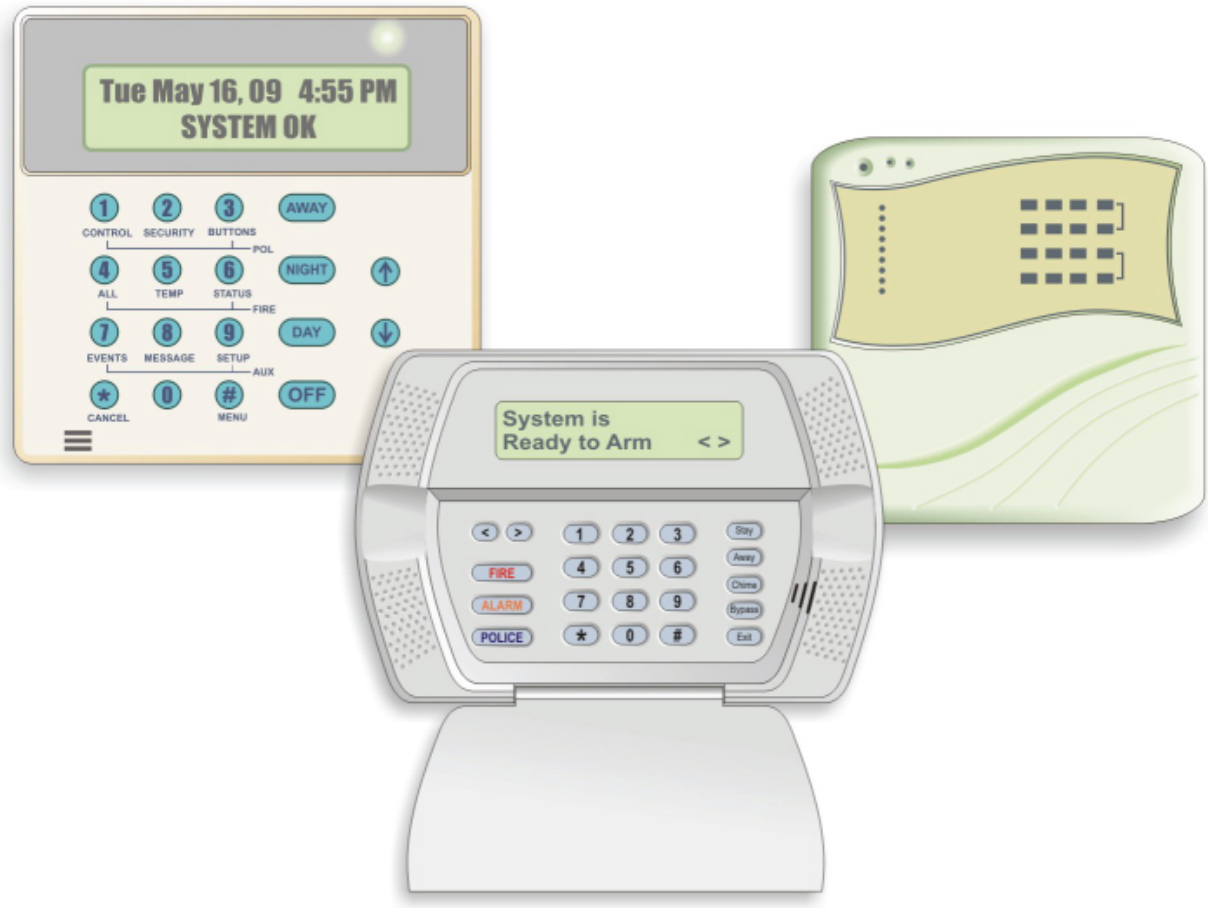


FIGURE 4.11 Controller Keypad

Keypads can be located in any area of a facility that is convenient for security personnel to operate external gates and doors. However, many new security systems typically include software that runs on a tablet computer or a smart phone app to perform these functions from anywhere.

Key Fobs and Panic Buttons

A key fob is a wireless keychain device similar to the type used to lock, unlock, and alarm a vehicle. Convenient and easy-to-use remote-entry key fobs enable security personnel to arm and disarm a security system with a push of a button when outside the facility. The key fob often features a panic button function that allows the user to contact help in case of emergency. An example of a key fob is shown in Figure 4.12.

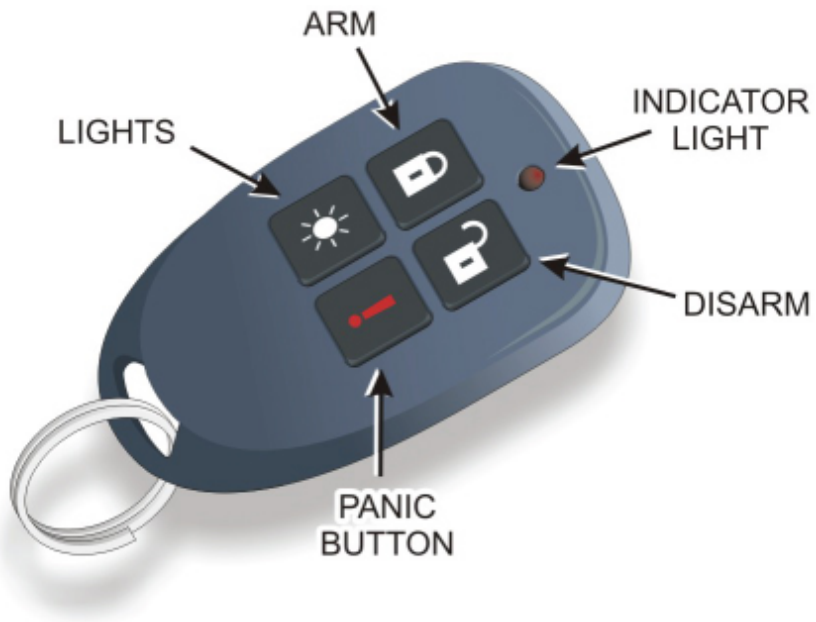


FIGURE 4.12 Security Key Fob

Panic buttons are devices that allow immediate triggering of an alarm system when facing an emergency situation such as the discovery of an intruder. As indicated in the previous paragraph, panic buttons are often integrated with a key fob but may also be mounted permanently at key locations inside the facility.

Fire-Detection Sensors

Many intrusion-detection and reporting systems include a fire-detection and alarm function as an integral part of the system. However, for larger or more complex security systems, standalone fire-detection and reporting systems may be used.

Two common types of fire-detection sensors are available: heat sensors and smoke detectors. They operate by detecting heat rise or the presence of smoke particles in the facility.

Heat sensors operate using a different technology than smoke detectors. The basic design features of each type are summarized in the following paragraphs. *Heat sensors* detect a rapid rise in temperature. They also set off an alarm when a fixed temperature is reached. On the other hand, smoke detectors, such as the one shown

in Figure 4.13, do not react to heat but use one of two common sensor designs to detect smoke.

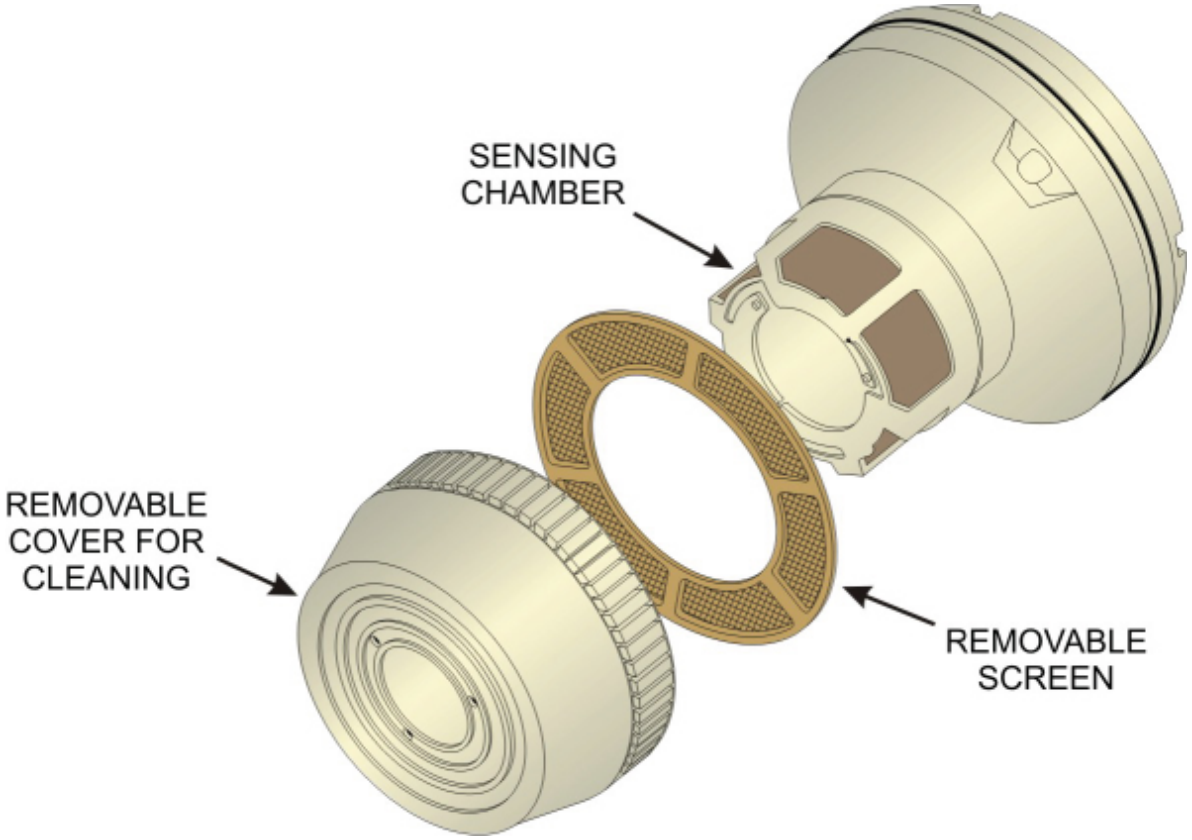


FIGURE 4.13 A Typical Smoke Detector

Ionization detectors form an electrical path inside a small chamber with a very small amount of radioactive material. When smoke enters the chamber, the particles attach themselves to the ions and change the electrical current.

Photoelectric detectors work by using a photoelectric cell and a light source. Normally, the light does not reach the photoelectric cell; but when smoke is present, the light is dispersed, and the detector triggers an alarm signal.

The main difference between the two detector types is that photoelectric types are more sensitive to large particles and ionization types are more sensitive to small particles.

Carbon Dioxide and Carbon Monoxide Detectors

Carbon dioxide (CO_2), a natural byproduct of normal respiration, is different from the toxic carbon monoxide (CO) gas—and much less dangerous. Outdoor air usually contains about 400 ppm (parts per million) of carbon dioxide, while carbon monoxide levels should normally be less than 0.2 ppm.

Although CO is a colorless and odorless compound produced by incomplete combustion, it is lethal at high levels. When dangerous levels of CO are detected, the detector sounds an alarm, giving people in the area an opportunity to safely leave the residence—or to apply immediate ventilation.

Carbon monoxide is generated through the incomplete burning of natural gas, kerosene, fuel oil, coal, or gasoline, and not by appliances that use only electricity. If the furnace, water heater, space heater, stove, or oven does not burn gas or fuel, it will not generate carbon monoxide. Accurate carbon monoxide data require that suspect appliances be operating before any readings are taken.

When a CO alarm activates, personnel need to call emergency services, the fire department, or 911. They must immediately move to a source of fresh air, either outdoors or by an open door or window. A head check should be taken to ensure that all personnel are accounted for. No one should return into the facility or move away from the fresh air source until the emergency services arrive and give the all clear.

Output Devices

Physical intrusion-detection systems typically include three basic types of output devices: visual notification, audible annunciators, and remote messaging. The visual and audible annunciators provide a local and general call for attention to a predefined alarm condition, while the remote messaging element is employed to notify specific personnel or organizations that an alarm condition exists. The following sections describe the various output signals and devices employed in a basic security system.

Sirens

The control panel provides the voltage for driving the external electronic siren or strobe light. The controller activates these devices when an alarm condition exists. Various types of audible annunciators (sirens, horns, buzzers, klaxons, and bells) are used to attract attention when an alarm condition is activated.

These different devices produce different levels of volume for use in various locations. Audible alarm sounders are used not only to attract the attention of others outside the facility or away from the area of the intrusion, but also to create a sufficiently high level of sound to discourage an intruder. Commercial security systems typically employ solid-state electronic sirens like the one shown in Figure 4.14. These sirens provide a higher level of sound output as well as a variety of tones and pitches.

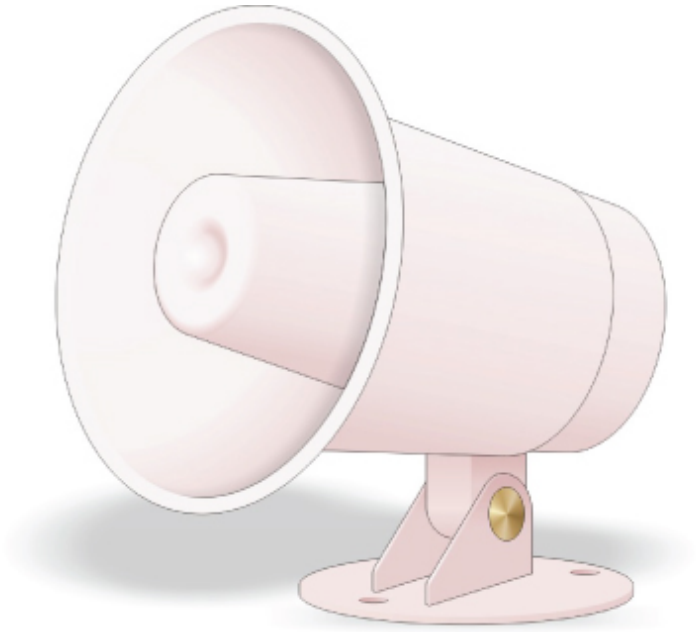


FIGURE 4.14 Electronic Siren

Interior sounders installed in concealed areas within the facility are designed to operate at maximum sound levels to frighten an intruder into making a fast exit. This is because the sound masks any outside approaching police siren. Interior sirens are available from several

vendors that operate at sound levels in the 110 to 120 dB range, which is near the threshold of pain.

Strobe Lights

Many security system installations include at least one strobe light to provide a visual indicator. These lights are typically mounted on the outside of the facility to attract attention of people in the vicinity of the intrusion and to discourage would-be intruders. Security strobe lights operate from various DC voltage levels provided by the security controller panel.

Security strobe lights, like the one depicted in Figure 4.15, produce light output levels specified in either foot-candles, or *candelas,* of light. A foot-candle is a measure of *luminance* (or light intensity) used by the lighting industry. Likewise, one candela is equal to foot-candles multiplied by distance squared:

$$C = fc \times d^2$$

FIGURE 4.15 Strobe Light

Security strobe lights are available in a number of different colors including red, blue, amber, and clear.

Remote Notification Systems

While strobe lights and sirens call general attention to alarm conditions in a localized environment, it is often necessary to notify specific people (such as a security specialist) or organizations (such as third-party security companies, fire departments, or police services) to respond to different types of alarm conditions.

The most common remote notification systems involve the use of a telephone line by the security-system control panel to automatically call a remote monitoring facility or key personnel when an alarm condition exists. When the security controller receives an active input signal from one of its zones, it activates the telephone dialer unit and causes a digital data message to be transmitted to a predetermined recipient. The message recipient can also use remote access to check on the status of the security system when away from the facility.

Some intrusion-detection and reporting systems employ a separate telephone dialer like the one depicted in Figure 4.16, or a built-in dialer. However, a growing number of systems utilize built-in cellular communications systems. Such systems provide additional dependability in that they can function even if the physical telephone lines are damaged.

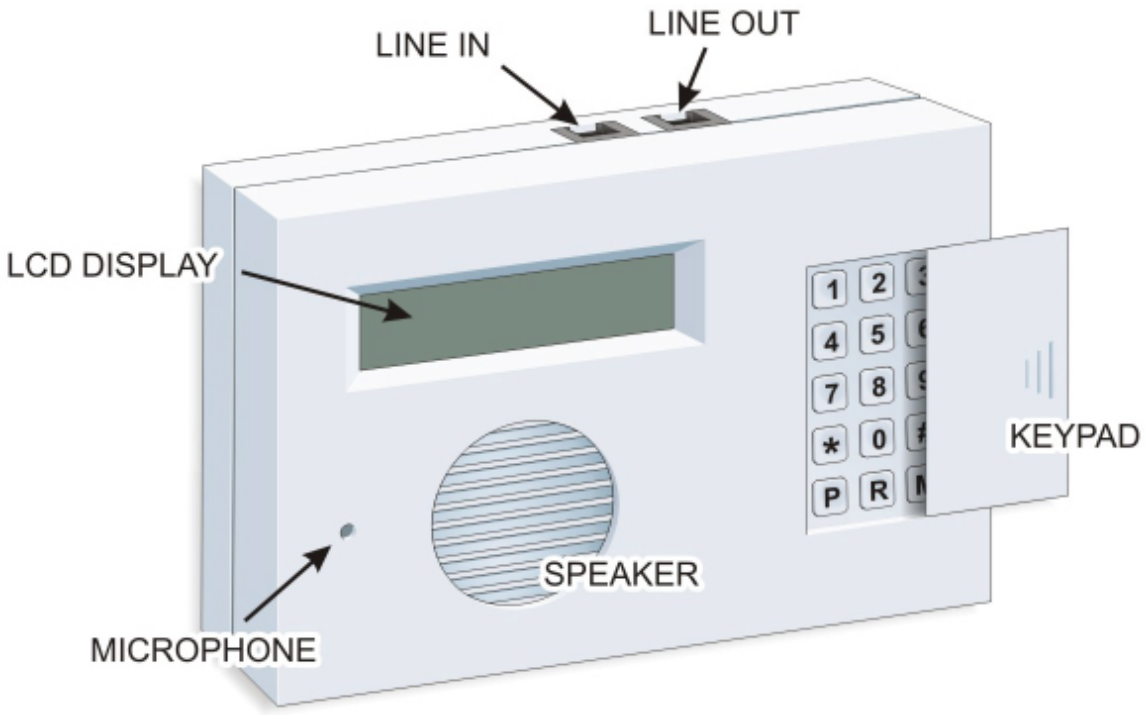


FIGURE 4.16 Automatic Voice/Pager Dialer Console

Third-Party Alarm-Monitoring Services

Depending on the nature of the organization, the intrusion-detection and reporting system may be totally based on employees of the organization. However, in many organizations, the security systems are supported by professional third-party alarm-monitoring companies.

These companies provide 24-hour/7-days-per-week monitoring services for a monthly fee. When they receive an alarm notification, they perform a response action based on their contractual agreement with the subscriber (client) company.

The sequencing of the response typically corresponds to the nature of the alarm notice they receive and when they receive it. They may initially try to contact designated personnel or contact law enforcement or fire department agencies when an unanswered alarm condition occurs. They may also dispatch armed or unarmed security personnel from the monitoring company to investigate the alarm.

Hands-On Exercises

In this exercise, you will learn how to secure the interior. The objectives are as follows:

BEFORE YOU BEGIN

Before you can complete this exercise, you must complete the exercises in Chapters 2 and 3.

- **For the ACME facility, define its security interior and determine the vulnerabilities associated with that perimeter.**
- **For the ACME interior and its vulnerabilities, perform research to determine what components or systems are available to secure the assets in the interior and what the cost options are for the components you find.**
- **Design an access-monitoring and control system that ACME can implement to secure this portion of their facility in the most cost-effective manner.**

The resources necessary for this exercise are as follows:

- **Internet access**
- **Pencil/pen and paper**
- **Completion of the exercises in Chapters 2 and 3**

Discussion

Returning again to the ACME Warehouse project presented in the previous lab procedures, the last preparation step before creating your recommendations to be delivered to the ACME management

staff is to research and design the intrusion-detection plan for the interior security zone of the facility.

In the previous procedures, you researched the options for monitoring and controlling access through the outer and inner perimeters, as well as monitoring the areas between those perimeters using video surveillance components.

In this procedure, you will be tasked to research components and strategies that can be used to monitor and control activity within the interior security zone. You will also be expected to make recommendations for implementing the most cost-effective solution that will provide the necessary levels of security.

Figure 4.17 depicts the ACME warehouse area. This portion of the facility is used to store ACME products for shipping to buyers and distributors. As the figure indicates, this area also contains the company's local offices, including:

- The CEO's office
- The shipping manager's office
- The accounting office
- The marketing office
- A supply closet for office supplies
- A janitorial closet for cleaning supplies

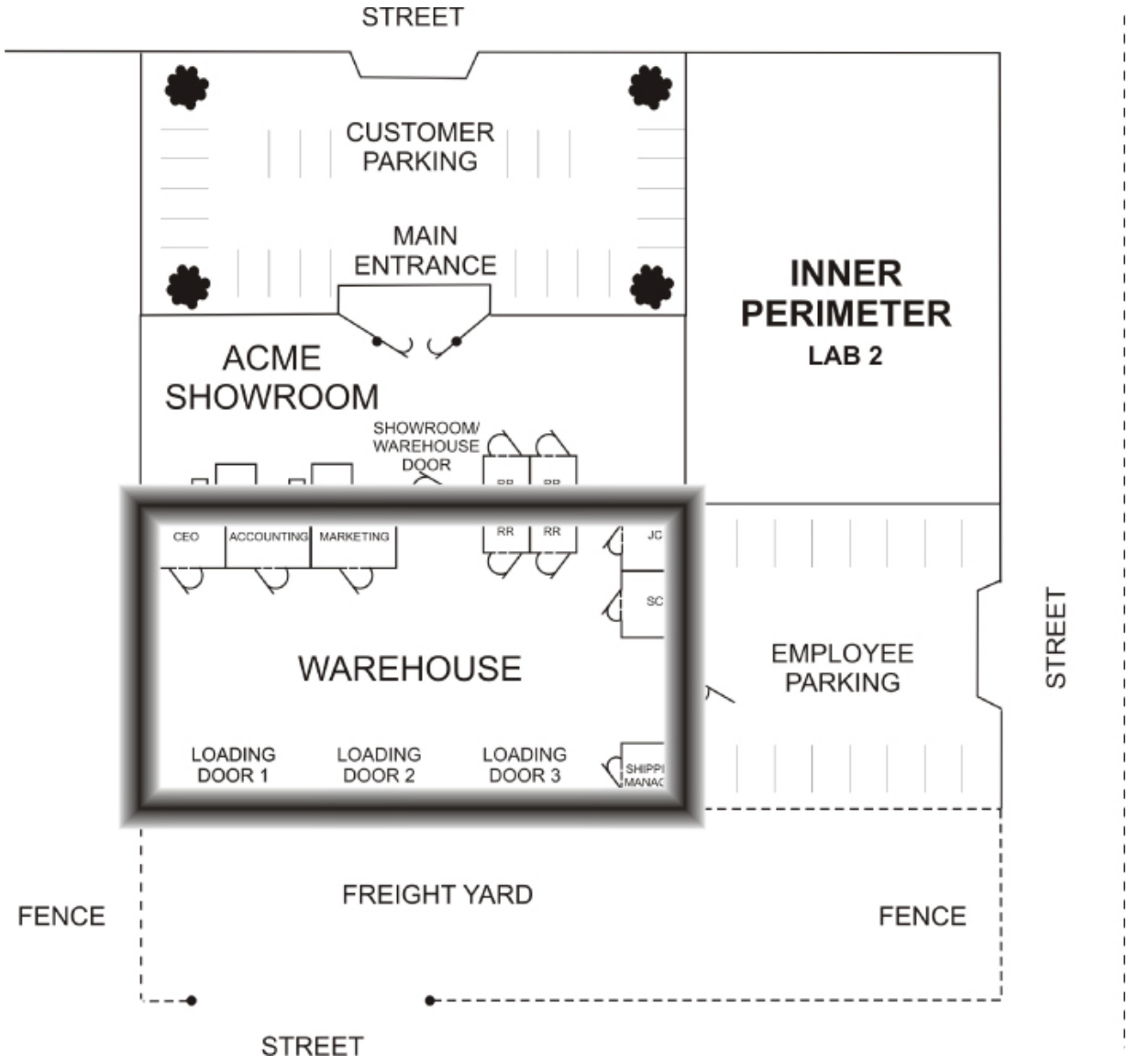


FIGURE 4.17 The Warehouse Area and Offices

The remainder of the warehouse area is open floor space filled with rows of shelving racks that hold ACME products.

It should be apparent that there are two security matters to be considered for the warehouse interior area:

- What are the interior security needs when the warehouse is in operation?
- What are the interior security needs when the warehouse operation is shut down for evenings and weekends?

Procedure

1. Review Figure 4.18 and identify/label the assets of the warehouse facility that should be monitored.

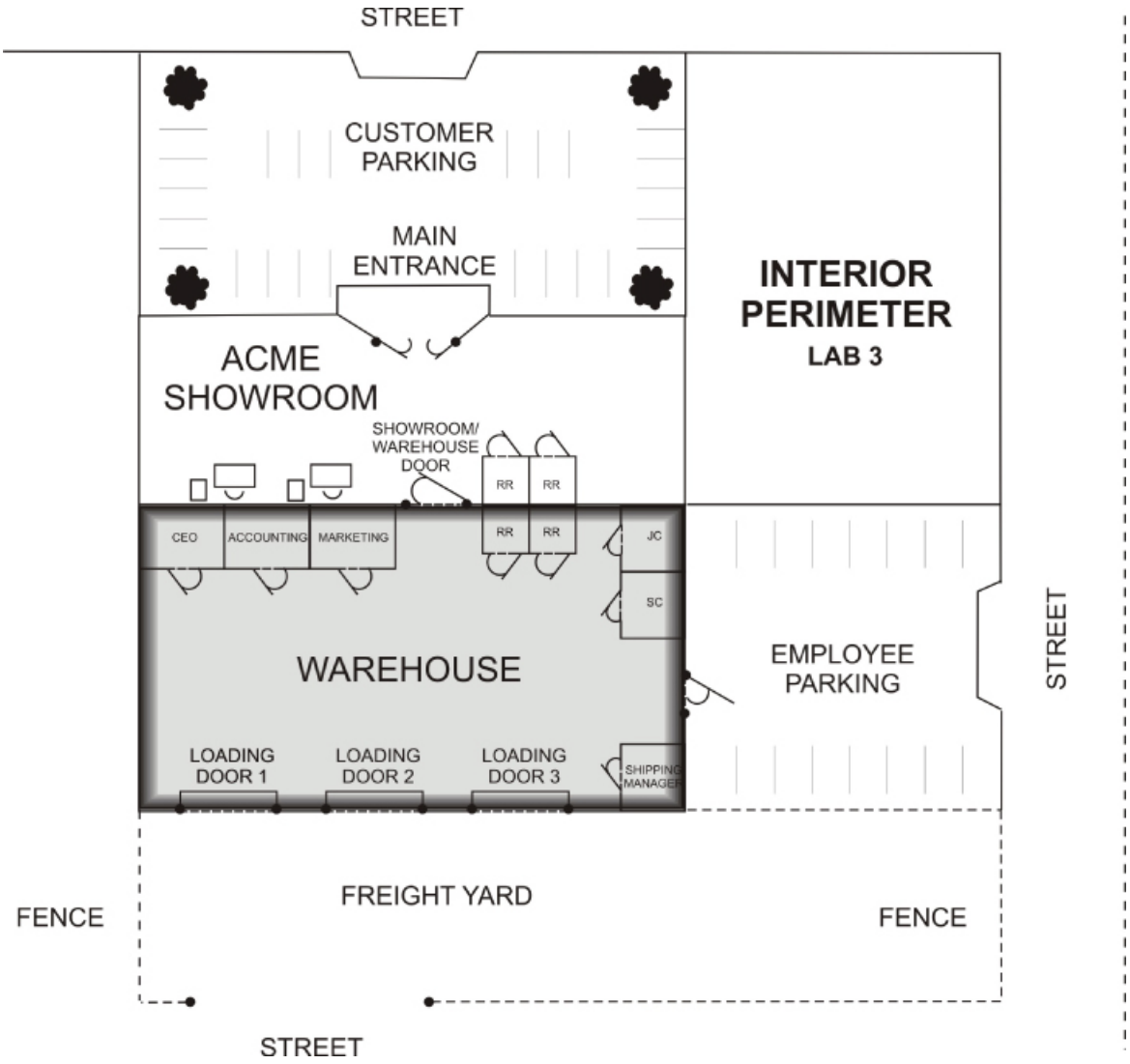


FIGURE 4.18 The Interior Security Zone

2. Use the Internet or other available research tools to research access-monitoring and control devices and systems that can be used to secure the access points you identified in the previous step.
3. Use Table 4.1 through Table 4.3 to organize the specified details about the access-monitoring and control products you find there.

For each item, try to locate at least two vendors.

TABLE 4.1 Door Locks

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Mag Door Lock Kit	Entry Vision	1	$274.99	$274.99
B	Electronic Keyless Door Lock	Gino Development	4	$89.99	$359.96
C	Schlage B581	Doorware.com	1	$52.00	$52.00

TABLE 4.2 Door Contacts/Sensors

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	Surface Mount	Seco-Larm	4	$1.90	$7.60
B	Wireless Surface	Insteon	4	$25.00	$100.00
C	Recessed Mount	Interlogix	4	$6.86	$27.44

TABLE 4.3 Motion Detectors

	Product Description	Vendor	Number Required	Cost Per Unit	Total Price
A	PIR Motion Sensor	Vedard Alarm	2	$8.50	$17.00
B	Pir 360 Motion Audio Sensor	Lithonia	2	$117.00	$234.00
C	PIR 360 Motion Sensor	Optex	2	$54.00	$108.00

4. List your recommendation for the access-control door locks you think should be utilized by ACME.

Answer: Mag Door Lock Kit, Electronic Keyless Door Locks, Schlage B581 deadbolt.

5. Where you would utilize the door locks you are recommending?

Answer: The Mag Door Lock Kit should be applied to outside warehouse pedestrian door for entry authentication and control. Electronic Keyless Door Locks should be installed for the CEO's office, the shipping manager's office, the accounting office, and the marketing office. The locks can be actuated without authentication steps from inside the offices, but require keys or passcodes to operate doors from inside of warehouse. Schlage B581 should be used for the outside showroom and the outside warehouse pedestrian door to secure the perimeter during closed hours.

6. List your selection for the door sensor types you would recommend to ACME for their interior assets.

Answer: The Interlogix Recessed Mount should be utilized to provide additional tracking of people's movement into sensitive offices such as the CEO's, both during operating hours and after hours of operation.

7. List your recommendation for the motion detectors ACME should use for their interior security zone.

Answer: The Lithonia 360 PIR Motion and Audio Sensors will allow full coverage/cross coverage of the warehouse floor after hours to trigger the security system if any other sensor fails before an intruder actually enters the security zone.

Review Questions

1. **Which type of access-control devices might be good recommendations for securing the CEO's office door?**

   Answer: A biometric ID device, a cipher lock, or a keyed lock. The information available in most executive offices typically requires some level of protection. The level of security depends on the organization's tolerance for risk and should be based on a risk assessment. This typically holds true for other management offices (for example, accounting and sales/marketing offices).

2. **Which type of access-control devices might be good recommendations for securing the doors of the supply and janitor's closets?**

   Answer: Either a simple keyed lock or no lock at all. These closets do not contain valuable assets and are often shared by various levels of employees requiring access so they may not require any security beyond a door.

3. **Where would infrared motion detectors be an appropriate choice for the ACME facility?**

   Answer: In the open floor area of the warehouse. There are no access points to monitor, so motion detectors can provide good

wide-area monitoring for interior zones. Of course, these devices would only be effective during the evening and weekend time periods when the warehouse operation was closed down and unattended.

CHAPTER 5
Infrastructure Security: Review Questions and Hands-On Exercises

Review the following summary points before proceeding to the "Review Questions" and "Exam Questions" sections at the end of this chapter to make sure you are comfortable with each concept. After completing the review, answer the review questions to verify your knowledge of the material covered in Part I.

Summary Points

- *Security* is the science, technique, and art of establishing a system of exclusion and inclusion of individuals, systems, media, content, and objects.
- *Physical security* is the science, technique, and art of establishing a system of exclusion and inclusion for tangible assets. In practice, this involves policies, practices, and steps aimed at combating theft, preventing physical damage, maintaining system integrity and services, and limiting unauthorized disclosure of information.
- *Cybersecurity* involves securing physical access to property, systems, and equipment ports while securing intangible assets including electronic, optical, and informational access to the system's data and controls.
- *Infrastructure security* refers to physical security initiatives that are applied to providing security for the basic physical and organizational structures needed for the operation of an enterprise, organization, or society.
- Securing the outer perimeter involves controlling who can move (walk, drive, fly) across the physical or logical line that marks

that perimeter. Examples of typical physical outer perimeters include property lines or the exterior walls of a building or complex.

- The inner perimeter typically involves physical barriers such as walls, doors, and windows—either exterior or interior depending on the context of the outer perimeter.
- The *interior* is the innermost level of security and consists of the interior of the building, office, cubicle, etc. that is surrounded by the inner and outer perimeters.
- Natural access control involves using natural design elements, such as structures and landscaping, to guide people as they enter and exit spaces.
- Territorial reinforcement employs structures, systems, and devices to prevent unauthorized entry and create a clear difference between what is public and private.
- Infrastructure security operation and management is based on three basic types of subsystems: access-control and monitoring systems; intrusion-detection and reporting systems; and video surveillance systems.
- Access control is the first major component of a physical security system. The first and most basic objective of any infrastructure security system is to deter potential intruders. This is the goal of access control. Intruders can't damage, destroy, or steal what you can't get to.
- A *right* is a legal privilege or permission granted to someone, or some group, by some recognized source of authority. This source can be a government, a legally recognized governmental agent, or a legally recognized owner of an asset.
- A person who has the right to access an asset is said to be *authorized* (by the recognized authority).
- Anyone who has not been given this right is labeled as *unauthorized*. When unauthorized people attempt to gain access

to an asset they do not have rights to access, they become *intruders*.

- A key component that brings all three levels of security together is a well-designed security policy that states how security is implemented at each level.
- A cohesive access control policy at each security level provides authorized people with appropriate levels of access to selected assets, while inhibiting access to assets by people who are not authorized.
- *Authentication* is the process of determining that someone is who they say they are.
- Effective access control involves being able to control the ingress, egress, and regress to an asset based on authorization. In particular, limiting the access of unauthorized personnel to important assets is the most fundamental security objective.
- Multiple factors are involved in authentication:
  - Knowledge—Something that only the designated person should know (something you know)
  - Possession—Something that only the designated person should have (something you have)
  - Inherence—Something that only the designated person is (something you are)
  - Location—Somewhere you are
- Many physical authentication systems are based on single authentication factors that depend on possession.
- Intelligent authentication methods involve *two-factor authentication* (a process that requires two of the factors to grant authorization) based on knowledge and possession.
- *False rejection* or false negative failures are reports that produce an incorrect rejection of the individual, thereby locking them out of a facility or security area to which they should have access.

- *False acceptance* or false positive failures are reports that incorrectly authenticate the individual, which could provide access to equipment or data that this person should not be able to access. Of the two types of authentication failure, this is the most significant in that it could grant access to malicious people.
- *Remote monitoring* refers to monitoring or measurement of devices from a remote location or control room. In the security realm, this involves having external access to the security system through a communication system.
- Remote-access monitoring systems are used to notify supervisory security personnel when an unauthorized access is attempted.
- Because open and closed conditions are not the same as locked and unlocked conditions, a single sensor cannot differentiate between these two sets of conditions. A second or different type of sensor needs to be installed and monitored to perform this differentiation.
- Remote-access control is a design feature that manages entry to protected areas by authenticating the identity of persons entering those secured areas (security zone or computer system) using an authentication system located in a location other than the access point.
- Remote-control access is a design feature that works with remote-monitoring systems to monitor, control, and supervise doors, gates, and conveyances from a distance.
- A functional intrusion-detection and reporting system typically includes an intelligent control panel connected by wires or radio signals to sensors at various locations throughout a facility or organization.
- Each security controller model is designed to handle a specific number of programmable zones. A zone can be a single point of protection such as a motion detector, or multiple points can be combined into a single zone.

- *Sensors* are a class of input devices that convert physical activity into a signal that can be presented to the security controller. They are available in a variety of configurations including magnetic switches for doors and windows, acoustic detectors, vibration detectors, motion detectors, and glass-break detectors. Sensors protect the perimeter, selected outside areas, and the open spaces inside the facility.
- Physical-intrusion-detection systems typically include three basic types of output devices: visual notification, audible annunciators, and remote messaging.
- Two types of fire-detection sensors are available: heat detectors and smoke detectors. They operate by detecting heat rise or smoke in the home.
- Digital video recorders (DVRs) are the preferred technology for recording surveillance video.
- Motion detectors work by detecting the changes in the infrared energy in an area.
- The use of multiple physical security zones has several purposes. It allows the user to arm only portions of the system, such as the perimeter doors and windows, while bypassing the interior motion detectors in a specific zone.
- An IP camera can be viewed from anywhere in the world where Internet access is available.
- The two important specifications that influence the cost of cameras are light sensitivity rating (lux rating) and resolution.
- Surveillance cameras should not be used where there is a reasonable expectation of privacy by individuals.
- In addition to determining what specifications security cameras must possesses for a given role, it is equally important to map out a camera deployment strategy to maximize the surveillance investment.

Security Challenge Scenarios

In Chapter 1, you were asked to record your observations for the risk-assessment challenges presented there. At that point, you may have had little or no knowledge of the security tools and techniques required to secure the environments presented in those scenarios.

Now that you have read the first four chapters, complete the information requested in the following section and compare that information to the original assessments you generated in Chapter 1 to measure how much you've learned.

Infrastructure Security Scenario 1

Identify:_____
_____

Protect:
_____
_____

Detect:
_____
_____

Respond:
_____
_____

Recover:
_____
_____

Infrastructure Security Scenario 2

Identify:_____
_____

Protect:
_____

_____

Detect:

_____

_____

Respond:

_____

_____

Recover:

_____

_____

Professional Feedback

In this section, you will compare your observations to those of a working security specialist—in this case, Philip Craig, the founder of BlackByte Cyber Security—to improve your understanding of cybersecurity.

ABOUT PHILIP CRAIG

Philip Craig is the founder of BlackByte Cyber Security, LLC, a consultancy supporting the Pacific Northwest National Laboratory (PNNL) research and national security agendas, as well as the National Rural Electric Cooperative Association and National Rural Telecommunications Cooperative.

For many years, Phil served as a Senior Cyber Security Research Scientist at PNNL, where he provided engineering and program management support in the fields of cybersecurity, supervisory control, and data acquisition (SCADA) technologies, computing, and communications infrastructure.

This included the development of complex system and policy solutions in a variety of critical infrastructures including the nuclear power, electric power, and water sectors. He developed and deployed both strategic and tactical cybersecurity defensive solutions for the electric power and nuclear sectors.

The Insights of a Practicing Professional

Practicing security professionals have a significant advantage when determining the most effective security solutions for many deployments very quickly. After repeatedly practicing the trade in the field, you too will be able to create certain models that will remain effective in the future.

Here is a time-proven approach that opens with three very basic questions that will position you to enter the initial assessment phase. Always ask your client:

1. What are we trying to protect?
2. Who are we trying to protect it from?
3. Why do we need to provide protection?

The first answer is always a physical thing (e.g., some material, component, product, etc.) that you can physically see, taste, touch, and smell. It may be a sensitive device or instrument in development or it may have a high monetary value. It also may be some material that has environmental sensitivity or that may be dangerous to the general public if protection methods are not utilized correctly.

The second answer is focused on a person (potentially an adversary).

The last answer could originate from a business need supporting the economic strength of the corporation or the requirement to follow a particular regulation. Needless to say, you can throw as many of your newly learned techniques as you can at the solution, but without the information you discern from asking these questions, you are wasting a significant amount of your time—and more importantly, your client's money.

Let's review your scenario. Consider the following construct:

- A building (containing multiple floors and spaces)
- An office environment (containing spaces for offices and cubicles)
- A cubicle (containing computing resources)

As you learned earlier, there are many physical and cybersecurity considerations. They exist in external, internal, and interior contexts with many attributes that influence the access to each. We will need to consider these influences and begin to provide physical and logical separations that are often called perimeters or demarcations.

Figure 5.1 represents a reliable model that provides a consistent approach for handling these considerations. For security purposes, we're always concerned primarily with threats, so this threat-informed model will always apply.

FIGURE 5.1 Threat-Informed Pyramid

Securing the Top Region

The items to deal with in the upper region of the threat-informed model include:

- *Objectives:* The adversary's overall objective is to disrupt, destroy, or steal a target
- *Target Sets:* The assets that represent the best opportunity to upset, compromise, damage, or otherwise discontinue functions and/or operations of a system.
- *Adversary:* An agent who is determined to carry out a particular objective driven by MOI (motive, opportunity and intent). Each adversary attribute will govern the adversary's overall decision-

making process to determine what is necessary to reach an objective and complete a mission.

Securing the Middle Region

The activities called out in the middle region of the threat-informed model include:

- *Credible Threat Scenarios:* A set of activities, when scripted or arranged in a particular sequence, would have the highest success of achieving an attack objective. Therefore, you must concentrate your efforts on identifying all these scenarios.
- *Analysis:* Those activities (threat vector analysis, attack trees, consequences, and susceptibility analysis) that must be performed to evaluate the best, most likely, most effective, or most probable means of a potential attacker's success in reaching an objective along with a description of the impacts of such success.
- *Defined Threat Environment:* The Defined Threat Environment represents the culmination of all the attributes associated with the topics above it in the "upper" and "middle" regions of the pyramid.

Securing the Bottom Region

The activities called out in the bottom region of the threat-informed model include:

- *Security Strategies (Detect, Deter, Deny, Delay, Respond, Recover):* Based on the defined threat environment, those strategies are formulated to ensure security functions to deter, detect, deny, delay, respond, and recover from an attack.
- *Security Controls Cyber/Physical (Management, Operational, Technical/Guards, Gates, Locks):* Mechanisms that are employed to ensure that the security strategies are effective.

- *Risk Determination – Policy – Training – Audit and Compliance:* The supporting programmatic elements necessary to document measures to determine the effectiveness of an overall security program.

All too often organizations are too quick to apply a comprehensive security policy and then build a program to ensure the policy is met. From a practicing security professional's standpoint, that is completely backward from how it should be approached. However, at your first job, or on any new job, you're going to likely step into an operational security program. It is important that you still take this approach or you'll struggle with the reasons that decisions have already been made.

So now you've been given a means to understand what, who, and why, as well as a model to enable a good process to assess and evaluate the security environment, what is next? How can you tackle the task?

Tackling the Task at Hand

First, you need to establish your perspective. We'll call it the "you are here" dot on a map of your environment. Two different perspectives are used: an outside-in and an inside-out. Picture a castle. In the days when castles were prevalent, they were actually giant fortified structures created to keep people out. This perspective is an "outside-in" perspective. The architects busily constructed methods that from an outside perspective protected their castles from being penetrated. Although many physical security methods still employ this perspective (and should), a more comprehensive approach is to use the "inside-out" perspective. This approach will ensure that the most interior areas are considered and you will be able to build a security posture using graded methods as you reach the most outer areas. This is called a *graded approach*. It allows security professionals to prescribe security controls as necessary so they don't overprescribe them and amass excessive costs or expend unnecessary resources or effort.

What Am I Protecting?

Document the object, material, and property. It can be a box of diamonds or intellectual property like the Colonel Sanders Kentucky Fried Chicken recipe.

Who Am I Protecting My Asset From?

You play the adversary! From an inside-out perspective, start at the most interior area (cubicles) and look for any artifacts that could challenge your security controls.

Make sure you are familiar with and understand the physical pathways: from the cubicles to the office areas to the building itself. Look for both physical and cyber ingress and egress. Always think like an adversary (the top of our triangle).

Why Am I Providing Protection?

Is it the asset's value? Is it a production process that could result in millions of dollars of lost revenue if disrupted? Is it some material that could cause challenge the safety of your employees or the public? Are there regulatory or other legal or contractually binding requirements?

Executing Your Plan

Prioritize and select the appropriate (necessary) security controls that will detect, deter, deny, delay, respond, and recover your security posture. Properly documented installation processes and procedures should be in place to help ensure that your security controls are properly installed.

Implement your plan as constructed. Make sure all physical and cyber methods are installed as required.

Check your implementation by procedure. When you are operational, there needs to be a method to constantly check to ensure that your security controls are effective. These controls usually range from simple internal email-phishing exercises,

rattling doors and windows, to actually executing a combined cyber/physical challenge exercise constructed to test your response and mitigation capability.

Improve your posture as you execute periodic assessments and exercises that may expose any weaknesses and opportunities to provide corrective or augmented capabilities. Without this cycle, you'll never be able to defend your operational budgets or get support from management.

There are hundreds if not thousands of ways to provide secure and trusted environments depending on the what, who, and why of any company or organization. The methods that are successful are those that you can defend with proper arguments that are well documented. Your future employer won't just keep you around because you're good, they'll keep you around because you're thorough.

Review Questions

The following questions assess your knowledge of the material presented in Part I.

1. **_____ is the science, technique, and art of establishing a system of exclusion and inclusion for tangible assets.**

   Answer: Physical security. In practice, this involves *policies, practices,* and *steps* aimed at combating theft, preventing physical damage, maintaining system integrity and services, and limiting unauthorized disclosure of information.

2. **_____ is a report that incorrectly authenticates the individual, which could provide access to equipment or data that this person should not have.**

   Answer: False acceptance or false positive failures

3. **Define *lux rating* as it applies to surveillance cameras and describe the typical range of lux ratings for these devices.**

   Answer: The amount of light required to obtain a reasonable video camera image is called the *lux rating*. Lux is a measure of the amount of light that falls on an object. One lux is approximately the amount of light falling on one square meter from one candle measured from one meter away. Typical camera ratings range between 0.5 and 1.0 lux.

4. **Using natural design elements such as structures and landscaping to guide people as they enter and exit spaces is referred to as_____.**

   Answer: Natural access control

5. **Which type of security device is used for programming, controlling, and operating access control and management devices?**

   Answer: Most intrusion-detection and reporting systems employ a *keypad* device for programming, controlling, and operating various access-control and management devices.

6. **Which type of cameras provides the best resolution in low-light conditions?**

   Answer: An IR camera. An infrared security camera has infrared LED lighting (light from a different region of the electromagnetic spectrum than we are normally used to seeing) installed around the outside of the camera lens. This lighting allows the camera to capture a good image in no light at all. With a little bit of light (called low light), the infrared camera can capture a picture that looks just like daytime.

7. **Which type of image sensor is used in cameras designed to produce the highest quality images?**

   Answer: CCD. The best surveillance cameras employ *Charged Coupled Device (CCD)* technology. They have high resolution,

low-operating light requirements, less temperature dependence, and high reliability.

8. **Describe the primary uses for keypads in security systems.**

   Answer: Most intrusion-detection and reporting systems employ a *keypad* device for programming, controlling, and operating various access-control and management devices.

9. **Describe the technologies used to report alarm conditions to key personnel or remote monitoring organizations.**

   Answer: The most common *remote notification systems* involve the use of a telephone line by the intrusion-detection and reporting system's control panel to automatically call a remote monitoring facility or key personnel when an alarm condition exists. Some systems employ a separate *telephone dialer* or a built-in dialer. However, a growing number of systems possess built-in *cellular communications* systems. Such systems provide additional dependability in that they can function even if the physical telephone lines are damaged.

10. **_____ employs structures, systems, and devices to prevent unauthorized entry and create a clear difference between what is public and private.**

    Answer: Territorial reinforcement

11. **With_____, the condition monitoring system can record and signal each time a specific gate or door is unlocked (granting access) and what type of access was granted. Unlocked monitoring can also identify who was granted access.**

    Answer: Unlocked condition monitoring

12. **List the locations in which perimeter-area input sensors are typically placed in an intrusion-detection and**

reporting system.

Answer: Perimeter-area inputs to the control panel typically include sensors at every perimeter opening including doors, windows, garage doors and windows, and doors to crawl spaces. Additional perimeter protection may include using sound, vibration, and motion-detector sensors to guard against entry through broken windows.

13. **Which physical technique is used to create a physical security zone on a security controller?**

    Answer: Logically group related sensors together to create a security zone. This is accomplished by connecting all of the related sensor switches (all sensors appear as switches to the security controller) together in a serial format that connects to a specific set of contacts on the controller's panel.

14. **List the four factors that are commonly employed in authentication systems.**

    Answer: There are multiple factors that can be used to establish authentication: Knowledge—something you know, possession—something you have, inherence—something you are, and location—where you are.

15. **Name the two major concerns associated with storing video surveillance information, particularly in larger enterprises.**

    Answer: How much video needs to be stored? For how long does it need to be stored? The answers to these questions enable the organization to determine its storage capacity needs.

Exam Questions

1. **Securing which of the following involves controlling who can move (walk, drive, fly) across the physical or**

logical line that marks this perimeter, such as property lines or the exterior walls of a building or complex?

A. **The interior space**

B. **The inner perimeter**

C. **The outer perimeter**

D. **The primary zone**

Answer: C

2. **Which of the following is *not* a subsystem involved in infrastructure security management?**

A. **Access-control and monitoring systems**

B. **Intrusion-detection and reporting systems**

C. **Video surveillance systems**

D. **Corporate cyber security policies**

Answer: D

3. **Which of the following options represent physical barriers? (Select all that apply.)**

A. **A locked door**

B. **A receptionist**

C. **An RFID badge reader**

D. **A surveillance camera**

Answer: **A and B**

4. **Which type of surveillance camera can be viewed from virtually anywhere in the world?**

A. **A digital camera**

B. **A digital IP camera**

C. **An analog camera**

D. **A hybrid camera**

Answer: B

5. **From the following report types, which options would produce an incorrect rejection of the individual, thereby locking him out of a facility or security area to which he should have access? (Select all that apply.)**

   A. **False rejection**

   B. **False acceptance**

   C. **False negative failures**

   D. **False positive failures**

   Answer: A and C

6. **Which sensor detects a beam of light (visible or invisible) and responds to a change in the received light intensity?**

   A. **Microwave sensor**

   B. **Pressure sensor**

   C. **Motion sensor**

   D. **Photoelectric sensor**

   Answer: D

7. **Which lens enables you to view an entire room but with some distortion of the image?**

   A. **Fish-eye lens**

   B. **Telephoto lens**

   C. **Fixed-focal-length lens**

   D. **Varifocal lens**

   Answer: A

8. **Which of the following best describes the meaning of *lux rating* as it applies to surveillance cameras?**

   A. **Rating for the size of the camera lens**

   B. **Amount of light required for an acceptable image**

   C. **Resolution of the camera lens**

   D. **Specifies the color resolution of a camera**

   Answer: B

9. **Which of the following cameras provides the ability to maintain a degree of secrecy by using illumination that is outside of the visible light spectrum?**

   A. **CCD camera**

   B. **Infrared security camera**

   C. **Black-and-white camera**

   D. **Color camera**

   Answer: B

10. **Which of the following cameras features the best set of specifications for monitoring a 24/7 cash machine that must operate in both daytime and low-level night-time lighting conditions, while providing a high-resolution, detailed view to monitor the different banking functions the machine is used for?**

    A. **Camera 1 – 800 × 600 pixel resolution, 1.0 lux rating**

    B. **Camera 1 – 2240 × 1680 pixel resolution, 0.5 lux rating**

    C. **Camera 1 – 1024 × 768 pixel resolution, 0.75 lux rating**

    D. **Camera 1 – 1536 × 1180 pixel resolution, 0.9 lux rating**

Answer: D

PART II
Securing Local Hosts

CHAPTER 6
Local Host Security in the Real World

The following challenges provide contextual reference points for the concepts you will learn in Part II. Because you have not yet read the chapters in Part II, the challenges in this chapter are designed to introduce you to the local host scenarios you'll face in the real world.

In this chapter, you'll learn to:

1. Apply applicable categories and sub-categories of the NIST Cyber Security Framework's "Identify" function to a specific scenario to document the network's assets and their possible vulnerabilities.
2. Use applicable categories and sub-categories of the "Protect" function to generate specific policies and actions that can be used to secure the network's assets for the specified scenario.
3. Apply applicable categories and sub-categories of the "Detect" function to identify technologies, policies, practices, and strategies that can be used to monitor the network in the scenario to determine whether security events are occurring.
4. Apply applicable categories and sub-categories of the "Respond" function to create an incident response plan to cover specific security events associated with the scenario presented.
5. Apply applicable categories and sub-categories of the NIST Cyber Security Framework "Recover" function to the scenario to implement solutions for recovering from specific cyber events.

Security Challenges

This chapter will kickstart your thought processes for what you are about to learn in Part II. Instead of simply trying to absorb all of the information you're about to learn in these chapters, you'll begin here by gaining a better understanding of the real-world relevance of that information.

In Chapter 10, you will return to these scenarios and apply what you learned in Chapters 7, 8, and 9. You will also compare your observations to those of the professional security specialists who have provided their observations and solutions for these scenarios.

Computing Device Security Scenario 1

You have been assigned to develop a local security policy and the configuration specifications for the desktop computers used by in-house employees at your firm. These PCs are mounted in special openings under the desk in each cubicle.

The computers are physically identical, and they all run the same operating system. However, they may have different types of job-specific company software installed, as shown in Figure 6.1. These computers are equipped with the following:

- Detachable keyboards and mice
- Six built-in USB connection ports
- Separate video display monitors
- UTP local area network connection ports
- Microsoft Windows 7 Professional operating systems
- Microsoft Office 2013 software
- Dual built-in DVD disc drives

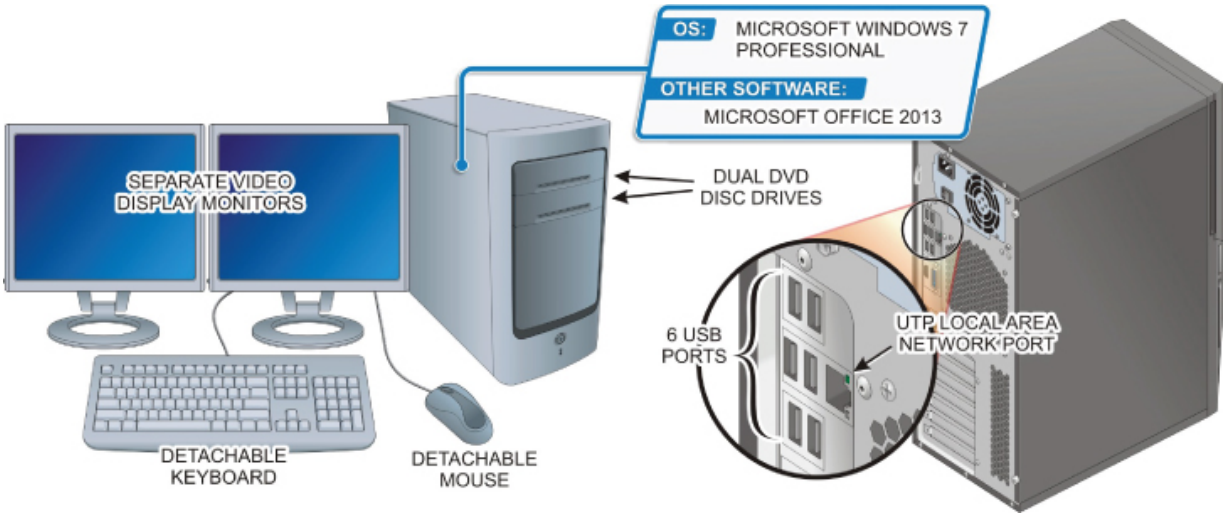


FIGURE 6.1 Corporate Desktop PC

Risk Assessment 1

From the information provided in this first scenario, consider the National Institute of Standards and Technology (NIST) functions detailed in this section and then write your observations as they relate to each category.

Identify

Create an inventory of physical and software assets associated with the user computers described here. Identify potential pathways that could provide unauthorized personnel with access to the physical and software assets associated with these computers (NIST ID.AM-1, 2; ID.RA-1).

Protect

Describe how to go about managing the identities and credentials of authorized users at the local level (NIST PR.AC-1, 2, 4; PR.PT-1, 3).

Detect

Using the computers and environment identified at the outset of this section, how might you determine whether someone was attempting to gain access to the computers described or the

software and intellectual property stored on them (NIST DE.CM-1,4; DE.AE-1,2,3,4)?

Which types of systems must be in place to identify occurrences of physical security breaches (NIST DE.CM-2, 3)?

Respond

Describe how to respond to a suspected security breach of one or more local host units (NIST RS.RP-1; RS.CO-2, 3, 4, 5; RS.AN-1, 2, 3; RS.MI-1, 2, 3; RS.IM-2).

Recover

List the policies and steps that should be put into place to recover from actions that might be taken to access, damage, or destroy the assets described in this scenario (NIST RC.RP-1).

Which items might a recovery plan include if local host security is breached (NIST RC.CO-1, 2, 3)?

Computing Device Security Scenario 2

Because you did such an outstanding job of creating the security policies and configurations for the company's desktop computers, you have been asked to produce the same type of materials for the notebook computers used by the organization's sales people.

These computers typically contain product information the sales people need to do their jobs when they are meeting with customers. As such, confidential company and customer information (such as proprietary price lists for different customers, customer contact and purchase history information, confidential communications between the sales person and the customers, as well as with company supervisory personnel, and information about products under development but not yet announced) is stored on these devices.

Obviously, these computers are portable PCs that work in the office and at different locations on the road. As depicted in Figure 6.2,

these computers are equipped with the following:

- Built-in keyboards and displays
- Two built-in USB connection ports
- UTP local area network connection ports
- Microsoft Windows 7 Professional operating systems
- Microsoft Office 2013 software
- Dual SD card reader slots
- Built-in wireless networking capabilities
- External VGA display connection ports
- Built-in DVD disc drives

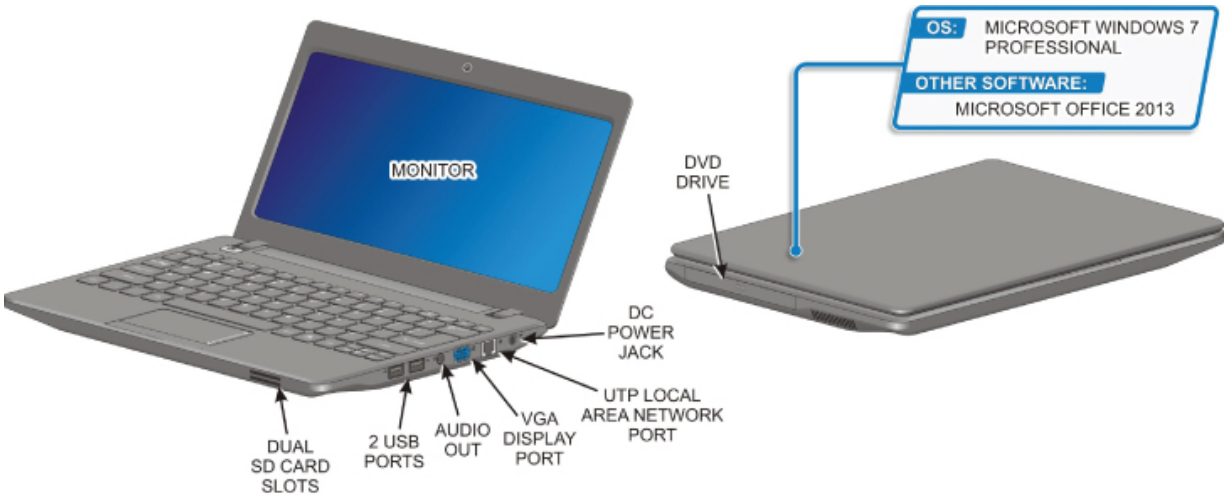


FIGURE 6.2 Notebook PC

Risk Assessment 2

From the information provided in the second scenario, consider the NIST functions detailed in this section and then write your observations as they relate to each category.

Identify

Create an inventory of physical devices and systems associated with the user computers described here (NIST ID.AM-1).

Create an inventory of software used on the company notebook computers (NIST ID.AM-2).

Map the organization's communications and data flow with these portable computers (NIST ID.AM-3).

Describe the risks associated with the environment and the computing devices described in this scenario. Create a risk assessment of identified asset vulnerabilities (NIST ID.RA-1, 2, 3, 4, 5).

Protect

For the equipment package described, determine which assets must be in place to mitigate the risks identified previously (NIST PR.AC, AT, DS, IP, and PT).

Describe how to manage the identities and credentials for the authorized users of these computers (NIST PR.AC-1).

Create a plan to determine how remote access will be provided and protected when the mobile devices are used away from the corporate facilities (NIST PR.AC-3).

Describe how data on the mobile computers will be secured as well as how it will be protected when communicated to and from the devices (NIST PR.DS-1, 2).

Detect

Establish a security plan to monitor these information systems to identify cybersecurity events and verify the effectiveness of protective measures (NIST DE.CM-1-8; DE.AE-1-5).

Which types of systems must be in place to monitor remote communications from these devices to detect potential cybersecurity events (NIST DE.CM-1)?

Which types of systems must be in place to monitor personnel activity to detect potential cybersecurity threats (NIST DE.CM-3)?

Respond

Create a plan to ensure that response processes and procedures are in place to provide timely responses to detected cybersecurity events (NIST RS.RP-1; RS.AN-1).

Considering the information kept on these mobile host devices, which type of response plan might be necessary if security is breached on one of the systems (NIST RS.CO-4, 5)?

Recover

Which steps should be put into place to recover from actions intended to access, damage, or destroy the assets you've identified (NIST RC.RP-1)?

Summary

Record your observations for risk assessments presented in this chapter. In Chapter 10, you will compare these original thoughts and observations with those you will generate after reading Chapters 7, 8, and 9. You'll also be able to compare your answers to those of professional security specialists.

CHAPTER 7
Securing Devices

Based on the scenarios in Chapter 6, you can see that protecting standalone Information Technology (IT) assets offers many challenges. Local host (Computing and Intelligent Control Device) security is implemented on multiple levels that include physical denial of use, limited access to system resources, and active protection against individuals and software intent on corrupting or stealing data. In this chapter, you'll learn to:

- **Identify three security perimeters associated with an end point computing device**
- **Provide physical security for end point computing devices**
- **Evaluate BIOS/CMOS Security Options**

The Three Layers of Security

If you think of standalone IT or ICS devices in terms of the three layers of security described in Chapter 2, you can think of the *outer perimeter* as the space around the outside of the physical device and its housing. The *inner perimeter* should be viewed as the device's operating system and application programs. Finally, the interior of the device consists of the intangible data assets of the information created, obtained, and stored electronically in the device. Figure 7.1 graphically illustrates these layers.

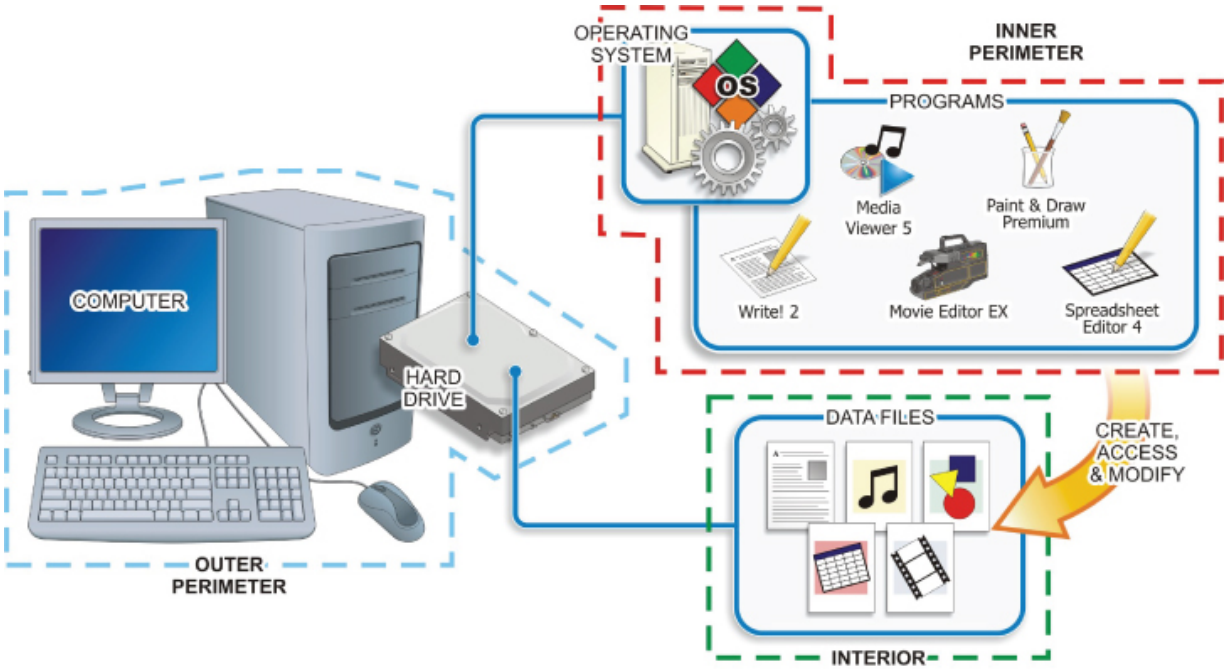


FIGURE 7.1 The Three Layers

The first level of securing your intelligent devices is to control access to them. Once again, an intruder can't damage, destroy, or steal what they can't get to. This applies to intelligent computing and control devices as well. So, the first step is to control physical access to the devices as much as is practical.

Autonomous or semiautonomous ICS devices, such as Programmable Logic Controllers (PLCs) or standalone microcontrollers, can normally be placed in secure, lockable enclosures where access is limited to only those people possessing the key. These devices tend to be prevalent in industrial control and utility environments.

In this chapter, the primary asset we will be dealing with is the personal computer (PC). For the most part, it is not practical to lock up desktop and portable PC systems that may be used by different people. In many cases, a given computer may routinely be used by different personnel—for example, a day shift employee and a night shift employee. In such applications, administrative security measures must be in place to guarantee proper authentication and access control.

Securing Host Devices

Protecting local computing and control devices begins with a locked door or an enclosure when possible. However, in business and industrial settings, many such assets are used in relatively open environments. In these environments, locking security cables, like the one depicted in Figure 7.2, may be used to physically attach the computing equipment to desks or other nonportable structures to make them more difficult to remove.

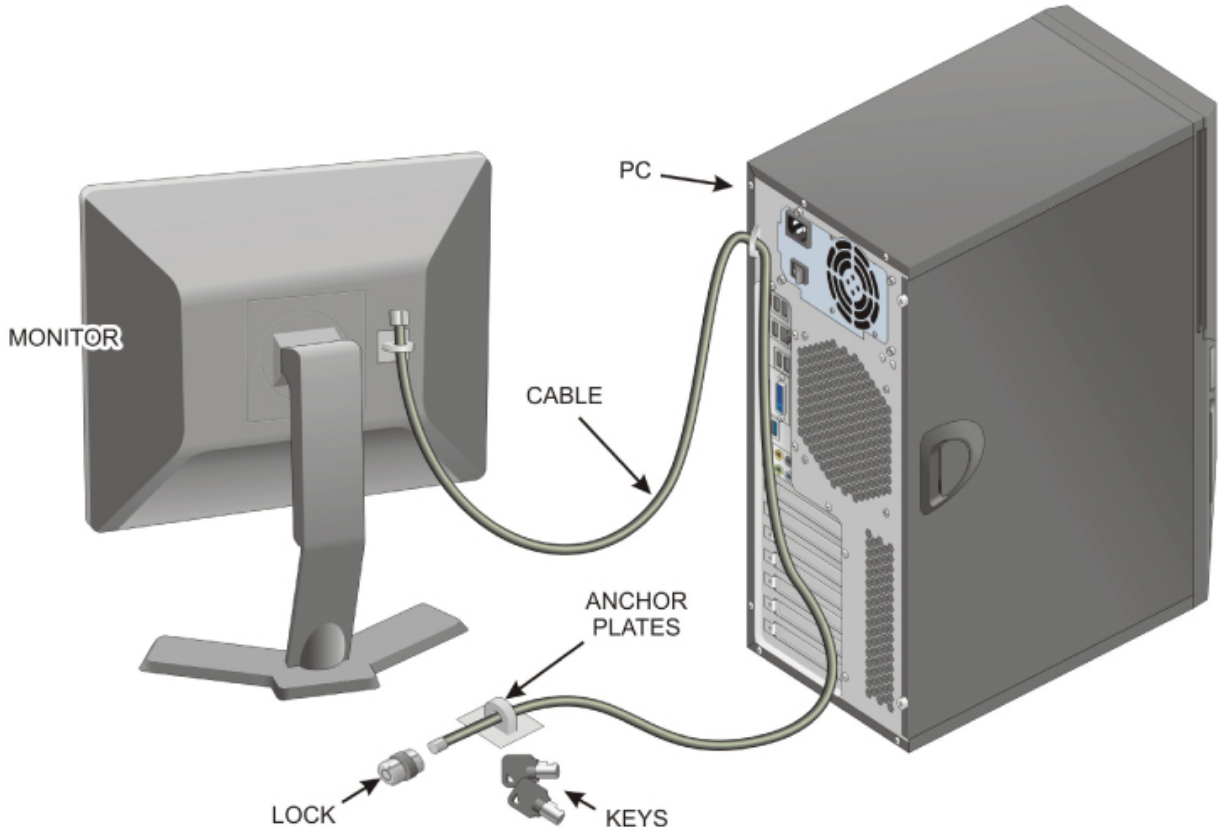


FIGURE 7.2 PC Security Cable

Docking stations like the one illustrated in Figure 7.3 are accessories designed for use with portable computing devices. The primary function of the docking station is to enable portable users to travel with their portable devices, yet still employ full-size peripheral and connectivity devices when they are in the office environment.

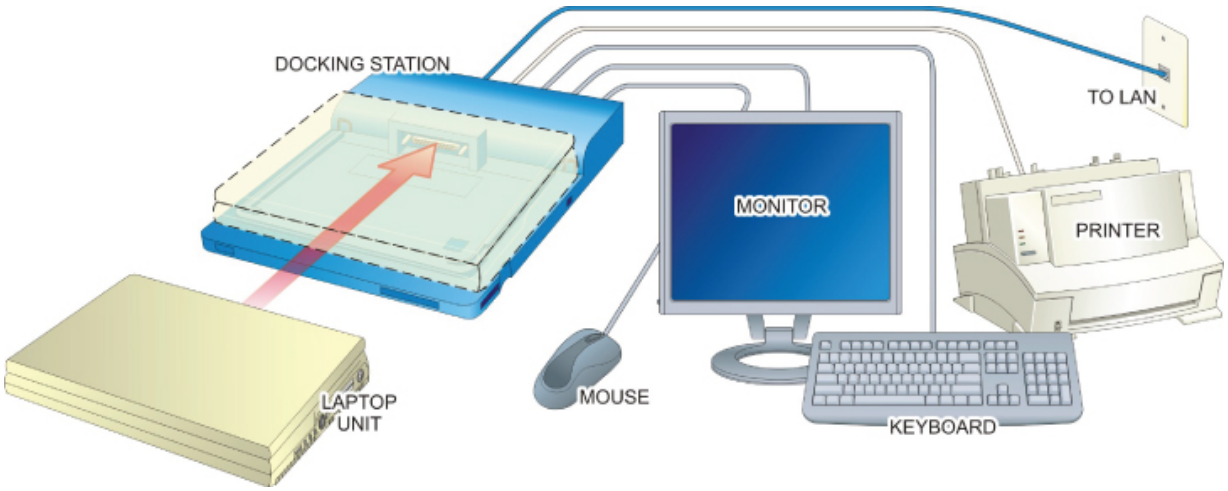


FIGURE 7.3 A Docking Station

The second function of many docking stations is to provide a lockable attachment to the desktop to prevent unauthorized users from picking up the portable unit while it is not in use and simply carrying it away.

In many office environments, specialized work desks and cabinetry can be used to secure the device in place and to limit some access to the device. This typically involves bolting the device to the workspace cabinetry or hiding it inside the cabinetry with limited openings for physical access to the device—maybe just large enough to turn the device on and operate the disc drive mechanisms.

Securing Outer-Perimeter Portals

After you have taken steps to protect the physical device from unauthorized access and/or removal, for your next level of protection, consider the physical case of the local computer or intelligent control device as its outer perimeter.

Also, remember what malicious people really want from such devices—they want the programs and data located inside the machine. So, where can such people access these items in order to damage, destroy, or steal them? In both computing and intelligent control devices, there are three general locations where they can gain access to these items:

- While it's in memory
- While it's in storage on devices such as hard drives and flash drives
- When it is being transferred from one place to another

In the case of the personal computers, depicted in Figure 7.4, how would you penetrate their cases to get to the intangible valuables inside?

FIGURE 7.4 Typical PCs

The most obvious point of access through the outer perimeter of a PC would be its basic input devices: its keyboard and mouse or touch-sensitive display. If someone can simply sit down in front of the system and freely use its input devices (keyboard, mouse, touchpad, or touchscreen), they have an avenue for accessing the information inside. All they have to do is push the On/Off button and wait for the device to boot up.

DISPLAYS AND THEIR INPUT CAPABILITIES

Unless a display has an input capability, such as a USB port, it is not considered to be an access device that can be exploited. The same holds true for nonwireless printers or other output-only devices.

BIOS Security Subsystems

There is one basic security tool built into the hardware of most personal computers that offers some basic protection before the operating system bootup completes. The Basic Input/Output System (BIOS) offers basic hardware security options that can be set through its BIOS Setup utility, also called the CMOS Setup utility. Figure 7.5 displays a typical Security Configuration screen. Normally, these options include setting user passwords to control access to the system and supervisory passwords to control access to the CMOS Setup utility.

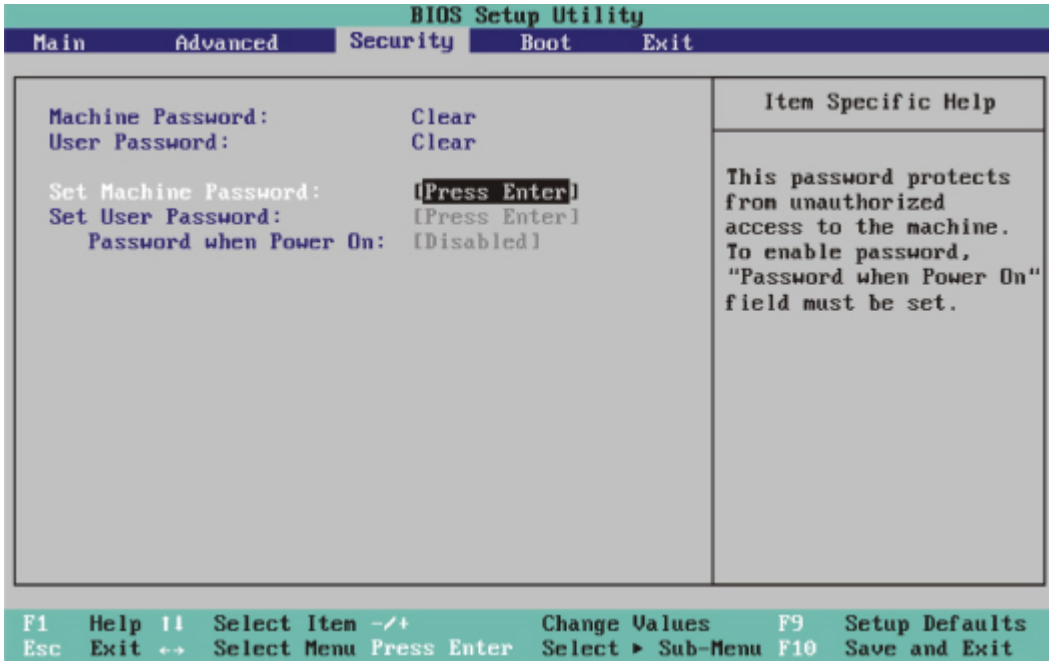


FIGURE 7.5 CMOS Security Configuration

The Set User Password option enables administrators to establish passwords that users must enter during the startup process to complete the boot process and gain access to the operating system. Without this password, the system will never reach an operational level that an intruder could use to access its internal perimeter and interior information.

However, this password does not provide access to the CMOS Setup utility where the user and supervisory password options are configured. A supervisory password option must be used to establish a password that can be employed to access the CMOS Setup utility.

The Security Configuration screen may also include options for setting virus check and backup reminders that pop up periodically when the system is booted. In addition to enabling these settings, administrators can also specify the time interval between notices.

One of the main sets of security options in the CMOS Setup utility consists of those that can be used to control access to the system's inner perimeter and interior assets. For the most part, these options

cover such things as limiting access permitted through the asset's physical ports and removable media systems, as well as access to the boot sector of the system's disk drive.

Because the CMOS password controls access to all parts of the system, even before the bootup process occurs, there is some inconvenience in the event that the user forgets a password. When this occurs, it will be impossible to gain access to the system without completely resetting the content of the CMOS RAM. On some motherboards, this can be accomplished by shorting a special pair of jumpers on the board.

With other systems, you must remove or short across the backup battery to reset the CMOS information. You will also have to unplug the power from the commercial outlet to reduce the voltage to the CMOS registers. When the content of the CMOS is reset, you must manually restore any nondefault CMOS settings being used by the system.

Local System Hardening

In computer and networking environments, the term *hardening* is used to refer to the process of making a system more secure. Computer hardening efforts begin with hardware, but also extend to the local host's operating system, its file system, and its applications.

At the hardware level, the primary area of hardening is the system BIOS and any other firmware add-ons that may have been introduced to the system. Because *firmware* by definition is a software product enclosed in a hardware device, it comes preinstalled in the system or on one of its devices.

To make firmware more secure than it already is requires updating. Depending on the physical structure of the firmware, these updates may involve physical or logical updates. Hardware manufacturers provide firmware updates to improve their existing, installed products—including upgrading their security tools. Their intent is to improve the reliability, security, or attractiveness of their product.

In most cases, firmware updates are designed to provide solutions to hardware incompatibilities or to provide the Data Link layer drivers necessary for the firmware to work with a particular operating system. However, some product improvements may simply extend the product's capabilities but may not necessarily make it more secure.

Additional Inner-Perimeter Access Options

In addition to the basic input devices used with personal computers, there are several other pathways built into most computer systems that provide access to the inner perimeter. Even non-networked, standalone computers may be susceptible to exploitation from outside sources through removable media systems and physical access ports (connection points).

Physical Port Access

Physical hardware ports enable the basic PC system to interact with optional, removable devices, as shown in Figure 7.6. They also provide a potential security threat because individuals with malicious intent can gain access directly into the computer internal communication and processing system through these ports.

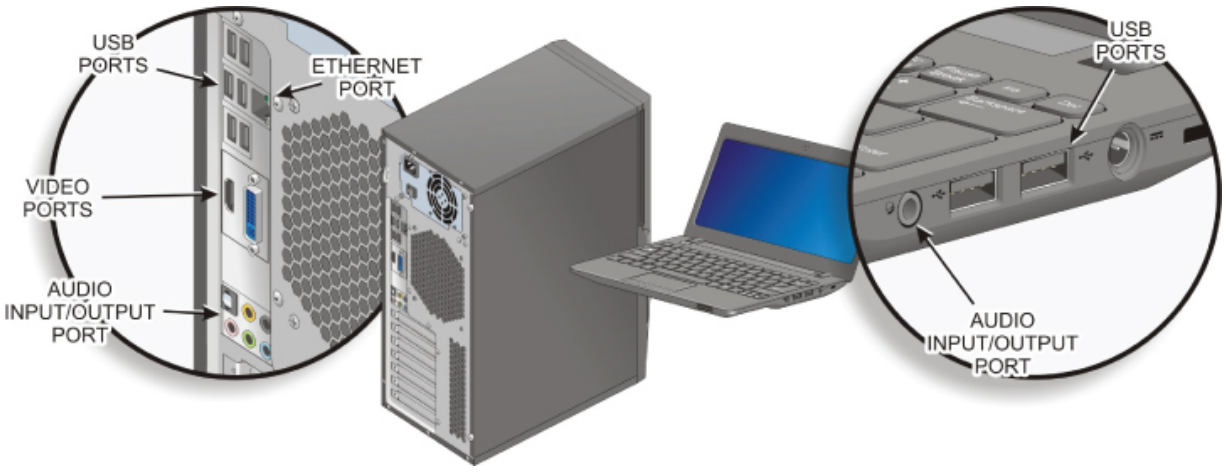


FIGURE 7.6 Physical PC Ports

Hardware ports provide access to the computer's internal communications buses that link all of its internal components,

including its data bus, memory, and internal storage devices (the three areas listed for gaining access to programs and data). Figure 7.7 depicts the layout of a typical PC's internal bus structure. The only component standing between someone with physical access to the port connection and the system's internal structure is the bus controller interface that is part of the computer's internal chipset. The operation of this circuitry is controlled by the system's BIOS and operating system.

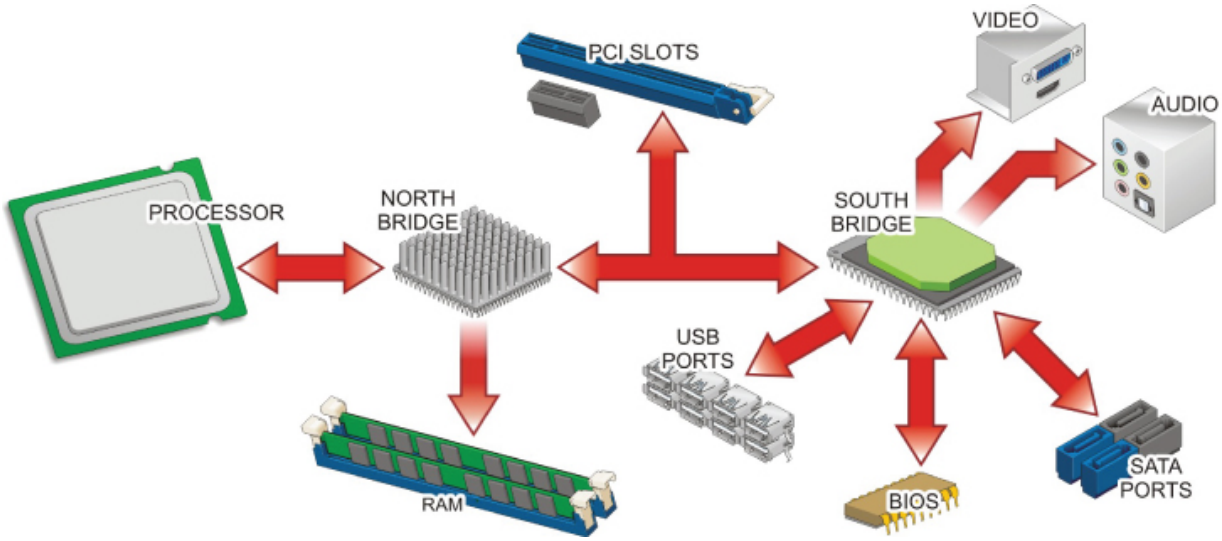


FIGURE 7.7 Pathways to the Vital Components

A CLARIFICATION OF THE WORD *PORT*

Be aware that the term *port* is also used to refer to logical TCP/UTP software ports used in computer network communications. You will encounter this version of the term shortly when you are introduced to firewalls.

Data can be downloaded into removable media devices through these ports and quickly carried away. Likewise, malicious programs, such as viruses and worms that you will be introduced to later in

this chapter, can be uploaded into the machine from the removable media source. Once these programs have been introduced to the host system, they infect it and can damage or destroy data and programs stored on it.

SECURING CONNECTION POINTS

A PC may possess several different hardware connection points. Not all of these connections pose a security threat. Only those connection ports that provide access directly to the system's internal bus structure need to be considered. For example, a standard VGA video port is an output-only connection that does not provide access to the system's internal operation.

The most widely used hardware connection ports in newer PCs are USB ports. However, you may still encounter older legacy ports such as IEEE 1394, RS-232, and RS-485 serial communication ports, as well as parallel printer ports and eSATA ports if the system supports them.

SECURING NETWORK AND WIRELESS CONNECTIONS

It is also possible and common for intruders to penetrate the PC's outer perimeter and access its internal buses, memory, and storage devices through network and wireless connections. These access routes and how to secure them are discussed in detail in Chapter 12.

Universal Serial Bus Ports

The most popular hardware port found in modern personal computers is the Universal Serial Bus (USB) port, depicted in Figure 7.8. This high-speed serial interface has been developed to provide a fast, flexible method of attaching up to 127 peripheral devices to the computer.

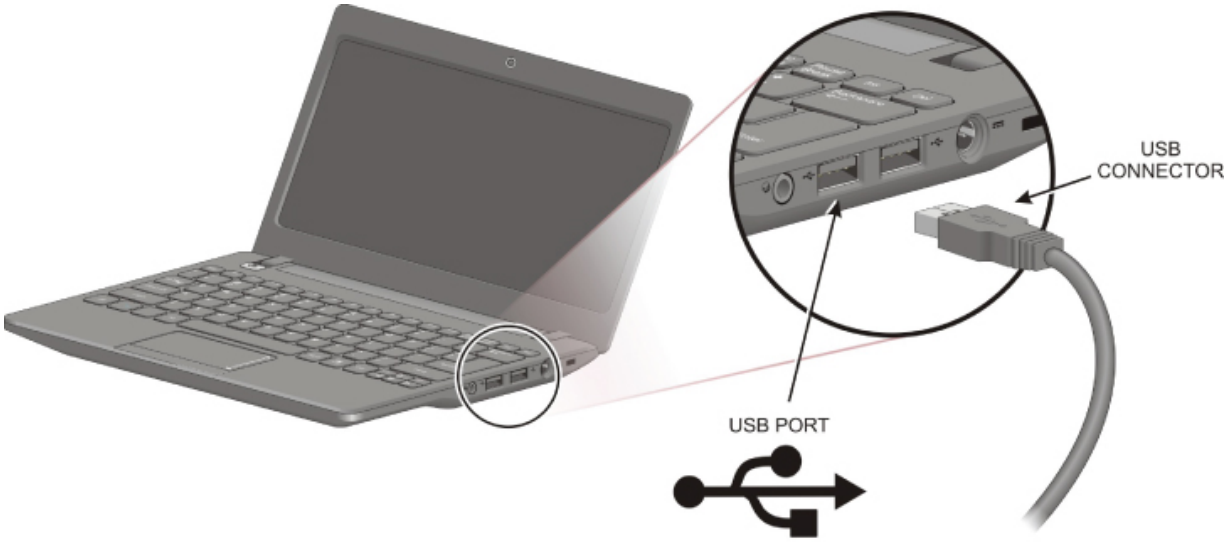


FIGURE 7.8 A USB Port

USB peripherals can be daisy-chained or networked together using connection hubs that enable the bus to branch out through additional port connections. A possible USB desktop connection scheme is presented in Figure 7.9.

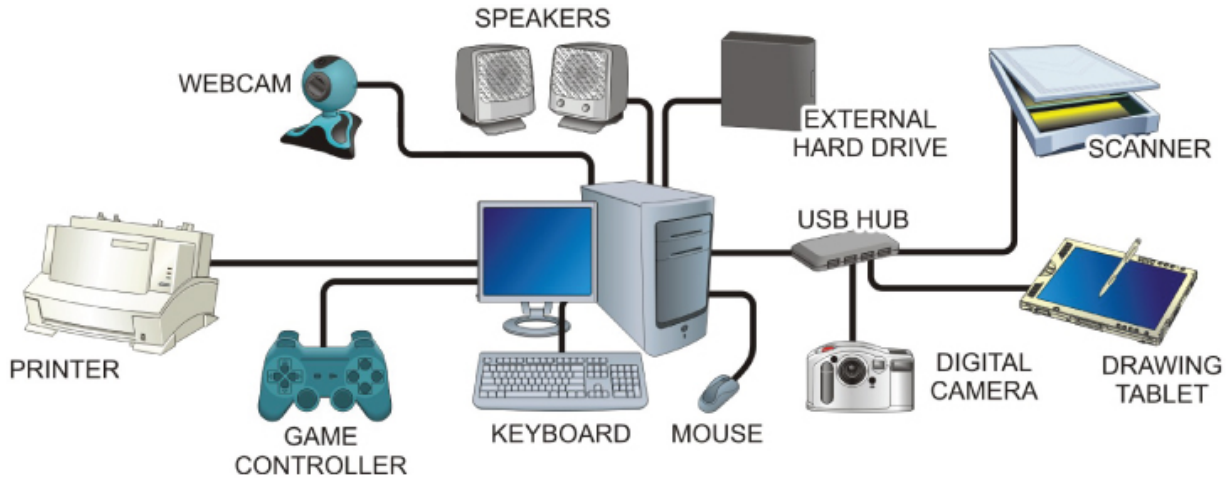


FIGURE 7.9 USB Desktop Connections

USB devices can be added to or removed from the system while it is powered up and fully operational. This is referred to as *hot-swapping* or hot-plugging the device. The Plug and Play capabilities of the system will detect the presence (or absence) of the device and configure it for operation.

The USB specification defines two types of plugs: series-A and series-B. Series-A connectors are used for devices where the USB cable connection is oftentimes permanently attached to devices at one end. Examples of these devices are keyboards, mice, and hubs.

Conversely, the series-B plugs and jacks are designed for devices that require detachable cabling (printers, scanners, and modems, for example). Both are four-contact plugs and sockets embedded in plastic connectors, as shown in Figure 7.10.

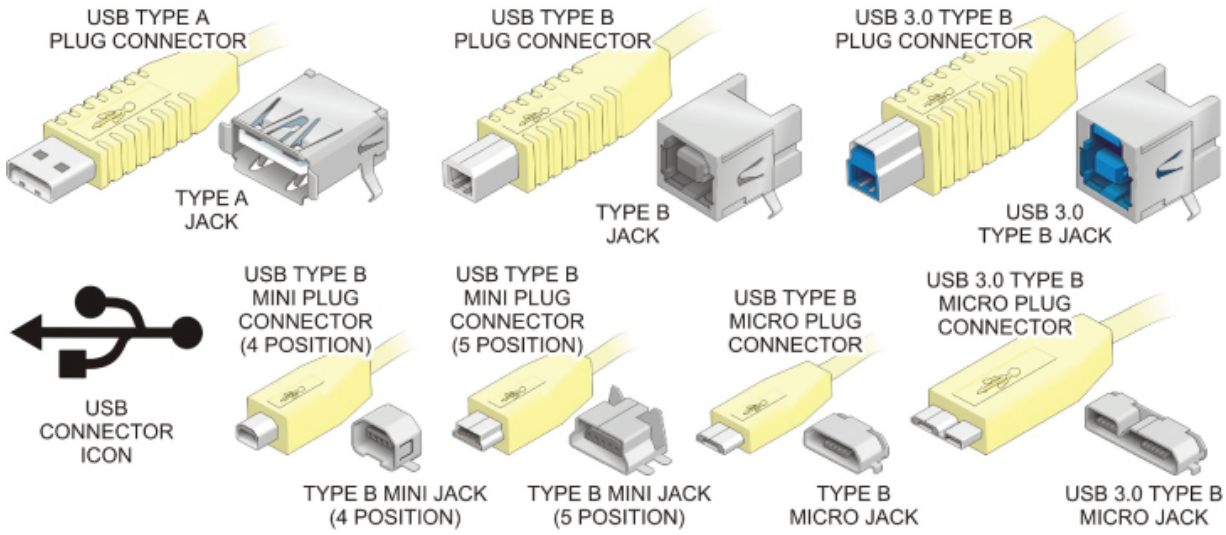


FIGURE 7.10 USB Connectors

Smaller 5-pin USB plugs and jacks (referred to as Mini-A and Mini-B) have been developed for the USB 2.0 and 3.0 specifications, and an even smaller Micro-USB connector version has been developed for the 3.0 version. USB 3.0 plugs are commonly blue in color. These connectors are intended for use with smaller devices such as digital cameras and cell phones. These structures are designed to provide rugged connections that are not prone to damage from repeated or incorrect usage.

The connectors for both series are keyed so that they cannot be plugged in backward. The connectors are designed so that the A- and B-series connections cannot be interchanged.

USB devices can be quite small and are easy to conceal and transport. Therefore, they provide an excellent vehicle for injecting malicious software into local host computers and intelligent control devices that might be very well protected from network access. For this reason, it is very important to control access to USB ports on the computer, as well as to control the reasons for which individual users can use the ports.

In the case of USB ports built into the computer's motherboard, the operation of the port connections is controlled by settings in the motherboard's CMOS Setup utility. For the security reasons cited

previously, it may be necessary to access the CMOS Setup utility to disable its USB function.

IEEE-1394 FireWire Bus Ports

The FireWire (or IEEE-1394) bus specification is similar to USB in that devices can be daisy-chained to the computer using a single connector and host adapter. PCs most commonly employ a PCI expansion card to provide the FireWire interface.

While AV equipment typically employs 4-pin 1394 connectors, computers normally use a 6-pin connector, with a 4-pin to 6-pin converter. Figure 7.11 depicts the FireWire connector and plug most commonly used with PCs.

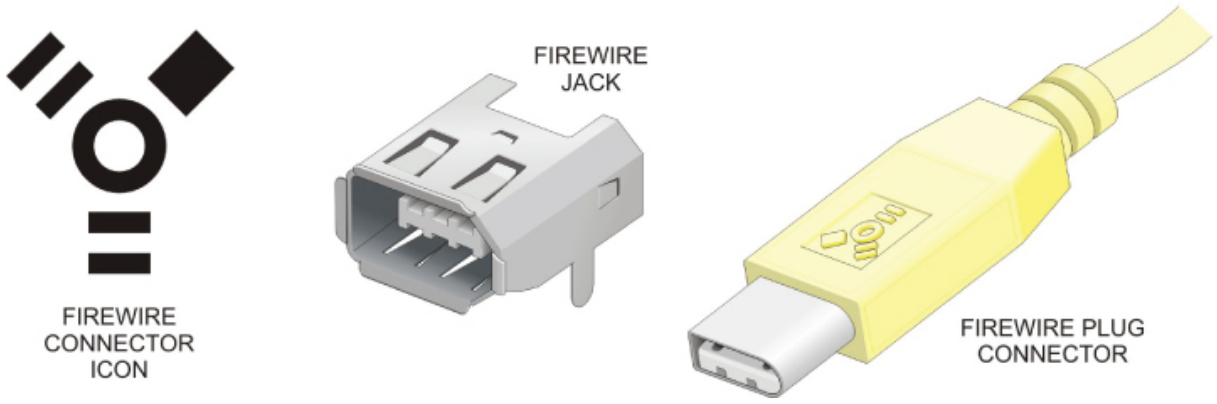


FIGURE 7.11 FireWire Plug and Connector

eSATA Ports

External SATA (Serial AT Attachment), or eSATA ports, are physical interfaces that link eSATA-compatible device with the system's internal SATA bus. This bus is the standard bus for connecting disk drive units to PC systems.

Figure 7.12 illustrates the implementation of a typical eSATA interface port. A shielded eSATA cable connects an external drive unit to the eSATA hardware port mounted on an expansion slot cover. Internally, a standard SATA cable connects the port to a SATA connector on the motherboard.

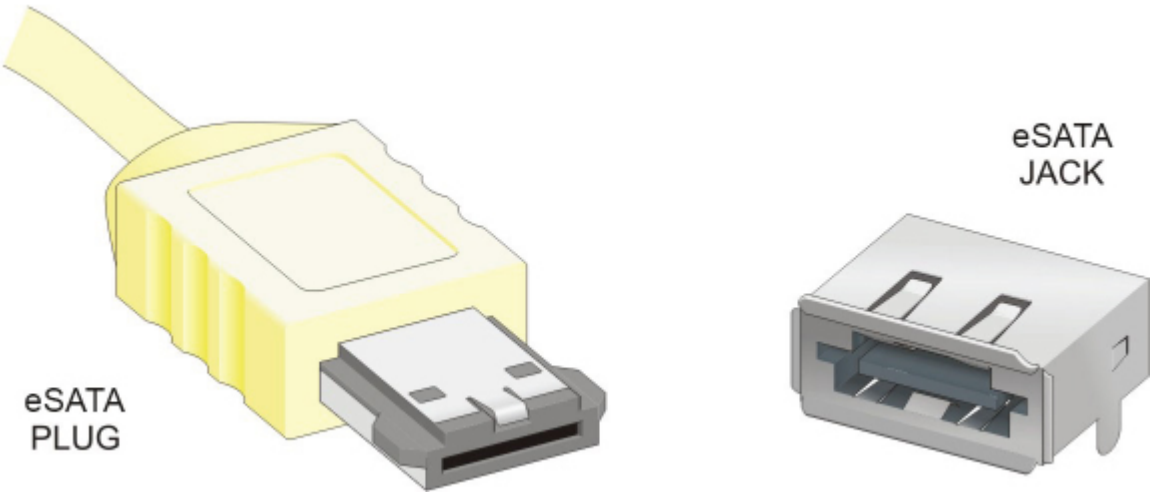


FIGURE 7.12 eSATA Interface Connections

Because these ports provide direct access to the buses that connect the disk drives to the system, they pose a security concern.

Legacy Ports

There are some older legacy hardware ports you might not encounter too often. Table 7.1 summarizes the physical port types used with PCs. They are most often located on the back of the PC, but some models may feature some of these ports on the front panel for convenience. The physical appearance of these ports is described in Figure 7.13.

TABLE 7.1 Typical and Legacy I/O Ports

Port	Connector
Keyboard	PS/2 6-pin mini-DIN
Mouse	PS/2 6-pin mini-DIN
COM1	DB-9M
COM2	DB-9M
LPT	DB-25F
VGA	DE-15F (3 row)
Game	DE-15F (2 row)
Modem	RJ-11
LAN	BNC/RJ-45
Sound	RCA 1/8“ minijacks or 3/32“ sub minijacks
SCSI	Centronics 50-pin
USB	4-pin USB Socket

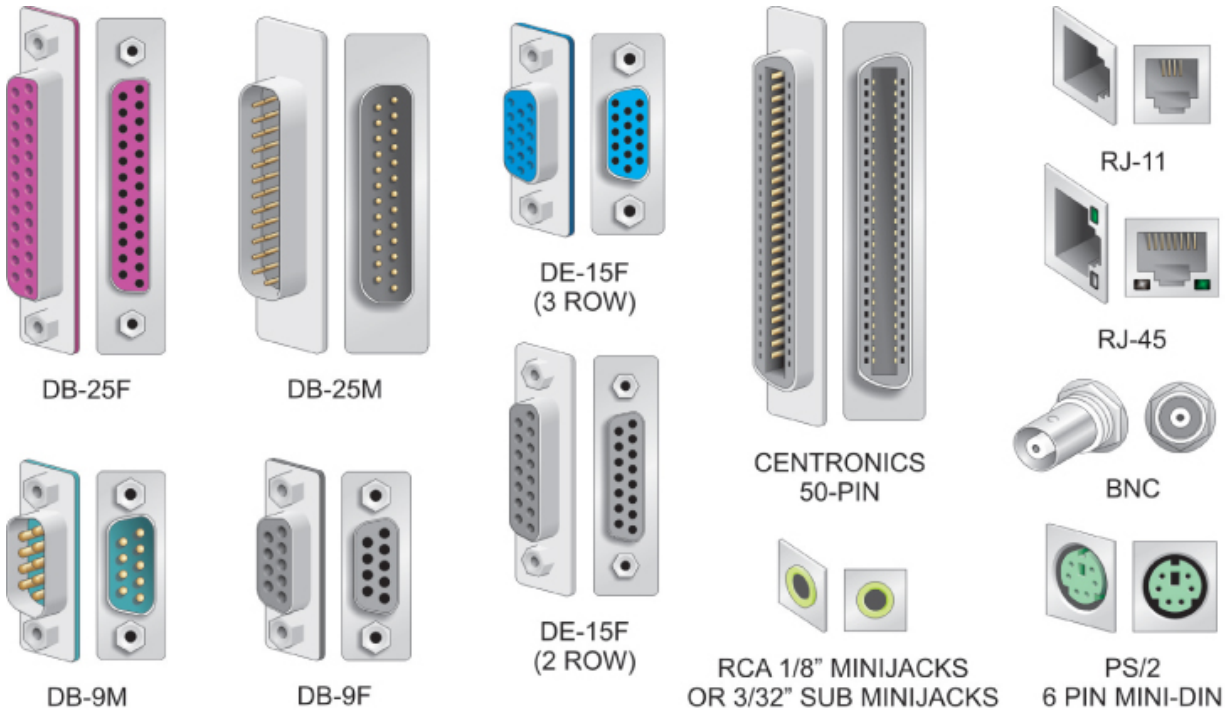


FIGURE 7.13 Typical IO Port Connectors

If you encounter these ports, the ones that pose a security risk include the RS-232/422/485 serial COM ports, Small Computer System Interface (SCSI), and the LPT parallel printer ports. These ports are all capable of handling two-way communications with the system's internal devices.

BIOS Port-Enabling Functions

It is common for a system's BIOS to offer device control options that provide control over the computer's external hardware connection ports. By disabling these ports, users and administrators can help to ensure that unauthorized users cannot use the ports to gain unauthorized access to the system, transfer information out of the system, or download malware programs into the system.

In addition to controlling access through the USB and IEEE-1394 ports, the BIOS may also offer control over serial ports, parallel ports, flash media readers, smart card slots, card bus slots, and eSATA ports, if the system possesses them, as shown in Figure 7.14.

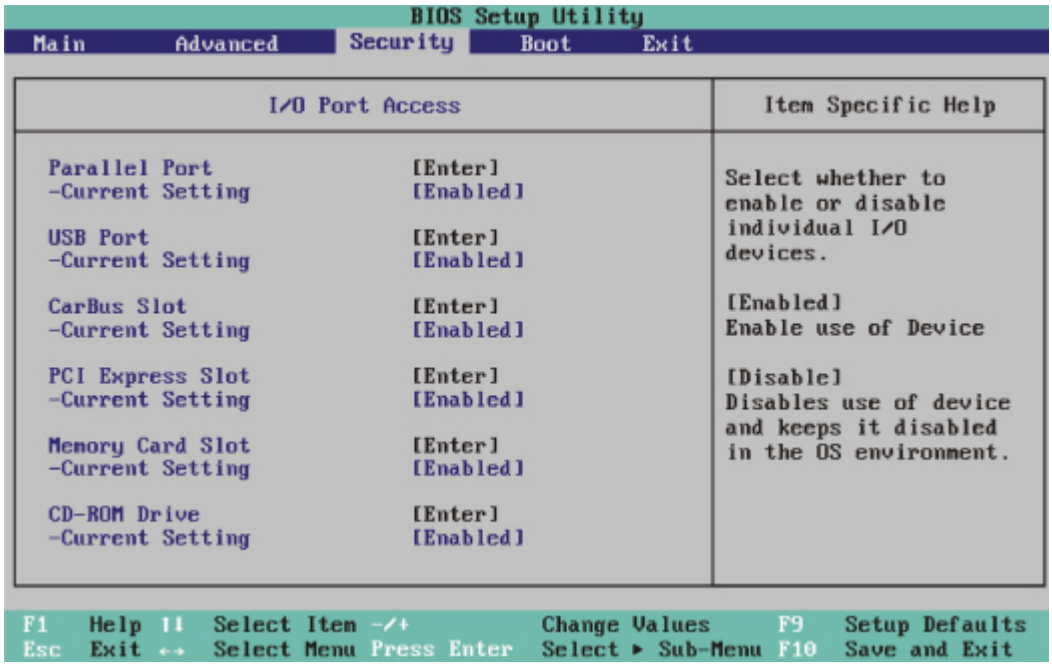


FIGURE 7.14 Port-Enabling Options

Removable Media Access

Removable computer media presents multiple security risks. These risks include potential loss of data through theft due to the portable nature of the media, as well as the potential to introduce destructive malware into the host system.

Figure 7.15 shows different types of removable media associated with PC systems. These typically include:

- Magnetic storage media such as external hard drives and backup tapes
- Optical storage media such as CD and DVD drives and discs
- Electronic storage devices such as USB flash or thumb drives, MMC memory sticks, and SD cards

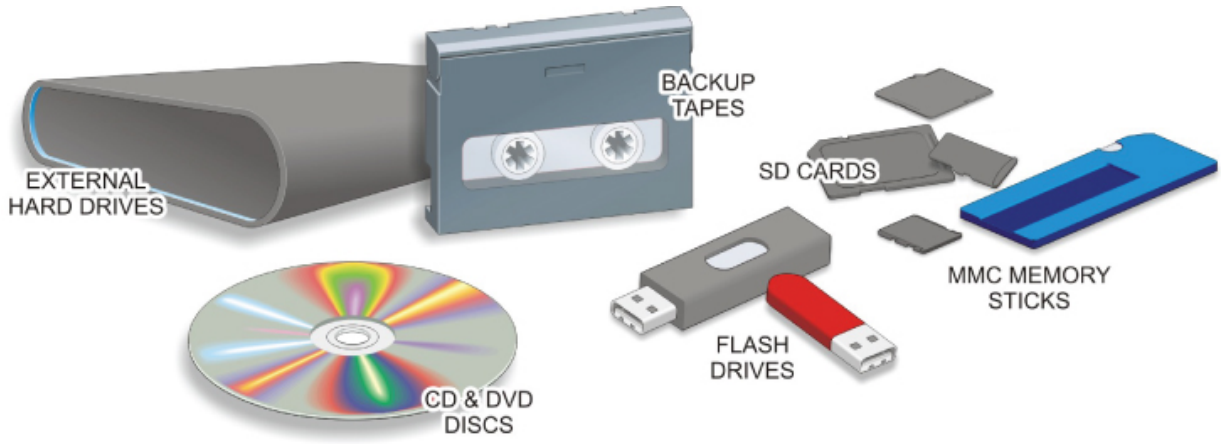


FIGURE 7.15 Removable Media

All three of these media device types provide access to the computer's internal system through its drives and hardware connection ports.

BIOS Boot Device/Sequence Controls

Most BIOS provide boot device enabling, disabling, and sequencing functions that should be used to control the circumstances of how the computer can be booted up for operation. Typically, the BIOS offers users and administrators the option to enable or disable the following types of devices:

- Optical disc drive(s)
- Hard disk drive(s)
- USB devices
- SD cards
- eSATA devices

Unless it is necessary to routinely boot the system from other devices, all boot options except the primary hard disk drive option should be disabled to provide the best security option.

Microsoft Autorun Feature

Similarly, some versions of Microsoft's operating systems include a featured called Autorun that automatically runs executable programs found on removable media devices as soon as it detects the presence of the media in the drive or reader. This feature provides a very serious security threat as malware programs located on the media will run automatically and infect the host device.

This feature is blamed for up to 50 percent of all malware infections in older Windows systems. The threat can be removed simply by disabling the Autorun feature in Windows by downloading an app to turn off Autorun. The other alternative is to modify the Windows Registry to turn off Autorun.

Hands-On Exercises

In this lab, you will examine the settings available in BIOS. First, you will find and examine the USB port control. Then you will examine the Administrator and User-access BIOS settings. Finally, you will examine various options in the boot menu, including boot order and Secure Boot.

Objectives

- Enter the BIOS.
- Navigate the BIOS.
- Find the settings to improve system security.

Procedure

1. Turn off the PC workstation.

   Pay attention to the workstation monitor when you turn it on in the next step. When you see the motherboard or computer manufacturer, there should be an option at the bottom of the screen. It will instruct you on how to enter the BIOS. Frequently used buttons include F2, F10, and Delete. The actual button you need to use will depend on the motherboard manufacturer; therefore, it is important to pay attention to the instructions on the screen.

Record the button you need to use on the following line:

2. Turn on the PC workstation. Attempt to enter the BIOS by pressing the correct button. If you are unsuccessful, turn off the workstation and try again.

NOTE

You may be prompted to repeat the required keystroke multiple times.

BIOS menu interfaces differ greatly among system manufacturers and motherboard vendors. Figure 7.16 is merely an example.

FIGURE 7.16 Sample BIOS Initial Settings Screen

The lab may end right now if your BIOS settings have already been password-protected by a system administrator. If this happens, the lab is over and you have one of three options to proceed:

a. Skip to the end of the chapter and answer the questions as best you can.

b. Try to get the administrator password to unlock and clear this setting.

c. If capable, you may have a jumper to reset the CMOS to factory defaults and clear the password. (Option C should be executed only by a competent technician.)

3. If your lab didn't end, use the arrow keys to navigate the menus. Press Enter to select a highlighted option. You can also use the Tab key if you are unable to highlight a desired option. Navigate

to Advanced Mode or your equivalent. See Figure 7.17 and Figure 7.18.

FIGURE 7.17 Advanced Mode Highlighted

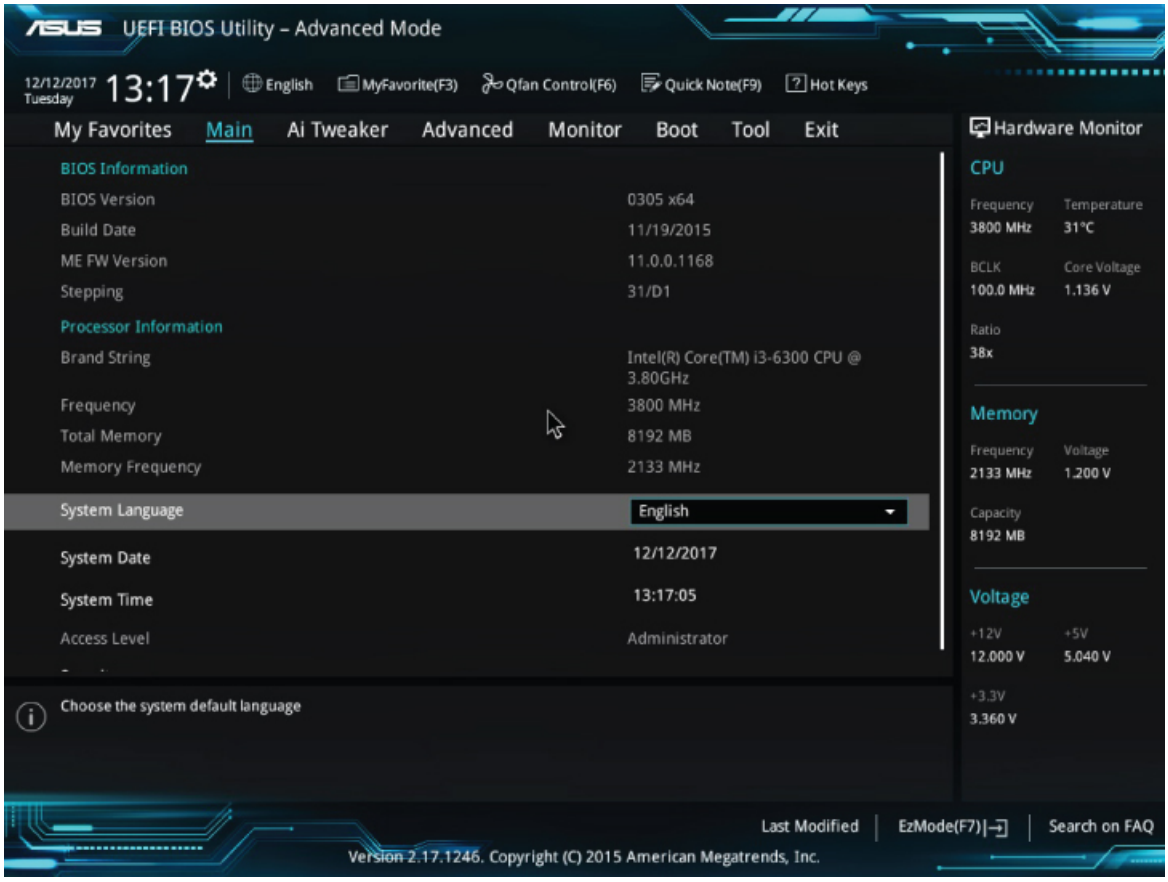


FIGURE 7.18 Advanced Mode Initial Menu

4. Figure 7.19 shows USB Configuration highlighted. Look for a menu or setting option like this.

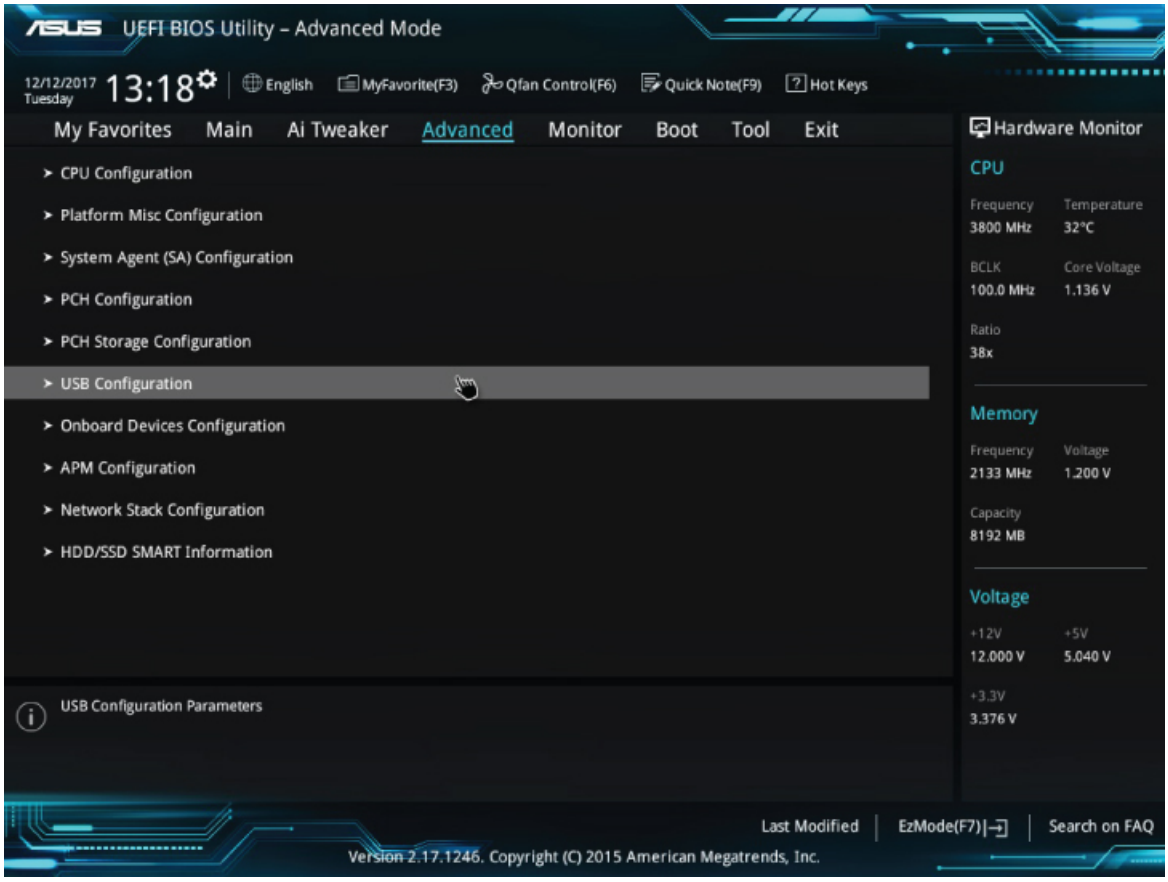


FIGURE 7.19 USB Configuration

5. From here, there should be some options. Look for an option that most closely matches USB Single Port Control (see Figure 7.20). This option could have a different name for your BIOS settings. Figure 7.21 shows where to enable or disable the USB ports.

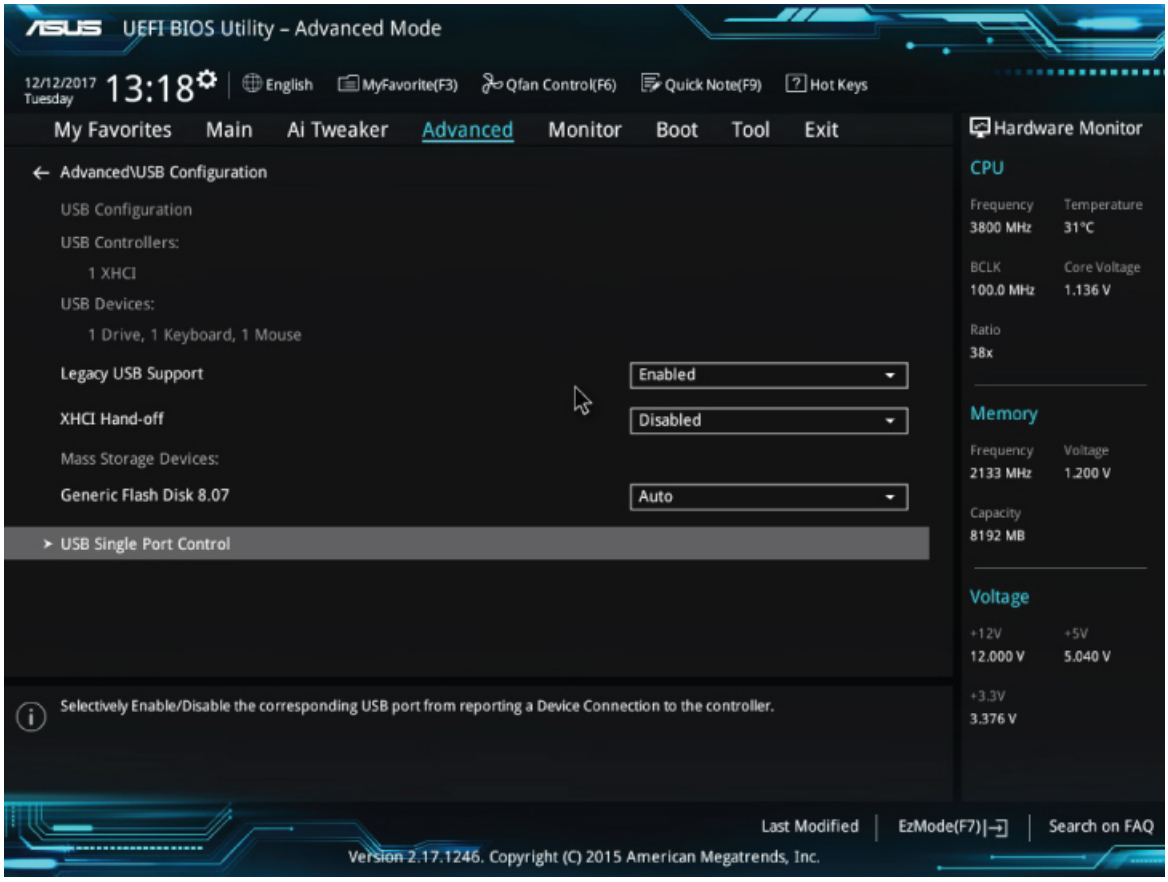


FIGURE 7.20 USB Single Port Control

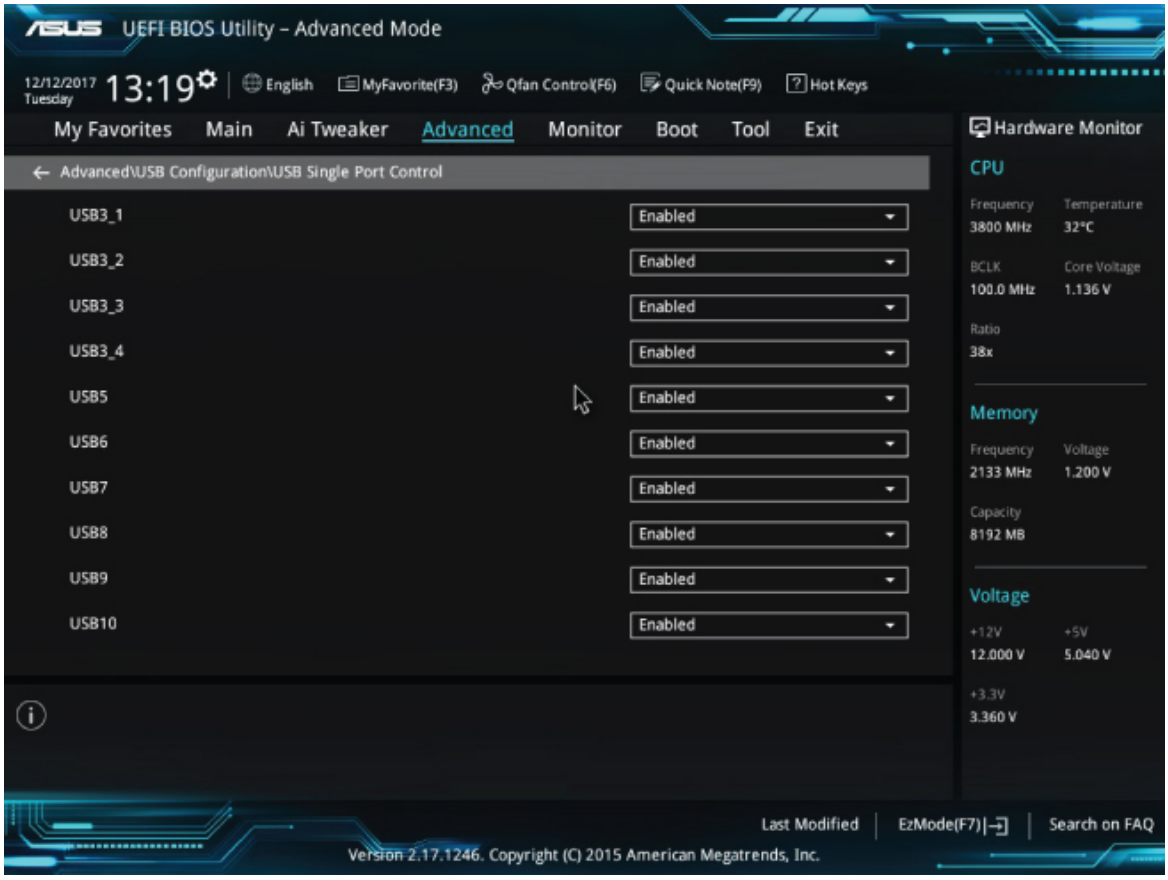


FIGURE 7.21 Enable or Disable USB Ports

6. Find a setting that lets you set up Administrator or User passwords for the BIOS. Do not change these settings. Leave the passwords empty. In this case (see Figure 7.22), the setting is simply labeled Security under the Main settings. Figure 7.23 shows the BIOS Administrator Password and the User Password settings.

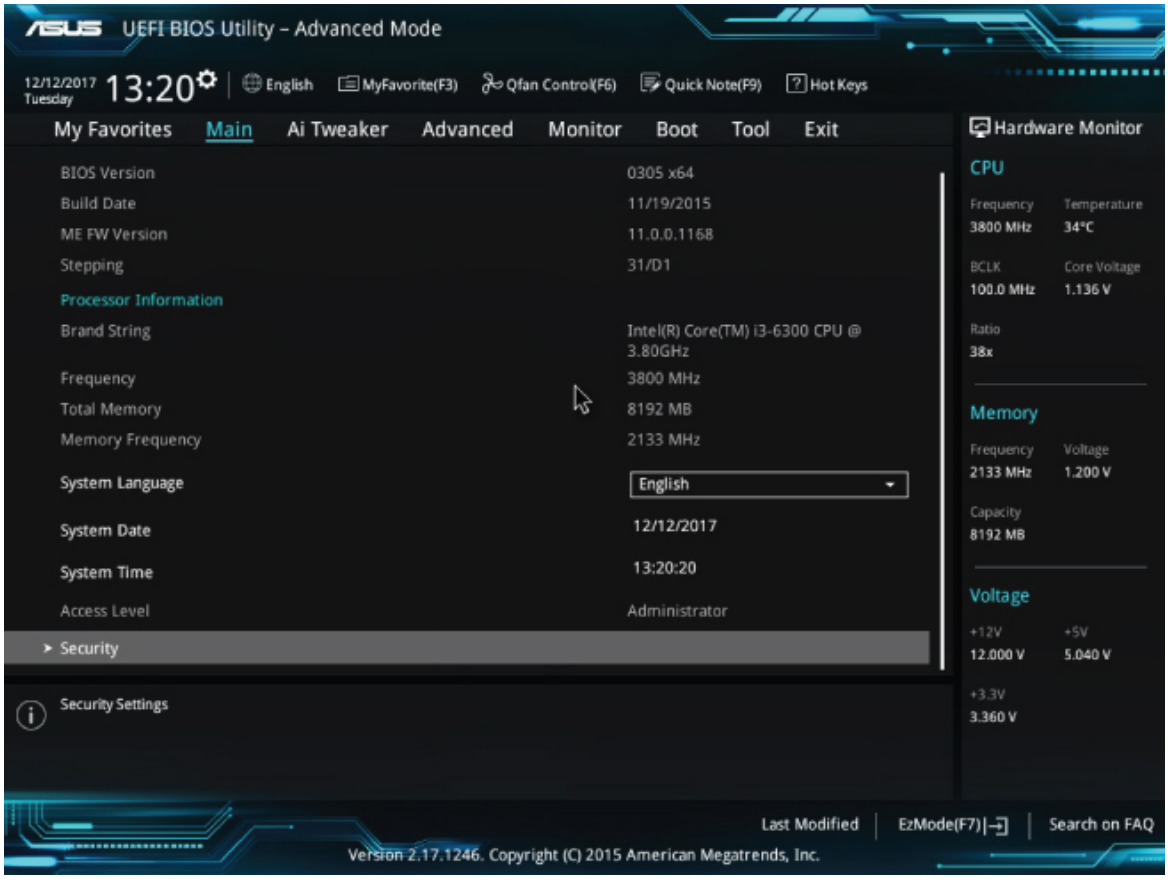


FIGURE 7.22 Security Settings

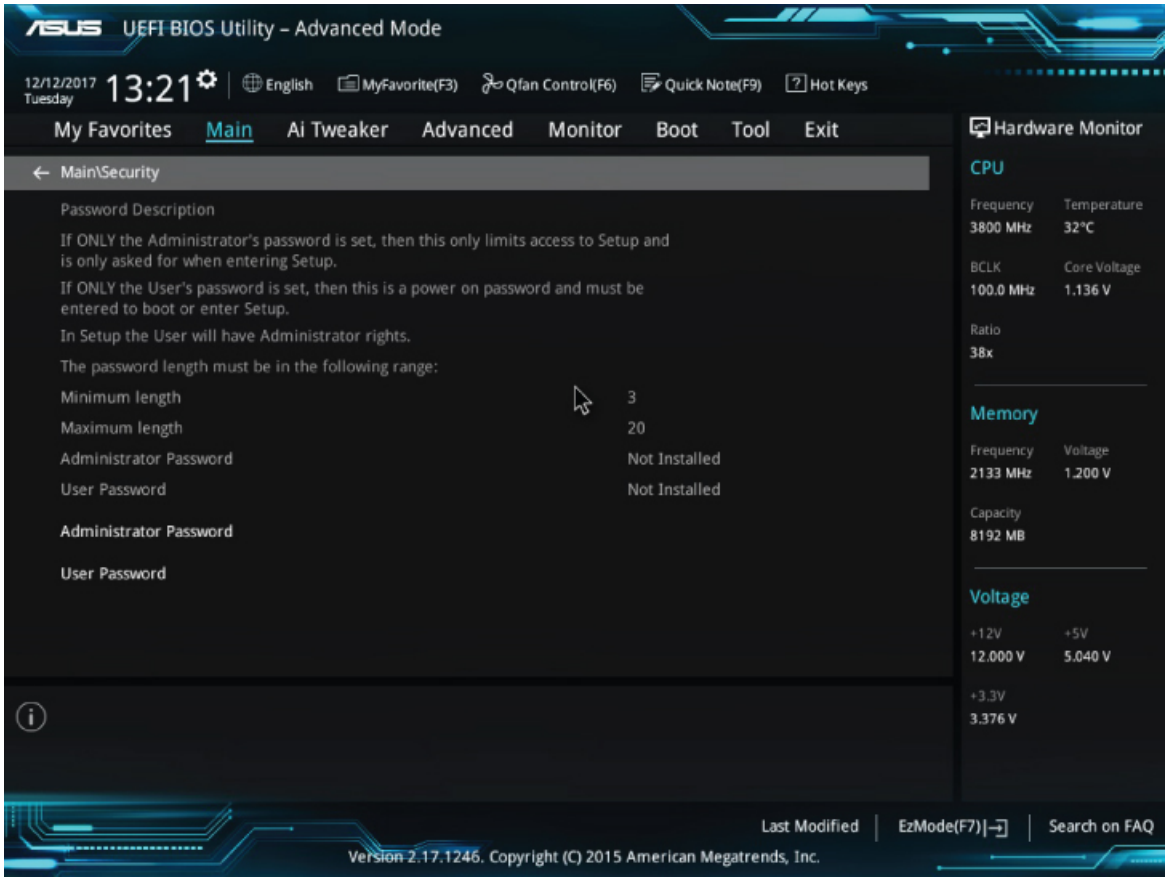


FIGURE 7.23 BIOS Administrator and User Password Settings

7. Navigate to the boot menu (see Figure 7.24). The boot menu lets you configure various settings related to system boot up.

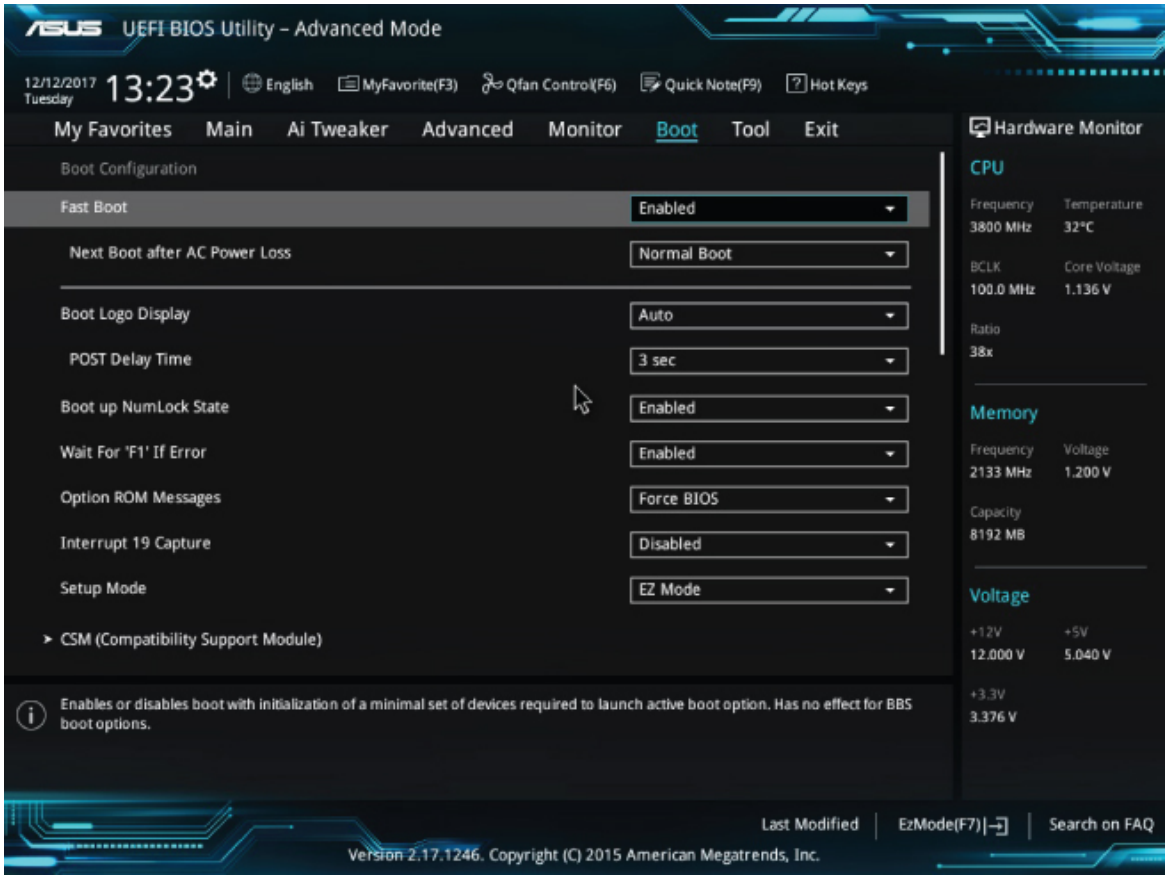


FIGURE 7.24 Boot Menu

8. Find the setting that controls the boot order (see Figure 7.25). For these BIOS settings, the boot order settings were about halfway down the boot menu. Each number corresponds to the order in which the motherboard will attempt to boot.

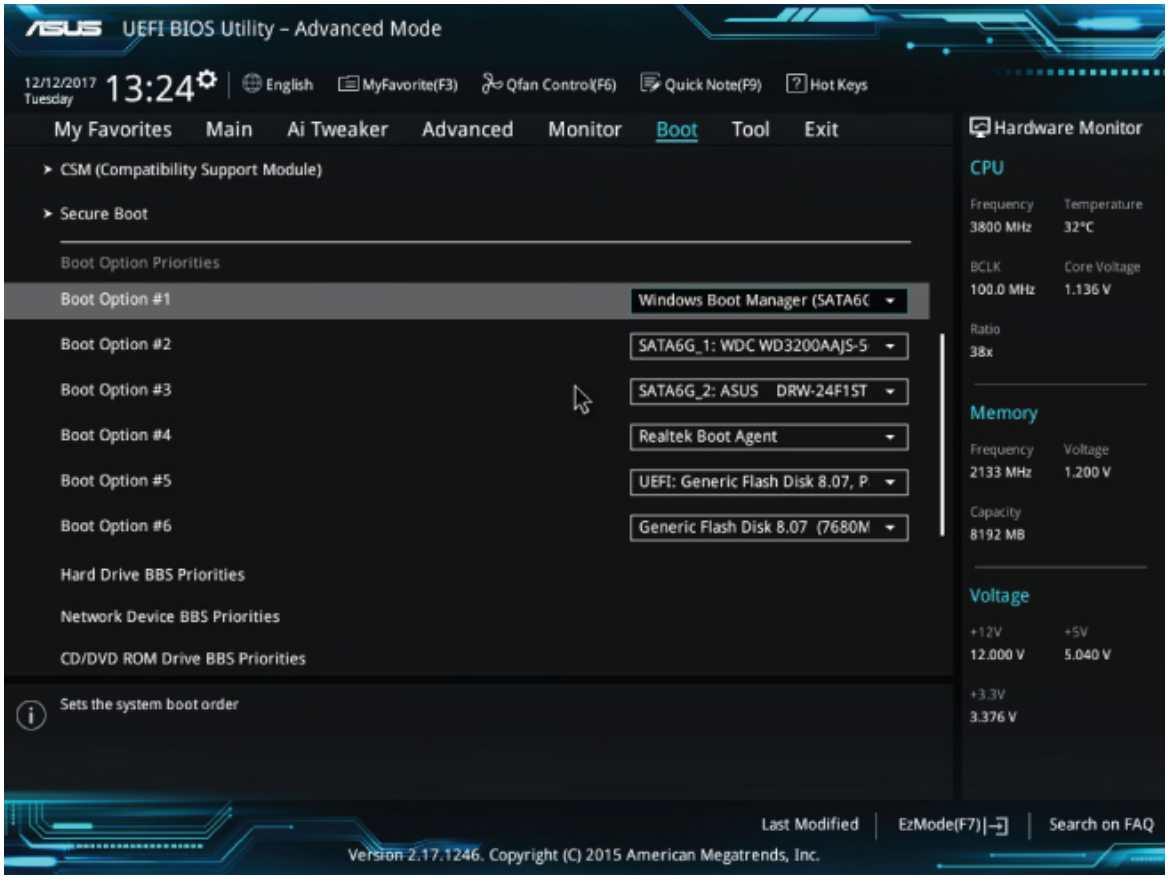


FIGURE 7.25 Boot Option #1 Attempted to Boot First

9. Find the Secure Boot option (see Figure 7.26). *Secure boot* is a relatively universal term, so you can look for these words, and you will most likely find the same option.

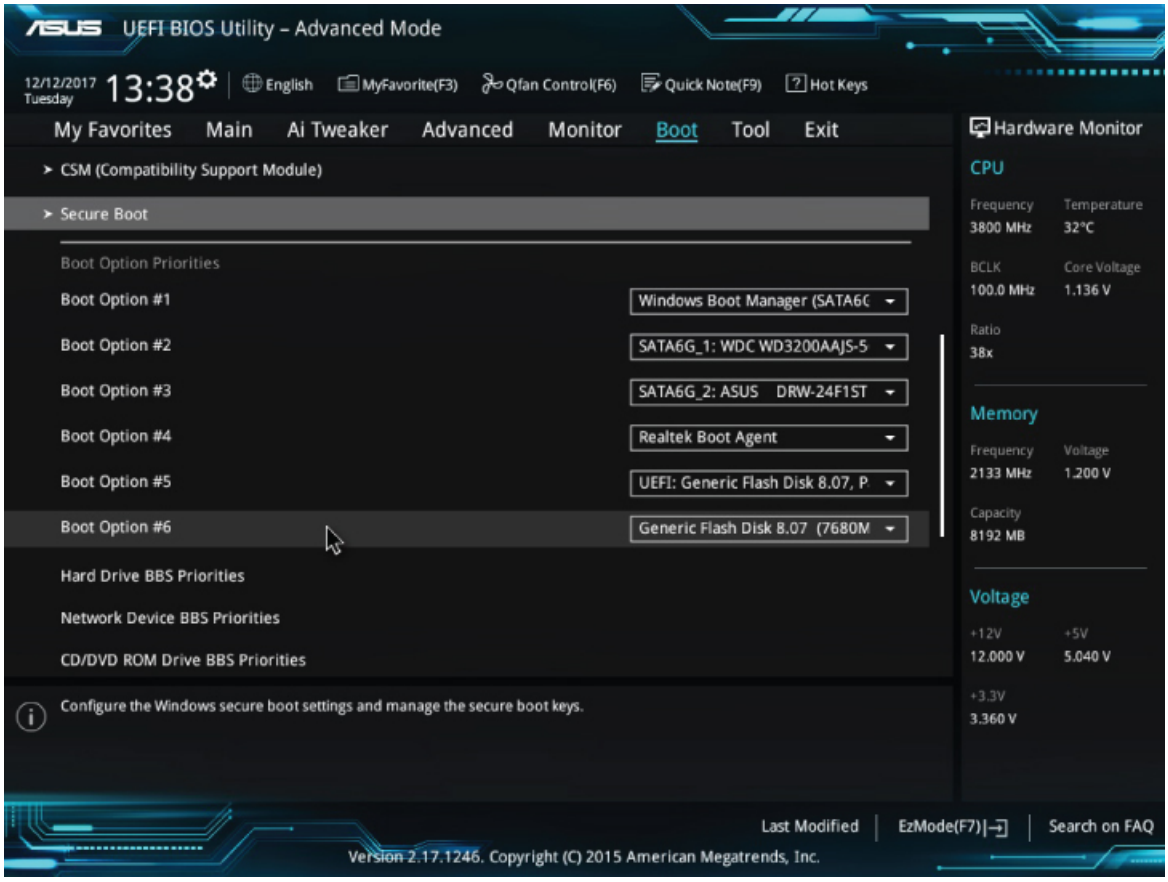


FIGURE 7.26 Secure Boot

10. Choose the option that lets you interact with your keys.
11. If possible, read any available documentation about secure boot keys. See Figure 7.27 and Figure 7.28.

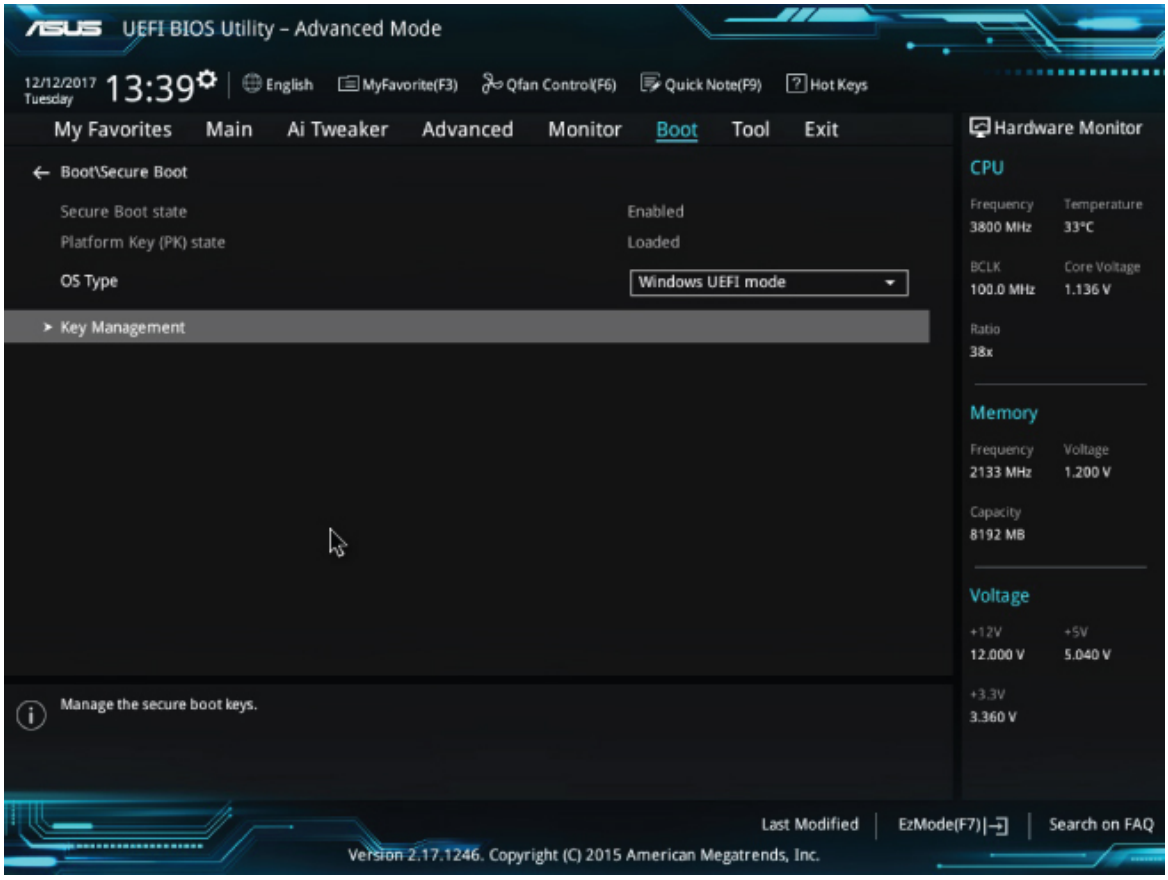


FIGURE 7.27 Key Management

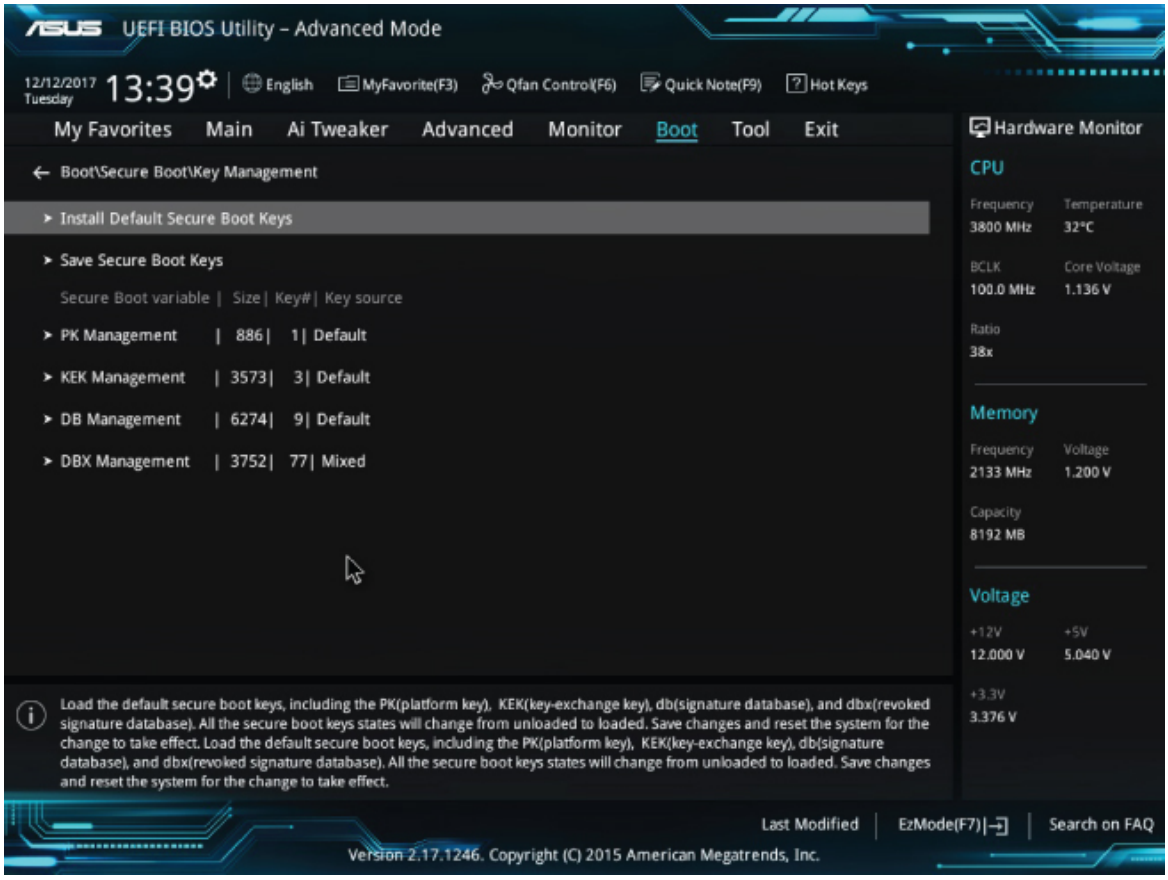


FIGURE 7.28 Key Management Settings

Review Questions

If your lab ended early, answer these questions.

1. Have you tried to visit the BIOS before this lab?
2. What was your reason for visiting the BIOS?
3. Why would you set an administrative password on your BIOS?

If you completed the lab, answer these questions.

1. Which options are available for accessing the various areas of your BIOS under your BIOS advanced settings or equivalent?
2. Where did you find the USB port settings?

3. Where did you find the BIOS Administrator and User Password settings?
4. What is the order of your boot devices?
5. What did you read about Keys in the BIOS?

NOTE

All of the answers will be specific to your particular BIOS. There are many versions and revisions of BIOS that you may be using, so simply go back through your particular BIOS and list your answers.

CHAPTER 8
Protecting the Inner Perimeter

In general, after you get past the outer perimeter defenses, you can think of the inner perimeter as part of the three-level structure illustrated in Figure 8.1. Consider this perimeter as consisting of the operating system and its application programs that form the gateway to the data stored in the interior zone (folders and files).

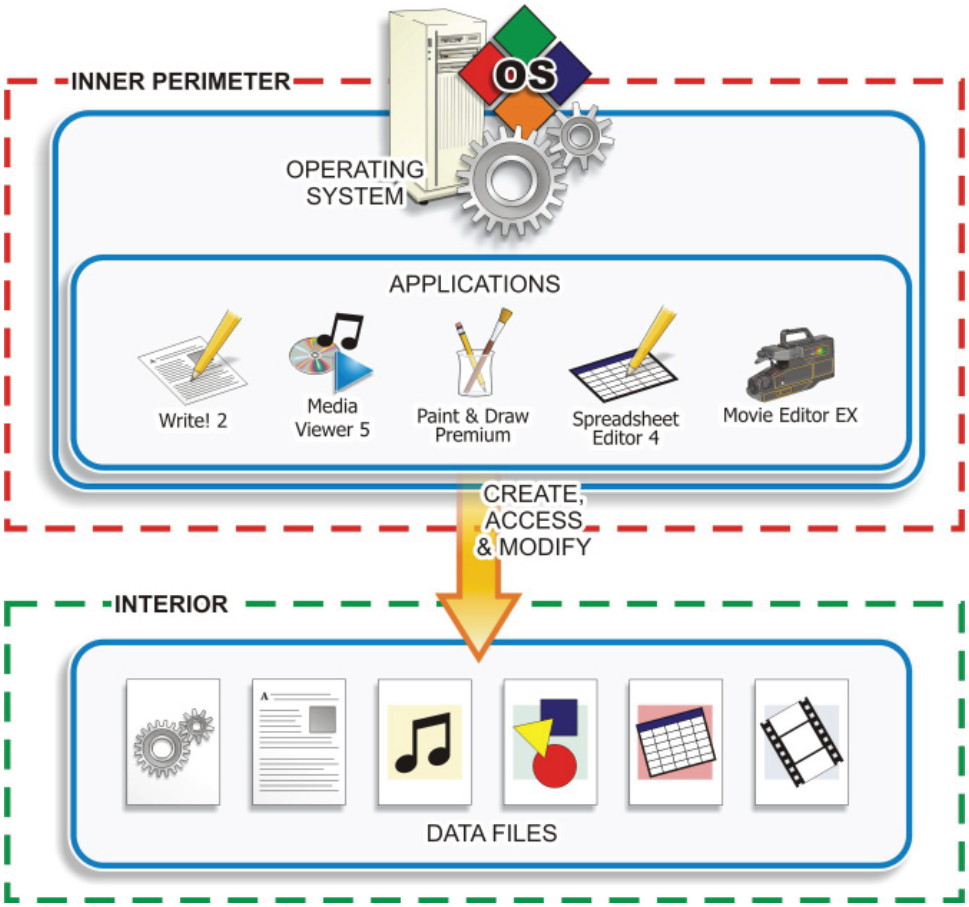


FIGURE 8.1 The Inner Perimeter

- **Describe Local Login and User Configuration Options for Host Devices.**
- **Compare and Contrast the Security Features of Common Operating Systems.**
- **Identify Common Logging and Auditing Options for Windows and Linux Based Systems**
- **Explain Options for Encrypting Data at Rest in Different OS Environments**

The Inner Perimeter

The valuable information we're trying to protect is generally the digital data stored in the computer hardware in the form of different types of files. These files are created and interpreted

by application programs. Without the application to interpret the data, it is very difficult to determine what the data actually means. See Figure 8.1.

The operation of the application program and access to the files are controlled by the operating system (OS). The operating system coordinates the operation of the hardware system and devices with the software applications. Applications are designed to run on specific operating systems, so they are dependent on those operating systems. They will not run on another operating system without some sort of translator being involved.

The operating system is also responsible for keeping track of where data is stored in the system and how it can be located and accessed. Without the operating system's file management system (FMS), there is no way to know how to find the data to steal, damage, or destroy it. Each major OS supplier uses a different FMS.

Therefore, to access data on a computer, you must gain access to the running system, which is controlled by its operating system. Then you need to be able to locate the file, which requires the ability to navigate the OS file system. Finally, you will need to open the file, which requires the application software or software designed to examine data at the digital-code level.

There is not much actual value in the operating system or common application programs for thieves to steal. These types of software are commonly available, relatively inexpensive, and hard to transfer and use between systems. These programs are basically just tools for creating and manipulating information. However, they are interesting to would-be hackers because they can be accessed and repurposed for malicious and illegal operations.

On the other hand, the data files stored on the computer can be very interesting to thieves. As you are no doubt aware, quite a bit of digital information exists about most people and it is all stored on computers somewhere. If someone can locate and gain access to those data files, they can find a way to extract the information from them.

Once they have access to the file (or a copy of it), they can either open it on their system using the same application originally used to create the file, or they can extract the information from the digital code. The latter tends to be somewhat more involved and difficult to accomplish and typically requires someone with hacker skills and tools to operate at that level.

However, not every malicious operator wants to steal information. Some people, organizations, and governments just want to damage or destroy data for one reason or another. This type of activity could arise from many different motives, as described in the Introduction to this book

So how do you keep unwanted persons from gaining access to these programs? Let's first look at typical operating systems from different suppliers and see what security options they offer. As you will see in the following sections, operating systems tend to have many security tools and options built into them.

Operating Systems

Operating systems are programs designed to control and coordinate the operation of the computer system. As a group, they are easily some of the most complex programs ever devised.

In all microprocessor-based environments, the operating system accepts commands from a program or an input source (such as a computer user) and carries them out to perform some desired operation. Likewise, the operating system acts as an intermediary between nearly as complex software applications and the computer hardware they run on.

SOME CLARITY ON OPERATING SYSTEMS

Unless the display has input capability, it is not considered to be an access device that can be exploited. The same holds true for printers or other output-only devices.

The most widely used operating systems in the world have nothing to do with personal computers. These operating systems are found in automobiles and consumer electronics products. They receive input from sensing devices such as airflow sensors (instead of keyboards and mice), process a control program according to a set of instructions and input data, and provide output to electro/mechanical devices such as fuel injector pumps (not video displays and printers). They also don't have much to do with disk drives.

A disk operating system (DOS) is a collection of programs used to control overall computer operation in a disk-based system. These programs work in the background to allow the user of the computer to input characters from the keyboard, to define a file structure for storing records, or to output data to a monitor or printer. The disk operating system is responsible for finding and organizing your data and applications on the disk.

As illustrated in Figure 8.2, the disk operating system can be organized according to four distinct sections:

- *Boot files* take over control of the system hardware from the ROM BIOS during start-up. They bring the OS kernel files into RAM memory so they can be used to control the operation of the system.
- *Kernel files* are the fundamental logic files of the operating system responsible for interpreting commands obtained from software programs for the central processing unit. These files are created to work with specific hardware architectures (microprocessors and chipsets).
- *File management files* enable the system to manage information within itself. These files are responsible for storing, tracking, and retrieving data into RAM memory where the microprocessor can access it.
- *Utility files* are programs that permit the user to manage system resources, troubleshoot the system, and configure the system.

FIGURE 8.2 Basic OS File Structure

The operating system acts as a bridge between application programs and the computer hardware, as described in Figure 8.3.

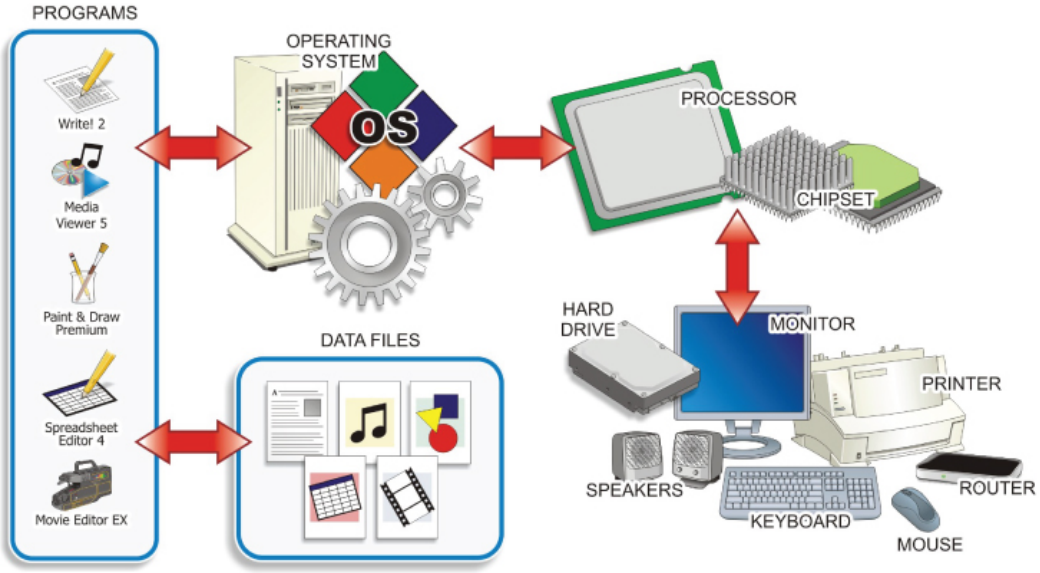


FIGURE 8.3 The Position of the OS in the Computer System

These application programs enable the user to create files of data pertaining to certain applications such as word processing, multimedia delivery, remote data communications, business processing, and user programming languages.

Because the operating system is a major part of the electronic gateway to the computer's applications and data, you must be aware of the different general types of OS available and what tools and techniques are available to protect them. For this discussion, let's divide computer operating systems used with computing and intelligent control devices into three general classes by the roles they fill:

- *Standalone operating systems* – These are operating systems that can be operated independently without external communications or management. This class of operating system includes different Windows, Mac, and Android-based versions found on consumer computers. However, this designation can also apply to the operating systems used in many intelligent control devices employed in industrial and manufacturing applications.

While these OS versions may be operated in a standalone manner, most modern versions possess some networking abilities that allow them to communicate with other intelligent devices or the Internet.

- *Client operating systems* – Client operating systems are designed to work in a network environment. In particular, they are designed to take advantage of the services provided by a master computer called a *server*. While server computers are responsible for providing oversight and control of the client computers through their various networking services, users do not commonly work at these computers. Instead, the client computers and devices serve as workstations, or autonomous nodes. Network clients are divided into three general subcategories:
  - *Thick clients* – These are fully functioning PCs and devices that could work locally but rely on the services delivered by the network server(s). Data is typically stored locally on a thick client.
  - *Thin clients* – These are fully functioning PCs and devices that don't possess hard drives for storage. The operating system is simply used to start the system up and then hand the operation off to a server. All data and programs are stored and executed on the server.
  - *Terminal clients* – These are server-dependent PCs and devices where the operating system does not exist on the client. Instead, the client actually boots up to a remote server and all programs and data are located and executed on the server.
- *Server operating systems* – These operating systems are designed to run on specialized server computers that function as the center of a client/server network environment. Server operating system versions are typically responsible for:
  - Data and resource security for the network and its devices
  - Centralized network administration
  - Cost benefits to the business or enterprise
  - Server operating systems provide security for the network and its clients by controlling access to:
    - Resources (disk drives, printers, directories, and files)
    - Services (email, Internet connectivity, messenger services, databases, and so on)
    - Administrative tools (user accounts, local and network utilities, computer management tools)

NETWORK OPERATING SYSTEMS

Network Operating Systems (NOS) are designed to extend the control of disk operating systems to provide for communications and data exchanges between computers connected by a communication media. Notable network operating systems include Windows Server OS versions, Linux Server distributions, and Unix.

Server operating systems are some of the primary tools responsible for security in a network environment. These operating systems and their security tools are explored in depth in Chapter

14. The remaining sections of this chapter deal with security tools that are available and can be implemented at the local standalone or client computer level.

Notable standalone, or client disk operating systems, include: Microsoft Windows versions, Apple Computer's MAC OS X, a variety of Linux operating system distributions, and the Android operating system from Google.

Operating systems and the programs and data they control are attacked from two common areas:

- By manipulating the operation of the OS kernel
- By attacking its file management system

The following sections address these two common areas of attack.

OS Kernel Security

Figure 8.4 illustrates the position of the OS kernel between the system's hardware and applications. Due to this positioning, it should be apparent that if you can get to the programming code in the OS kernel and disable it, you have disabled the operation of the entire computer system. However, if you can access the kernel and manipulate the code, you have taken over operation of the computer.

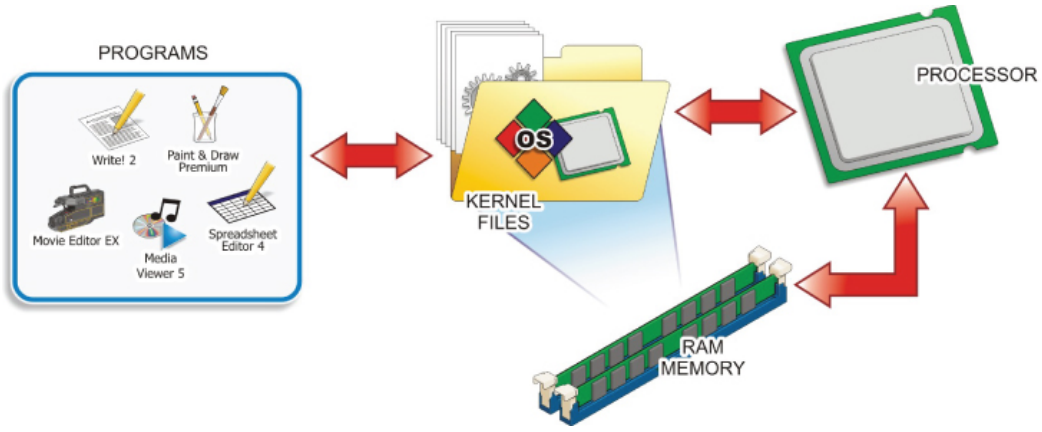


FIGURE 8.4 The Position of the Kernel

Attackers who possess enough knowledge of a given operating system's memory-handling strategy can exploit the OS kernel in a number of different ways:

- They can change the value of a variable in the kernel programming to change its behavior.
- They can change the return address of some standard OS function so that when the OS tries to return to its basic pipeline of instructions, it is rerouted into code supplied by the attacker.
- They can change a pointer in the program that directs the execution of the instruction code to an exception handler supplied by the attacker.
- They can insert malicious code into an application's code that has been loaded into RAM memory for execution. The inserted code is designed to overwrite kernel components that interact with the application.

All of these attacks rely on gaining access to specific areas of the computer's memory where the OS kernel operates.

Most operating systems utilize a feature built into microprocessing hardware to protect certain areas of memory that contain specific blocks of instruction code. This feature is referred to as the *No eXecution (NX) bit,* or the eXecute Disable (XD) bit. NX bit technology is used to flag certain areas of memory as storage-only.

Any section of memory marked with the NX attribute means it's only for storing data. Therefore, processor instructions cannot be stored there. This is a popular technique for preventing malicious software from taking over computers by inserting their code into another program's data storage area and then running that code from within this section, as they would with a buffer overflow attack.

Some operating systems ship with built-in executable-space-protection features, referred to as Data Execution Prevention (DEP) modes, to defeat these types of attacks. The operating system accomplishes this by creating unique, isolated memory regions for each application running on the machine. Each isolated memory region becomes a virtual environment managed by the microprocessor's virtual memory management module.

In Unix, Unix-like, and Linux operating systems, this function is provided as an advanced implementation of its standard `chroot` operations (its system for creating and managing multiple virtualized copies of the operating system).

File System Security

The *file management system* is extremely important in protecting the existence and integrity of data stored on a hard drive or removable storage device. If the file system is destroyed or becomes corrupted, the data becomes inaccessible and is lost. In addition, if unauthorized users are given access to the file system and its stored data, they have been given the opportunity to damage, destroy, or steal it.

One of the main tools for protecting the file system and its data is the use of access control lists (ACLs) to provide Resources Access Control. The file management system uses ACLs to grant or deny specific users access to its different files, as well as to control what types of activities the individual can perform once access has been granted. For example, you may be given the capability to run a file, read it, write it, or perform other actions on it under the control of the file management system.

The operating system's ACLs are also used to control access to other objects such as TCP/UDP ports as well as I/O devices. Their ACL tables maintain records that identify which access rights each user has to a particular system object.

Depending on the operating system, resource access control can be implemented in the form of Mandatory Access Control (MAC) or Role-Based Access Control (RBAC). Unix and Linux systems typically offer MAC approaches, while Microsoft's Windows platforms provide RBAC control.

POSIX (PORTABLE OPERATING SYSTEM INTERFACE)

POSIX (Portable Operating System Interface) is a set of interoperability standards developed to standardize variations of Unix and Unix-like operating systems. POSIX-compliant systems (Unix, Linux, and Apple OS X systems) support some type of ACL for managing traditional Unix file-access permissions.

In MAC versions, the operating system takes action based on the administrator's policy configuration settings to determine who can do what and to what extent they can do it. Under RBAC, the system restricts or permits access to objects based on the user's role within the organization. The RBAC structure is typically the access control method employed in large enterprises.

In Microsoft Windows environments, these capabilities are assigned to folders and files in the form of permissions. *Permissions* can also be defined as privileges to perform an action. In Unix and Linux-based systems, users are assigned *access rights* to files.

Another tool for protecting data is to encrypt it so that becomes unusable without a key to decrypt it. The encryption/decryption process can be performed on data when it's stored and retrieved from a device (PR.DS-1, data at rest) or when it is being moved from one location to another (PR.DS-2, data in motion).

THE PRIMARY CYBERSECURITY GUIDELINES

The NIST Framework for Improving Critical Infrastructure Cybersecurity specifies protection strategies for protecting "Data at Rest" (PR.DS-1) and protecting "Data in Transit" (PR.DS-2).

Most of the major disk operating systems available offer some type of data encryption capabilities through their file management systems. Depending on the design of the operating system, encryption may be applied at the device level, the disk (or volume) level, or the file and folder level. Third-party encryption applications are available for use with many of these operating systems as well.

The data encryption services available with different operating systems are discussed in the following sections. Data encryption techniques are covered in detail later in this chapter.

The following section compares and summarizes the key structural and security features of the most widely used operating systems. This comparison involves the operating system's versions, kernel architecture, file management systems, and native data-encryption capabilities.

File System Attacks

Typical attacks mounted on OS files systems include:

- Using race condition attacks
- Using data streams to hide files
- Performing directory traversals

Using Race Condition Attacks

A *race condition* exists when an attacker exploits the timing of consecutive events in a multiuser/multitasking environment to insert malicious code into the system between the events.

For example, a time of check-time of use (TOCTOU) condition exists when an operating system creates a temporary file. During the time between when the OS checks to see if a file by that filename exists and when it actually writes the file, the attacker executes a program to save a malicious code package using the filename of the temp file.

The malicious code could contain higher access permissions so the attacker can read or manipulate the file, or it could contain a link to a script file that grants access to the password file where the administrative password is stored.

Using Alternative Data Streams to Hide Files

Advanced hackers use this NTFS OS compatibility feature to hide root kits or other hacker tools to establish an anonymous base to launch attacks on the system.

The ADS feature was originally built into NTFS to provide support for Apple's Hierarchical File System (HFS) file system, which sometimes "forks" data into different files. However, this technique has been adopted for storing file metadata and to provide temporary storage.

As mentioned earlier, hackers use the ADS feature to hide their tools from the system as it is virtually impossible to detect with native user interfaces. After the hidden ADS files have been embedded in some standard OS file, they can be executed without being detected as an illegitimate operation. The only sign of an ADS operation is an illegitimate timestamp on the file where the hidden tools have been injected.

Performing Directory Traversals

These attacks exploit poorly secured software applications to access files that should not be accessible in order to "traverse" to a higher level folder or directory, as shown in Figure 8.5. Such attacks are also referred to as *backtracking, directory climbing attacks,* or *canonicalization attacks*.

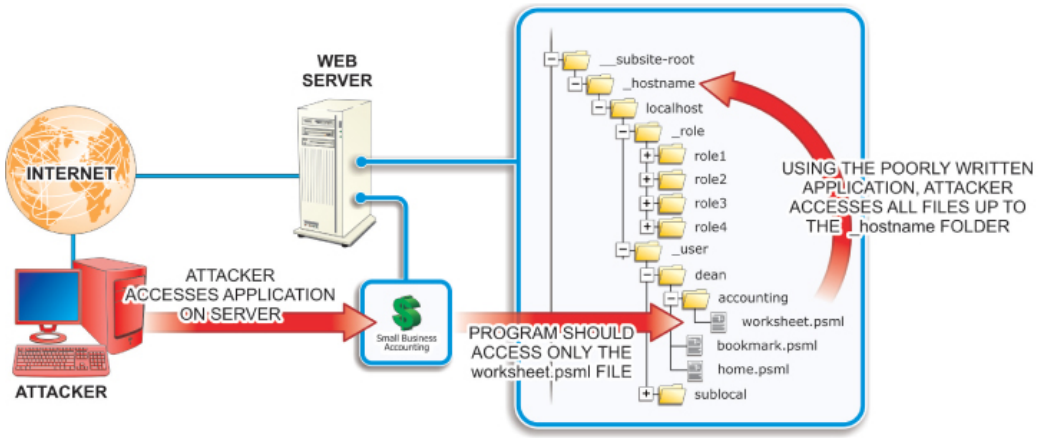


FIGURE 8.5 Directory Traversal

Hackers use this form of HTTP exploitation to access a web server's directory tree. After the hacker has gained access, they can navigate the tree to view restricted files or execute commands on the server. Such attacks are launched using common web browsers against poorly configured web servers.

These attacks can be minimized through careful web server configuration, filtering web browser input, and using vulnerability scanner software.

The following section compares and summarizes the key structural and security features of the most widely used operating systems. This comparison involves the operating system's versions, kernel architecture, file management systems, and native data-encryption capabilities.

Microsoft Windows

The Windows line of operating systems from Microsoft offers the most widely used disk operating systems with personal computers. Windows is a graphical user interface (GUI)-based operating system that enables users to navigate through the system using a series of pop-up windows and menus.

- Windows Client versions – Windows XP, Windows Vista, Windows 7, Windows 8, and Windows 10
- Windows Server versions – Windows Business and Small Business Server (SBS) versions 2003, 2008, 2012, and 2016

All Windows operating systems are designed to work with x86 32-bit and x86 64-bit processor types from Intel, AMD, and VIA. Windows operating systems after Windows XP SP2 and Windows Server 2003 support XD-bit operations on some 32-bit x86 processors, as well as on 64-bit x86 processors that offer NX-bit support.

Windows operating systems support the following basic file system formats:

- FAT/FAT16/FAT32 – The File Allocation Table series of FMS are cluster-based versions of an older file management system that was developed to manage data storage on floppy disks. Because of its widespread use in Microsoft DOS and early Windows versions, it has evolved and remained in use until the present.

  The number in the FAT title represents the number of bits in the table entry that tracks the location of the data cluster on the disk. The original FAT standard employed a 12-bit table entry and could track the locations of 4096 (1 × 212) table entries. The FAT file system is still commonly found on USB storage devices, SD cards, and other flash memory devices, as well as many other portable and embedded devices. FAT file system versions offer relatively little in the way of security tools for the data stored in their structures.
- NTFS – The New Technology File System is Microsoft's proprietary and default file management system for its operating systems. NTFS brought with it enhanced security features including access control lists (ACLs) and the encrypting file system (EFS).
- ISO 9660 (CDFS) – The Compact Disc File System is the standard file management system for optical disc storage.
- UDF – Universal Disk Format is the successor of the CDFS file management system. In particular, it is widely used in DVD and advanced optical storage devices.

The Windows operating systems include file- and folder-level encryption through its encrypting file system (EFS) feature. Full disk-level encryption is provided on some high-end Windows OS versions through a native utility called BitLocker. These utilities are discussed in detail later in this chapter.

Microsoft Windows operating systems provide an integrated Windows Firewall feature that enables the local administrator (or owner) to establish and configure a local firewall to control the flow of information into and out of the local host computer from an external network connection through a process called *packet filtering*.

LOCAL AND NETWORK-BASED FIREWALLS

The operation of local firewalls is covered in Chapter 9. Network-based firewalls, which are designed to control the flow of data into and out of a network, will be discussed in Chapter 12.

Unix

The Unix line of operating systems provides modular, multitasking, multiuser OS environments originally developed to run on mainframe and minicomputers. Proprietary versions of the Unix OS include several BSD (Berkley Software Distribution) variations, along with Apple's OSX and iOS operating systems. Several notable Unix-like operating systems have been derived from the basic Unix operating system, including multiple Linux distributions.

Different Unix OS versions have been designed to work with a number of different microprocessors. Likewise, different Unix OS versions provide support for number of different file systems formats:

- UFS – The UNIX File System was the first structure designed for the original UNIX operating system and continues in use with UNIX and its derivatives. The structure of this file system standard presents a unified tree structure beginning at a main directory known as root (/).
- NFS – The Network File System was developed by Sun Microsystems to enable client computers to access files across a network. Because NFS was developed as an open protocol standard any company can (and have) incorporate it into their own suite of supported protocols. It is used primarily in UNIX OS versions, but is also supported in Microsoft Windows and Apple's MAC OSs.

Some Unix operating systems include built-in encrypted file system capabilities. The original encryption tool included as a standard part of the Unix operating system is *crypt*. However, this tool is considered to be a very low-powered encryption tool that is relatively easy to crack. For that reason, it is not widely used. The Data Encryption Standard (DES) is a stronger encryption tool used with many Unix distributions. Pretty Good Privacy (PGP) is another widely used Unix encryption tool. This tool does both private and public key encryption/decryption and offers a very strong method to secure data.

Unix distributions based on the Free BSD kernel offer encryption services through PEFS, GELI, and GBDE utilities. Private Encrypted File System (PEFS) is a file-based encryption system. GELI and GEOM Based Disk Encryption (GBDE) are disk-level encryption utilities. Another notable encryption tool for other Unix or Unix-like operating systems is EncFS.

FreeBSD and OpenBSD distributions also offer multiple built-in firewall utilities to control the flow of data into the local computer. These options include ipfirewall (ipfw), IPFilter, and Packet Filter (PF). As with the integrated Windows Firewall mentioned earlier, these applications enable the local computer to control the flow of incoming and outgoing data through a process called *packet filtering*. Local firewalls and packet filtering are covered in detail later in the chapter.

A WORD ABOUT ENCRYPTION TOOLS

Many countries have created laws outlawing the use of strong encryption. Therefore, different operating systems may be available with and without different encryption tools based on where they are being sold.

Linux OS Distributions

Many personal computer users run versions of a freely distributed, open-source operating system called Linux. Linux is a very powerful, command-line operating system that can be used on a wide variety of hardware platforms including Windows PC and Apple Mac systems.

A community of programmers works with the Linux oversight committee to continually upgrade and enhance the basic Linux structure to keep it current and competitive. In addition, several companies have developed proprietary additions to the basic Linux structure to produce their own distributions (Linux-speak for versions) of the operating system:

- Major Linux client distributions – Ubuntu, Red Hat, SUSE, Slackware, Mandrake, Fedora, FreeBSD, Debian, and others
- Linux Server distributions – Red Hat Linux Server, Ubuntu Server, SUSE Server, and others

Different Linux OS distributions have been designed to work with x86 and x86 64-bit microprocessor types from Intel, AMD, and VIA, as well as Motorola/IBM-PowerPC processors and Sun Microsystem's SPARC processors. The Linux kernel supports the NX-bit on some x86 processors, as well as on x86-64, PowerPC microprocessors, and other 64-bit processors that offer NX-bit support.

LINUX DISTRIBUTIONS AND CAPABILITIES

The Linux name is actually used to describe a number of different distributions with differing capabilities.

Linux OS distributions commonly provide support for several different file system types:

- ext/ext2/ext3/ext4 – The ext series of Extended File Systems are the primary file management systems designed for the Linux kernel. Ext2/3 is widely used in SD cards and other flash-based storage devices.
- ReiserFS – The Linux kernel provides support for the Reiser file system which is the default system on some Linux distributions. It is a journaling file system (one that keeps track of changes in a circular log file, referred to as a journal, before committing them to the file system). ReiserFS includes UNIX permissions, ACLs, and attribute security features, but does not include any data encryption services.
- Linux OS – Linux OS distributions also commonly provide support for the ISO9660, FAT, and UDF file system formats described for Windows files systems.

The major Linux operating systems provide built-in file-system-level encryption services through a package called eCryptfs. This level of encryption enables the encryption service to be applied at the individual file or directory without significant disk management overhead.

Linux distributions offer built-in local firewall functions through a kernel utility called Netfilter. In addition to providing packet filtering for local firewall implementation, this utility offers additional protection through processes called network address translation (NAT) and port address translation (PAT) for directing packets through a network in addition to masking the private IP address from hosts outsider the network.

Apple OS Versions

Apple Inc. produces personal computers that are not intrinsically compatible with PCs. They have distinctly different hardware designs and do not directly run software packages developed for the Win/PC environment.

All newer Apple Mac computers run on a proprietary version of Unix called Apple OS X. While the structure of OS X is Unix-based, the user interaction portions of the system employ Apple's trademark GUI-based desktop. This gives the Mac a very powerful and stable engine with very user-friendly interfaces with which to work:

- Apple client versions: macOS, OS X, and Mac OS X
- Apple Server versions: macOS Server, Mac OS X Server, and OS X Server

MacOS was designed to work with x86 and x86 64-bit microprocessor types from Intel, Cyrix, VIA, and AMD, as well as PowerPC processors from IBM and Motorola. These microprocessors all support NX-bit functions to protect certain areas of memory from virus manipulation.

MacOS supports the ISO9660, FAT, NFS, UFS, and UDF file system formats described earlier. In addition, support for the following FMS standards is provided in different macOS versions:

- HFS/HFS+ – The Hierarchical File Systems are proprietary Apple file systems developed as the primary file system for their Mac line of computers using macOS. It is also used in Apple's line of iPod music devices. Support for the updated HFS+ version has been included in non-Apple operating systems including the Linux kernel and Windows (including support in Apple's Xbox 360 gaming console).
- SMBFS/CIFS – The Server Message Block File System, also known as the Common Internet File System, was developed to provide shared access to files and devices, along with network communications. This FMS is mostly used with computers running Windows prior to the advent of Active Directory. However, support for newer SMB releases has continued through all current Microsoft OS versions in addition to making its way into several non-Microsoft operating systems.

Apple macOS operating systems include disk-level-based data encryption through a service called FileVault; FileVault2 macOS users can also use the built-in disk utility to encrypt their disk and store subsets of their home directory.

iOS

iOS is a proprietary Apple mobile operating system designed to support Apple's line of iPhones and iPads. While iOS shares many structures with macOS, it is not compatible with macOS applications.

iOS is designed to work with reduced instruction set computing (RISC) processor types from the Acorn RISC Machines (ARM) Ltd company. These devices use significantly less energy and produce much less heat than their x86 complex instruction set computing (CISC) rivals. This makes RISC processors a natural for use in small, battery-powered devices such as phones, tablets, and pads. From the ARMv6 version forward, this architecture has supported an Execute Never (XN) page protection feature.

The iOS system includes integrated device-level file encryption to protect the data if the device running is lost or stolen. It also offers protection from unauthorized users using or modifying the data. In addition to its hardware encrypting feature, iOS offers a class-based tool called Data Protection. With this protection tool, file-based encryption keys are created each time data is written to the device's flash memory structure.

Android OS

The Android operating system was developed for use with tablet and smart phone devices that primarily use touchscreen gestures for operation and control. It is currently the most popular mobile operating system in use due to the number of smart phone and tablet devices it is used in, as shown by the graph in Figure 8.6.

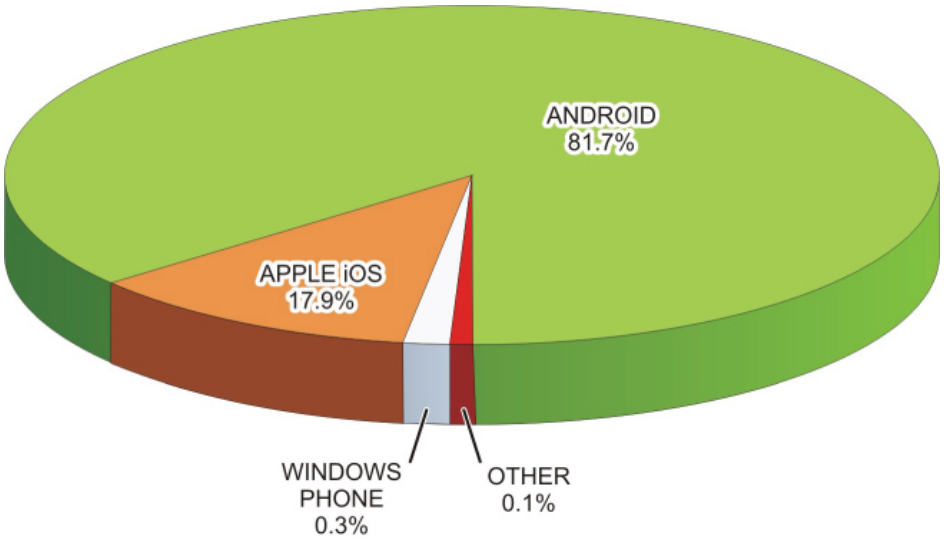


FIGURE 8.6 2014 Smartphone OS Graph

Android is based on the Linux OS kernel but typically includes a wrapper of proprietary user interfaces, utilities, and applications. Because of its open-source availability, Android has been embraced by a development community and made its way into a number of devices in consumer, military, business, and educational applications.

The Android OS is designed to run on 32- and 64-bit ARMv7/8 processors. This includes proprietary I.MX5/i.MX6 ARM processors from Freescale Semiconductors (a former division of Motorola). These microprocessors support the XN page-protection feature. There is also a version of the Android OS kernel designed to support x86 architectures. Of course, these processors support the XD-bit or NX-bit feature.

The kernel configuration of different Android devices supports different file systems that are specific to that device. However, there are some flash memory file systems that are common to Android systems:

- exFAT – Microsoft's extended File Allocation Table file system for flash memory devices.
- F2FS – Samsung's Flash-Friendly File System (version 2) is an open-source Linux file system for flash storage devices.
- JFFS2 – The Android default Journal Flash File System (version 2). This FS version replaced the YAFFS2 (Yet Another Flash File System) as the default Android flash file system used in earlier kernel versions.
- Ext2/Ext3/Ext4 – Versions of the Linux Extended File System that replaces F2FS and JFFS2 as the file system for internal Android flash devices.

In addition to these flash-memory file systems, Android devices also commonly support the Microsoft File Allocation Table (FAT) file systems (FAT12, FAT16, and FAT32), along with their VFAT extension.

The Android OS offers disk encryption based on a utility called `dm-crypt` to store data on the device's flash memory device. This utility is an integral feature of the Android's Linux kernel.

Operating System Security Choices

Because of its popularity, Microsoft Windows presents the biggest target for both mischievous and malicious malware and *grayware* (annoying unwanted software) writers. Therefore, Windows receives an unrivaled percentage of all the attacks associated with viruses and spyware.

This fact has led some Windows customers to adopt other operating system platforms such as Linux or macOS, which are much less of a malware target. Table 8.1 summarizes some common security features associated with various operating systems.

TABLE 8.1 Operating System Security Comparisons

Name	Resource Access Control	Subsystem Isolation Mechanisms	Integrated Firewall	Encrypted File Systems	No Execute(NX)
Linux	**POSIX, ACLs, MAC**	**`chroot`, capability-based security, seccomp, SELinux, AppArmor**	**Netfilter, varied by distribution**	**Yes**	**Hardware/Emulation**
macOS	**POSIX, ACLs**	**`chroot`, BSD file flags set using chflags**	**PF**	**Yes**	**Hardware/Emulation**
Windows Server	**ACLs, privileges, RBAC**	**Win32 WindowStation, desktop, job objects**	**Windows Firewall**	**Yes**	**Hardware/Emulation**
Windows	**ACLs, privileges, RBAC**	**Win32 WindowStation, desktop, job objects**	**Windows Firewall**	**Yes**	**Hardware/Emulation**

Common Operating System Security Tools

After the system has booted up, steps can be taken to prevent unauthorized personnel from accessing the operating system and its applications. These steps include:

- Implementing local login requirements
  - Establishing user and group accounts
  - Setting up password policies
  - Establishing lockout policies
- Implementing additional authentication options
  - Using biometric authentication devices
  - Using physical authentication devices
- Using Local Administrative Tools
  - Enabling system auditing and event logging
  - Implementing data encryption tools
  - Overseeing application software security
- Providing remote access protection
  - Establishing firewall settings
  - Configuring browser security options
  - Establishing and implementing malicious software protection
  - Applying security updates and patches

Figure 8.7 shows the Local Security Policy/Security Settings options available in a Microsoft Windows control panel. The first set of options includes password and account lockout policy choices to locally control access to the system. You can also implement local admin policies for system auditing, users rights, and security policies.

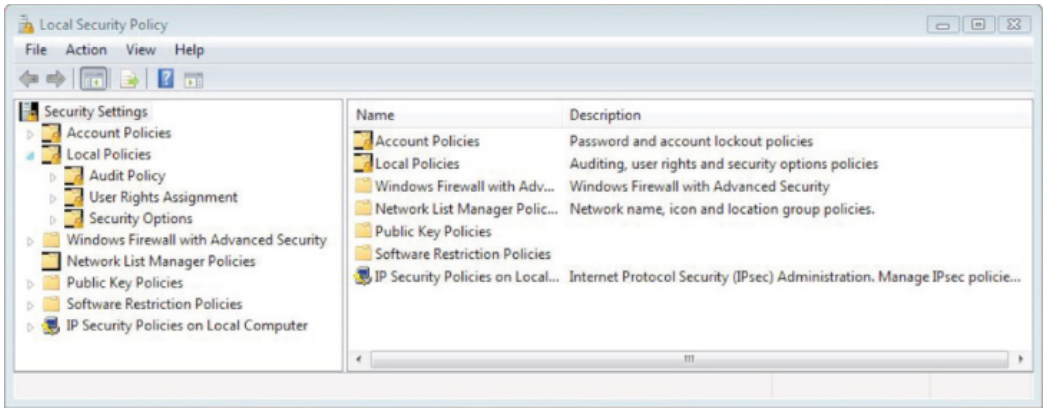


FIGURE 8.7 Local Security Policy/Security Settings

The Windows Firewall and Advanced Security tools enable the local administrator (or owner) to establish and configure a local firewall as described earlier.

The remaining tools shown in Figure 8.7 are security tools that enable local policies to be established to control the local computer's interactions with an external network. In the following sections, you will learn how to implement them for best local-host security practices.

A WORD ABOUT SECURITY TOOLS

It should be apparent from a quick look at the tools in Figure 8.7 that the policies are designed to control the interaction of the local computer with an external network. While the tools are local, they are also used in networked environments. There are cases where both local and network administrative policies cover the same security elements. In these cases, the network policy will override the local policy if they are configured in conflict with each other.

Implementing Local Login Requirements

The main user authentication tool used with personal computing devices is the username and password login. In general, there are three types of user-related logons with which to contend:

- A logon to the local machine
- A logon to a specific software application
- A network logon

At the local computer level, the local logon is typically required. This level of logon validates the user for using the local computer's resources (files and devices). However, in a shared computer environment where multiple users may be enabled to use the same computer, local user and group credentials are created and configured through a user accounts database that is stored on the local computer.

A WORD ABOUT LOCAL LOGONS

In a network environment, the network login typically supersedes and replaces the local login option. This logon level confirms the user's credentials for accessing remote resources.

These credentials are used to gain initial access to the computer, control access to its local resources, and control access to network resources. In a Windows environment, these accounts are created and managed through the Local Users and Groups utility under Computer Management, as depicted in Figure 8.8.

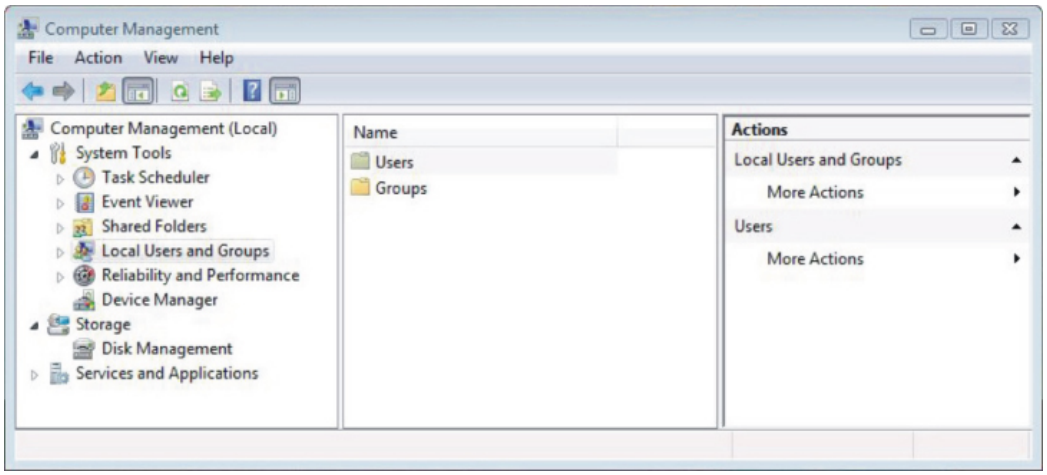


FIGURE 8.8 Microsoft Local User and Group Accounts

The first time a standalone system is started an administrator's account is automatically created in the operating system's local accounts database. The administrator has rights and permissions to all of the system's hardware and software resources. The administrator, in turn, creates other users and then grants rights to them and permissions to system resources as necessary.

The administrator can deal with users on an individual basis or may gather users into groups that can be administered uniformly. In doing so, the administrator can assign permissions or restrictions on an individual or an entire group. The value of using groups lies in the time saved by being able to apply common rights to several users instead of applying them one by one.

The other default group created when the operating system first starts is a type of account known as a Guests group. This default group typically has minimized access to the system, and all of its members share the same user profile. The Guest user account is automatically a member of this group.

Each user and group in the local environment has a profile that describes the resources and desktop configurations created for them. Settings in the profile can be used to limit the actions users can perform, such as installing, removing, configuring, adjusting, or copying resources.

When users log into the system, it checks their profiles and adjusts the system according to their information. These credentials are used to gain initial access to the computer and control what access each user has to its local resources. In addition, access to certain software applications and other resources may be controlled by additional application-level passwords.

Passwords

For a password to be effective it must possess a certain amount of complexity. Its length, width, and depth must be such as to thwart the efforts of the previously mentioned password-cracking techniques.

The length of a password directly affects the ease with which it can be cracked. The longer the password is, the more difficult it will be to crack. It is generally recommended that passwords should consist of at least eight characters. If permitted by the OS, longer passwords can be used, provided the employees or clients can remember them.

The width of a password relates to the number of different types of characters that can be incorporated, including those not belonging to the alphabet. Combinations of numbers, special

characters, and uppercase and lowercase letters make passwords stronger, especially when an operating system considers uppercase and lowercase letters as completely different characters.

Passwords can contain control characters, alternative characters, and even spaces in some operating systems. Ideally, all the following character sets should be drawn from when users are required to create strong passwords.

- Uppercase letters such as A, B, C
- Lowercase letters such as a, b, c
- Numerals such as 1, 2, 3
- Special characters such as $, ?, &
- Alternative characters such as @, %

The depth of a password involves how difficult it is to guess its meaning. Although a good password should be easy to remember, it should nevertheless be difficult to guess. For a number of years, the top two passwords overall have been “123456” and “password.” Attackers know common terms and techniques used in creating passwords as well, such as appending and replacing.

Appending is the act of adding a set of characters to the end of another set of characters (example123). *Replacing* is using a set of characters to replace another set of predictable characters (ex@mp1e). The meaning of a password should not be something that could be easily guessed or deduced through simple reasoning. One approach that seems to work well is to think in terms of phrases rather than simply words.

Mnemonic phrases are often incorporated, allowing the creation of passwords that cannot be easily guessed, but yet do not need to be written down to be remembered. Mnemonic phrases can be spelled phonetically, using, for example, “UraTygr!” instead of “You’re a tiger!” Alternatively, the first letters in each word of a memorable phrase can be incorporated, such as “Ihnybtf,” which is abbreviated from “I have not yet begun to fight!”

Another effective method is to choose a meaningful phrase that can be easily recalled. Then, the initials of some words in the phrase can be converted into alternative characters. For example, the number “4” could be substituted wherever the letter “f” is used.

Additional Password Security

The need for additional password security has become more recognized with the increased ease with which scam artists continue to steal them. Passwords have ultimately been gathered as easily as simply asking for them. Personnel should simply never talk about passwords with anyone, no matter how harmless or legitimate such conversations might seem.

Although standard password-protection practices may be adequate to keep some would-be intruders at bay, certain situations require a more sophisticated approach. In these cases, extra protection can be afforded through the use of encryption techniques and one-time passwords (OTP).

Password encryption is the process of taking a standard password and applying an algorithm to it in such a way as to make it meaningless to sniffers, crackers, or other eavesdroppers. Two-factor authentication, such as one-time passwords, are good only for one transaction but add another valuable layer of security.

Best password practices include the following:

- Use a consistent naming convention across the organization so that users can understand theirs and not resort to recording them so they can be found by others.
- Always supply a password to an account and make the user change it upon first login.
- Protect passwords (don't write them down in open spaces).
- Do not use default passwords.
- Educate users to create strong passwords.
- Enforce password policies at all levels of an organization.

SAFEGUARDING PASSWORDS

True password security involves users safeguarding their passwords from others.

Account Lockout Policies

Operating systems provide password lockout policy settings that enable administrators to enact password policies that prevent attackers from repeatedly trying to access the system. This prevents the attackers from using brute force attacks to guess the account password so they can break into the system.

Brute force attacks involve the repeated use of login attempts to try to guess the password. As shown in Figure 8.9, typical lockout policy settings include:

- Account Lockout Duration – How long (in minutes) the account will be locked out before it automatically unlocks. Setting this value to 0 will prevent the account from unlocking until the administrator manually resets it.
- Account Lockout Threshold/Max Failures – How many times account access can be attempted before the account is locked out. The default value for this setting is 0, which disables the account lockout function.
- Reset Account Lockout Counter After/Lockout Duration – The amount of time that can pass before the account lockout value is returned to 0.

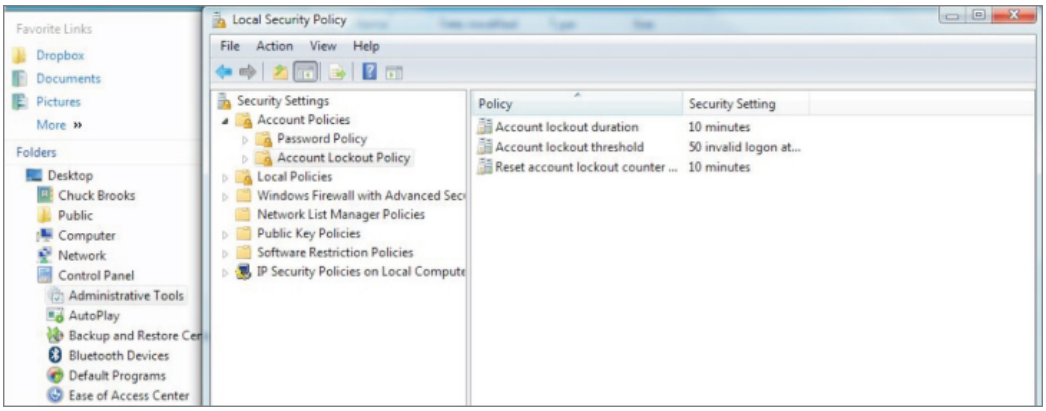


FIGURE 8.9 Windows Lockout Options

Computer Locking

Users should never leave their computer unattended after they have logged on. Doing so opens the door for others to access and manipulate their computer, data, and network. All users should be trained to either log off or lock their computers when they are away from them, even if only for a few minutes.

Locking the computer protects it from intruders and preserves the current system state. When the computer is unlocked, the applications and data that were active in the system are still open, making it much easier for the user to pick up where they left off.

Users should also be instructed to make sure they log off at the end of the day. This closes all applications and ensures that data files are saved.

Implementing Additional Authentication Options

Recall from Chapter 2 that authentication is defined as the process of determining that someone is who they say they are. At the local computing or control device level, authentication can be implemented in terms of physical or biometric authentication systems to replace or augment password authentication methods.

Physical Authentication Devices

There are hardware devices that can be used to make personal computer systems unusable by people other than authorized users. These devices include items such as smart cards and biometric devices similar to the ones described in the preceding chapter. However, unlike the devices designed to protect access to physical infrastructure, these devices are designed specifically to be used with personal computing systems.

USING SMARTCARDS

Some organizations issue their employees smart cards that they can use to get into their buildings, log on to their PCs, and access appropriate applications with a single security device.

The card system combines the users' secret PINs (i.e., something the users alone know) with tokens generated by the network's Certificate Authority authentication system to generate a unique pass code. The pass code validates the user and their access to different resources.

Biometric Scanners for Personal Computing Devices

As discussed in Chapter 2, biometric scanners are becoming significantly more sophisticated, including facial scanning devices, searchable databases, and supporting application programs.

In addition to serving as authentication devices for facility access, many biometric scanning devices have evolved for use with personal computers. However, the biometric authentication device most widely used with personal computers is the fingerprint scanner. Figure 8.10 shows different fingerprint scanner devices designed for use with PCs.

FIGURE 8.10 Fingerprint Scanners

Some fingerprint scanner manufacturers offer miniature touchpad versions that sit on the desk and connect to the system through a cable and USB connector. Other fingerprint scanners are built into key fobs that simply plug directly into the USB port. Some manufacturers even build these devices into the top of the mouse.

Some models actually store the scanned images and account access information on the device. This allows the identification file to travel with the user if they work with different computers at different locations.

After the fingerprint scanner software has been installed and configured, the password manager will prompt you to scan in your fingerprint rather than type a password on future log-in attempts.

Using Local Administrative Tools

All of the different operating systems discussed previously offer management tools to control who, when, and how the local computer is used. Collectively, these tools are referred to as *administrative tools* (in Microsoft Windows OS versions, the Control Panel applet where these tools are configured and launched is titled "Administrative Tools").

These tools typically include programs designed to control the usage of the computer's memory, administer and optimize hard-disk-drive usage, configure OS services running on the computer, control the hardware/OS handoff during startup, and troubleshoot operating system problems. However, in each case there is a subset of these management tools dedicated to security-related functions. In the following sections, we will investigate common security-related OS tools and their implementations.

Event Logging and Auditing

Auditing is a security function of the operating system that enables the user and operating system activities performed on a computer to be monitored and tracked. This information can

then be used to detect intruders and other undesirable activities.

These entries provide a fundamental tool for unauthorized-intrusion-detection efforts. There are two common types of audit records to consider:

- Native audit records – Event records generated by most modern multiuser operating systems. Because these records are already being generated by the operating system, they are always available, but they may not contain the desired events or be in a readily usable form.
- Detection-specific audit records – Records generated to provide specific information about desired actions or events. These actions or events can be based on operating system activities, application events, or security events.

The auditing systems available with most operating systems consists of two major components:

- Audit policy (or audit rules), which defines the types of events that will be monitored and added to the system's security logs
- Audit entries (or audit records), which consist of the individual entries added to the security log when an audited event occurs

Windows Auditing Tools

In a Microsoft Windows environment, audit entries are maintained in the security log file. Figure 8.11 shows a typical security log displayed in the Windows Event Viewer utility. For auditing to be an effective security tool, the security log should be reviewed and archived regularly.

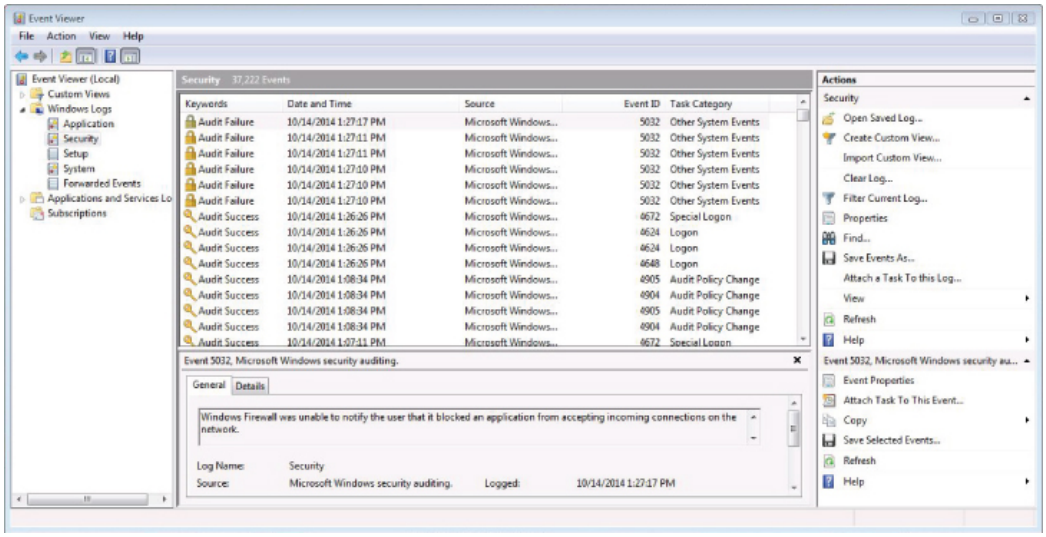


FIGURE 8.11 Viewing Security Audit Logs

In Windows, auditing is configured through the Local Security Policy option located under the Administrative Tools menu, as shown in Figure 8.12.

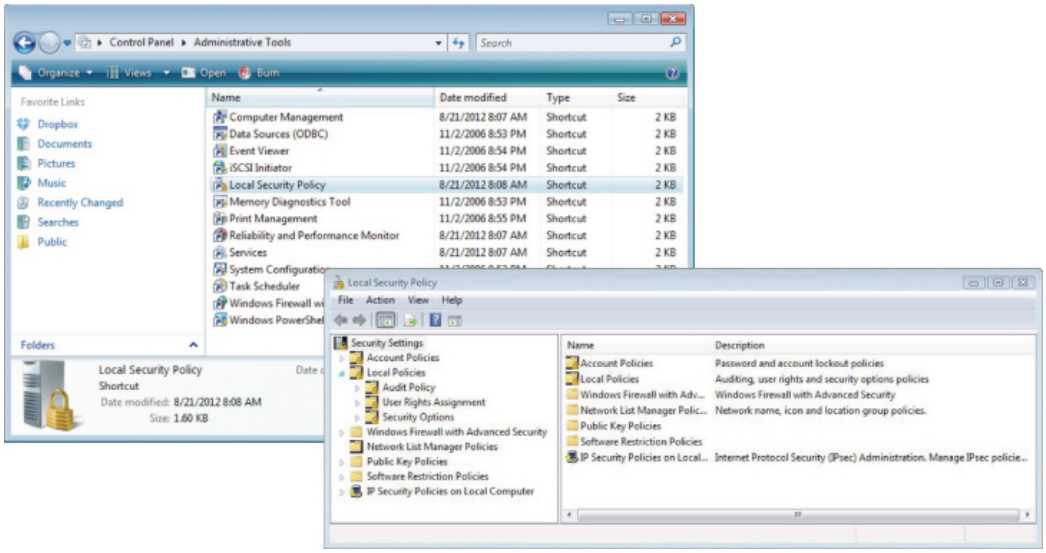


FIGURE 8.12 Configuring Auditing in Windows

Selecting a policy to be configured in the right pane will produce the Local Security Setting window, depicted in Figure 8.13. Place check marks beside the option or options that should be tracked and audited. You can check Success, Failure, or both.

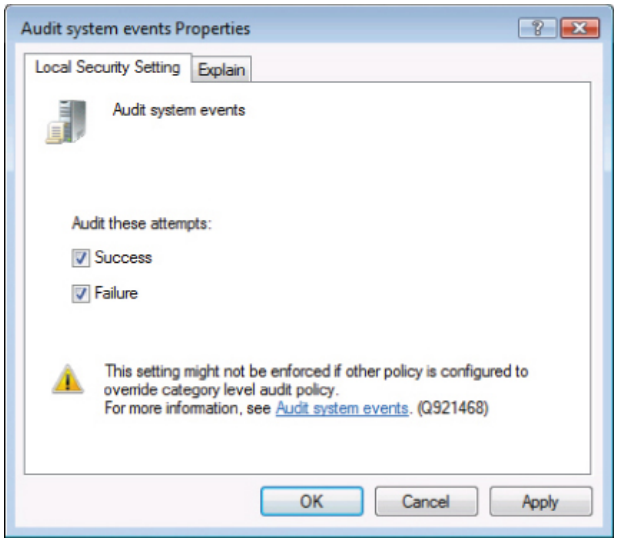


FIGURE 8.13 Establishing a Local Security Policy Setting

In Windows, auditing must be configured both as a general system policy setting and on each object (file, folder, and printer) that requires auditing. With this in mind, when you are configuring an audit policy, you must consider what effect the policy will have on the system and its performance. If you were to set up auditing on every file, folder, and printer in a system, the auditing process would place so much extra work on the system that the system could literally slow to a halt.

Linux Auditing

Linux systems also feature security auditing capabilities for tracking specified security events. Figure 8.14 provides a generic representation of a Linux security auditing framework. As with

other auditing systems, the Linux modules map computer processes to user IDs so that administrators can trace exploits to the specific user who owns the process and is performing potentially malicious activities in the system.

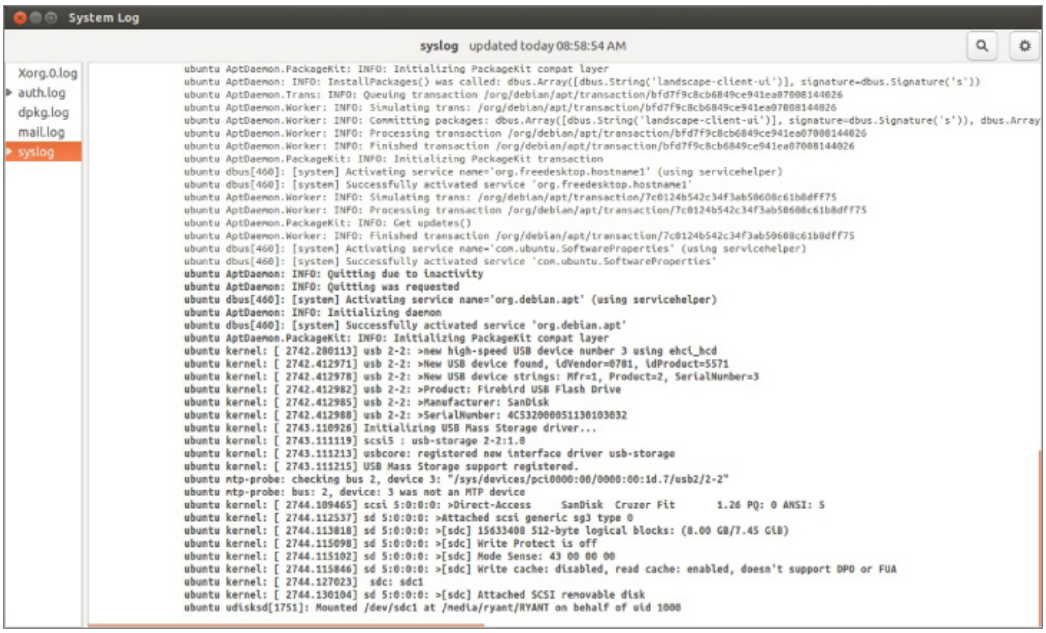


FIGURE 8.14 Linux Auditing

At the heart of the system is the audit daemon that works with the Linux kernel's audit module to record relevant events and write them to a log file on the disk. Audit rules are configured in a file that is executed when the system boots up. The audit controller utility employs the parameters in these rules to determine which system events are tracked and how they are written to the audit log file.

When an application encounters a situation that triggers a preconfigured audit event, a message is presented to the kernel's audit interface and passed to the audit controller. Under the direction of the audit controller, the audit daemon writes the event away to the audit event log.

Linux auditing systems also include a report generation tool that the administrator can use to generate custom security reports. It may also include a search utility to provide quick/specific examination of log entries for specific events.

As with Windows Group Policy configurations, you must consider the level of auditing you want the Linux audit system to perform on the computer and its operational consequences.

Implementing Data Encryption

The term *cryptography* is used to define the art of protecting communications from unintended viewers. One of the oldest methods of hiding data in plain sight is to develop a code (algorithm) for altering the message so that unauthorized people cannot read it. The process for doing this is referred to as *encryption*. Encrypting data involves taking the data and processing it with a key code (or encryption key) that defines how the original (plaintext) version of the data has been manipulated. This concept is illustrated in Figure 8.15.

FIGURE 8.15 Data Encryption

Anyone who is given the encryption key can use it to decode the message through a decryption process. *Symmetric encryption* uses the same key to encrypt and decrypt data. *Asymmetric encryption,* described in the following paragraph, uses two different keys to encrypt and decrypt information.

A particularly effective asymmetric key system is Public Key Encryption (PKE). This technique employs two keys to ensure the security of the encrypted data: a public key and a private key. The *public key* (known to everyone) is used to encrypt the data, and the *private* or *secret key* (known only to the specified recipient) is used to decrypt it. The public and private keys are related in such a way that the private key cannot be decoded simply by possessing the public key.

Data encryption in a digital device or network can occur at many levels:

- As file-system level (file and folder level) encryption
- As disk-level encryption
- As transport-level encryptions

Disk-level encryption involves using technology to encrypt the entire disk structure. This technique offers value in that it protects everything on the disk from unauthorized access including the operating system files and structure. Disk encryption in a personal computer system may be performed at the software or hardware level. At the software level, disk encryption technology is available through most major disk operating system versions as well as through third-party suppliers.

The disk encryption software runs at a level between the operating system's device drivers and the higher-level applications. For the most part, computer programs and designated users are not aware that the encryption/decryption process is occurring. Figure 8.16, illustrates a simplified version of the encryption/decryption process.

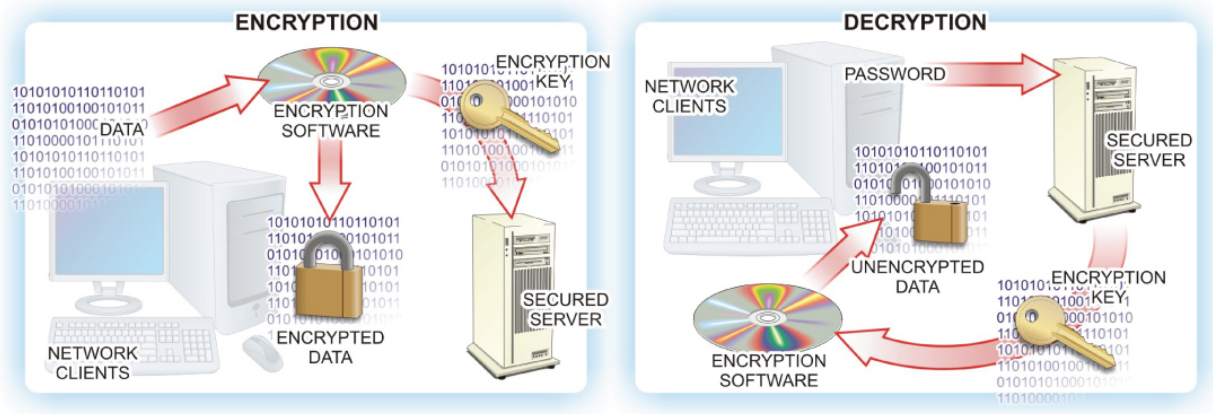


FIGURE 8.16 The Encryption/Decryption Process

During the initial disk encryption process an encryption key is generated and stored on the system. This key is stored in an encrypted format that requires a password or passphrase to decrypt. When a user supplies the password or passphrase, the system applies the decryption key to the data, unlocking it for the computer's applications to use. When new data is generated, it is encrypted before it is stored on the disk drive.

Hardware-Level Disk Encryption

Many computer motherboard designs include a built-in microchip called a Trusted Platform Module (TPM) that is used to store cryptographic information, such as encryption keys. Information stored on the TPM is more secure from external software attacks and physical theft.

This technology protects the operating system and user data to ensure that a computer is not tampered with, even if it is left unattended, lost, or stolen. The encryption managers in these operating systems prevent access to a hard drive by encrypting the entire drive.

If the computer motherboard is equipped with a compatible TPM chip, disk operating systems use the TPM to lock the encryption key that protects the data stored on the hard drive. The key cannot be accessed until the TPM has verified the state of the computer during startup.

During the computer startup process, the TPM compares a hash code derived from important operating system configuration values with a snapshot of the system taken earlier. If the codes match, the operating system will release the decryption key that unlocks the encrypted disk drive. In doing so, this process verifies the integrity of the operating system's startup process, as shown in Figure 8.17. The key will not be released if the TPM detects that the operating system installation has been altered.

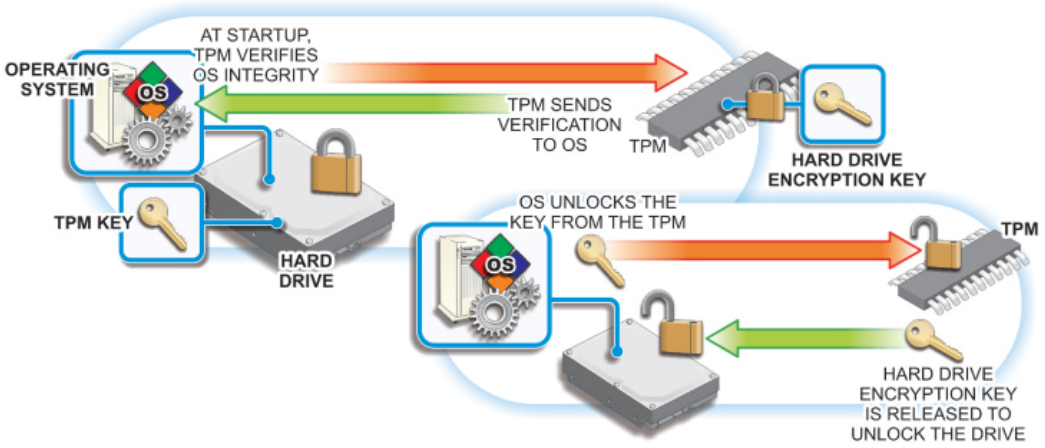


FIGURE 8.17 Using the TPM

The theory is that the data on a hard drive would be safe if the computer were stolen because the operating system would not allow the hard drive to be accessed. One problem associated with this method is, if the motherboard fails and is replaced, a backup copy of that startup key will be needed to access the data on the hard drive.

MOVING TPM CHIPS

A TPM chip cannot be moved from one motherboard to another.

This drive must be present to unlock the data stored on a volume. In such cases, it is recommended that you make backups of the startup key. The most secure option is to require that a PIN or password be used any time the computer is started along with the automated TPM process.

BACKING UP STARTUP KEYS

Be aware that if the TPM fails or all the copies of the startup key become lost or corrupted, the recovery of the data will prove to be very difficult. Individual computer users must determine whether their security needs warrant going this "extra mile" to protect their personal computers. However, in a business environment, this requirement is typically dictated by the system administrator.

Operating System TPM Tools

In selected Microsoft Windows operating systems, a utility called BitLocker is available to engage the motherboard's TPM module. It works with Windows to encrypt the entire hard drive or hard drives (this includes all the volumes in the system).

There are four ways to employ the BitLocker utility:

- BitLocker works with the TPM chip to store the BitLocker encryption key. This secures the hard drive data even if the drive is removed. As noted, one problem associated with this method is, if the system board fails and is replaced, a backup copy of that BitLocker encryption key will be needed to access the data on the hard drive.
- If the computer is not equipped with a TPM chip, the startup key on a USB flash drive must be inserted in the system prior to bootup.
- Startup keys can also be used on computers that do possess TPM chips. One problem associated with this method is the tendency of users to leave the flash drive installed in the computer.
- The most secure option is to require that a PIN be used along with the automated TPM process any time the computer is started.

Linux operating systems also possess tools to engage the TPM encryption capabilities of compatible motherboards. In these systems, it is necessary to confirm that the Linux kernel involved supports the TPM version on the motherboard. The three kernel modules involved in TPM configuration are `tpm_bios`, `tpm`, and `tpm_tis`. The generic `tpm_bios` and `tpm` modules are loaded first and then the `tpm_tis` module is loaded with specific parameters.

Several Linux software tools are available to manage TPM on Linux-based machines. Trousers is an open-source daemon that controls all of the communications with the TPM through a single module. Likewise, the TrustedGrub module is capable of detecting and supporting TPM functionality in Linux systems. It is a downloadable extension of the Grub bootloader that has been modified for this purpose.

When you initialize the TPM, the module will request an owner password and a Storage Root Key (SRK) password that it can use to generate the cryptographic key. The owner password is required to perform administrative tasks on the system, while the SRK is required to load a key into the TPM. These keys must be maintained and can never be lost because continued access to the system would be nearly impossible without them.

File- and-Folder-Level Encryption

As the title implies, file-and-folder-level encryption is applied to individual files and folders. File- and-folder-level encryption tools enable users to encrypt files stored on their drives using keys that only the designated user (or an authorized recovery agent) can decode. This prevents data theft by those who do not have the password or a decoding tool. It greatly enhances the security of files on portable computers by enabling users to designate files and folders so that they can only be accessed using the proper encryption key.

This type of encryption is typically implemented as an attribute setting that can be established for specified files or folders and is linked to the authorized users in the system. These users can open these files and folders just as they would any ordinary files or folders. However, if someone gains unauthorized access to the computer, they will not be able to open the encrypted files or folders.

Microsoft File Encryption Tools

Windows provides effective local hard-drive security through its encrypting file system (EFS) feature, as shown in Figure 8.18.

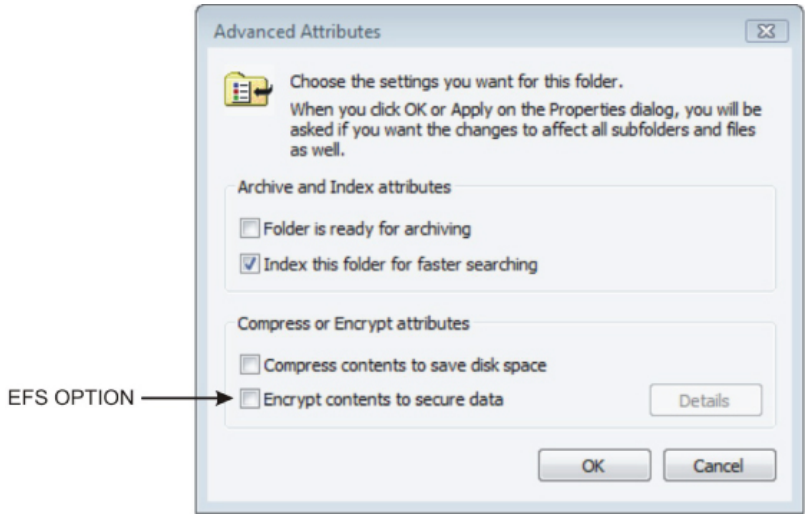


FIGURE 8.18 Windows Drive Encryption Options

The EFS feature enables the user to encrypt files stored on the drive using keys that only the designated user (or an authorized recovery agent) can decode. This prevents data theft by those who do not have the password or a decoding tool.

Windows users can implement the EFS option to encrypt their files and folders on NTFS drives. To do so, they simply click the Encrypt Contents To Secure Data check box in the file or folder's Advanced Attributes windows. Users can open these files and folders just as they would any ordinary files or folders. However, if someone gains unauthorized access to the computer, they will not be able to open the encrypted files or folders. EFS is simple to use because it is actually an attribute that can be established for files or folders.

The EFS feature further enhances the security of files on portable computers by enabling users to designate files and folders so that they can only be accessed using the proper encryption key.

A WORD ABOUT EFS

EFS prevents files from being accessed by unauthorized users, including those trying to bypass the operating system and gain access using third-party utilities. It uses both symmetric and asymmetric encryption when securing the information.

Hands-On Exercises

Objectives

- Describe permissions available for NTFS.
- Set and test file and folder permissions.
- Verify permissions set up on user accounts.
- Set and test file/folder level encryption.

Resources

- PC-compatible desktop/tower computer system
- Windows 10 Professional installed
- TestUser accounts setup on your PC/workstation
  - User: **TestUser1** with Password: **testuser1**
  - User: **TestUser2** with Password: **testuser2**
- Both accounts should be set as standard users.
- AxCrypt installed (https://www.axcrypt.net/download/)

Discussion

The New Technology File System is Microsoft's proprietary and default file management system for its operating systems. NTFS brought with it enhanced security features including access control lists (ACLs) and the encrypting file system (EFS).

NTFS permissions can be configured as Allow or Deny options within the associated access control list. This is an example of a discretionary access control list, in which the user who is considered the owner of a file or folder chooses the permissions of said information. Figure 8.19 illustrates an ACL.

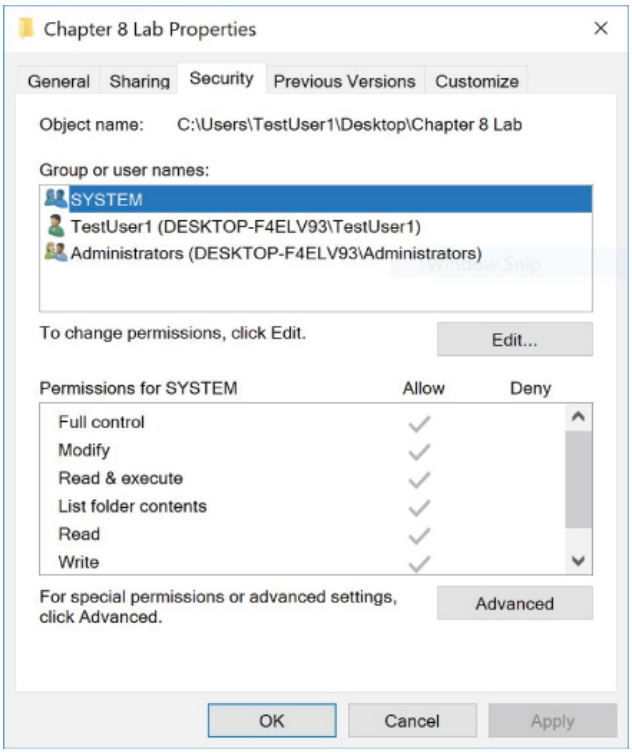


FIGURE 8.19 Access Control List

In this lab, you will manage and test permissions, and you will explore encryption at a file level with AxCrypt. Keep in mind that these procedures provide an introduction to permissions. This lab will explore permissions management on a local host computer. This lab will not feature share permissions, server permissions, inheritance, or Linux file permission management. You

will manage file and folder permissions for a select set of users. Finally, you will test various permission settings to gather a better understanding of the importance and power of ACLs.

Procedures

Setting Up and Creating Files and Folders

To be able to test the NTFS permissions you will put into place, you must first become the owner of files and folders. The owner of a file has the discretion to allow or deny access to other users.

1. Power on the computer, and if necessary choose Windows 10 Professional to log into.
2. Select TestUser1 to log in, with a password of **testuser1**.
3. Once logged in, right-click the Windows icon and select File Explorer.
4. Along the left side of the File Explorer window, locate and click on the C: drive.
5. Right-click in any white space located in the middle pane and then hover the cursor over New to expand the options. Click the Folder option. You will be prompted to name the folder. Enter **Permissions Test** as the name and press Enter.
6. Double-click the Permissions Test folder to access its contents. Here you will create another folder, specific to you.
7. Right-click the white space and select New ➢ Folder. Name this file `Perm_Test_(add your initials here)`. Example: John Doe would name his folder `Perm_Test_JD`. Figure 8.20 shows the new folder prepared in the Permissions Test folder.

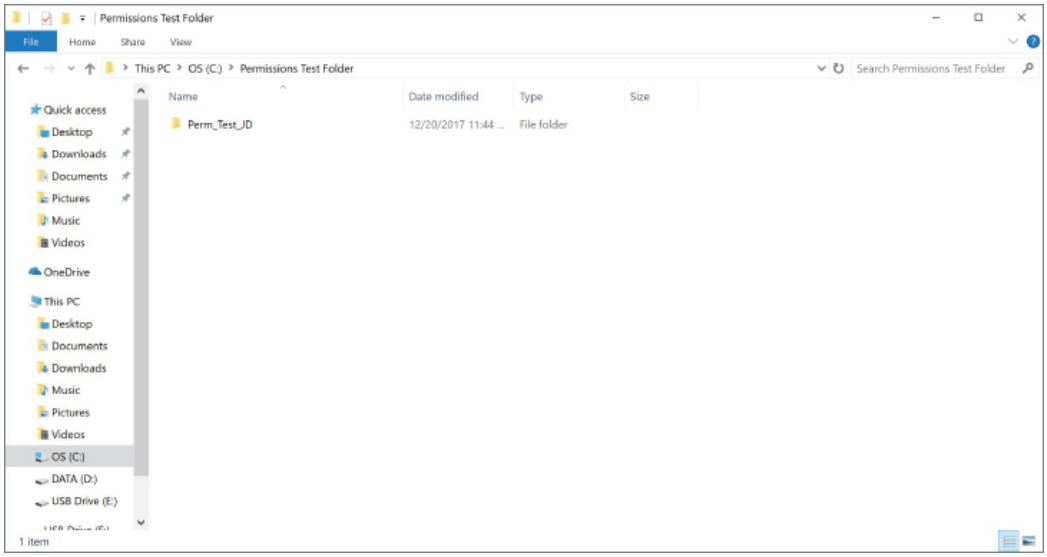


FIGURE 8.20 `Perm_Test` **Folder Created**

8. This folder should be empty. Right-click in any white space and move the cursor to hover over New. Here you will select Text Document. Name the file `test1` and press Enter.
9. Repeat Step 8 three times to create files `test2`, `test3`, and `test4`.
10. There is no information in these files, so open each `.txt` document by double-clicking and typing **This is a test. This is only a test.** into each file. Save and close each text file.

Creating File Permissions

In this section, you will explore the options available to restrict certain users' access to the files and folder you just created. You can prevent specific users or groups from executing, reading, writing, and modifying files that you have deemed important. This is accomplished through the ACL as part of each individual file.

1. Verify that you are within the `Perm_Test` folder you created in the previous steps. Right-click `test1` and click Properties. This will launch the `test1` Properties window, as shown in Figure 8.21.

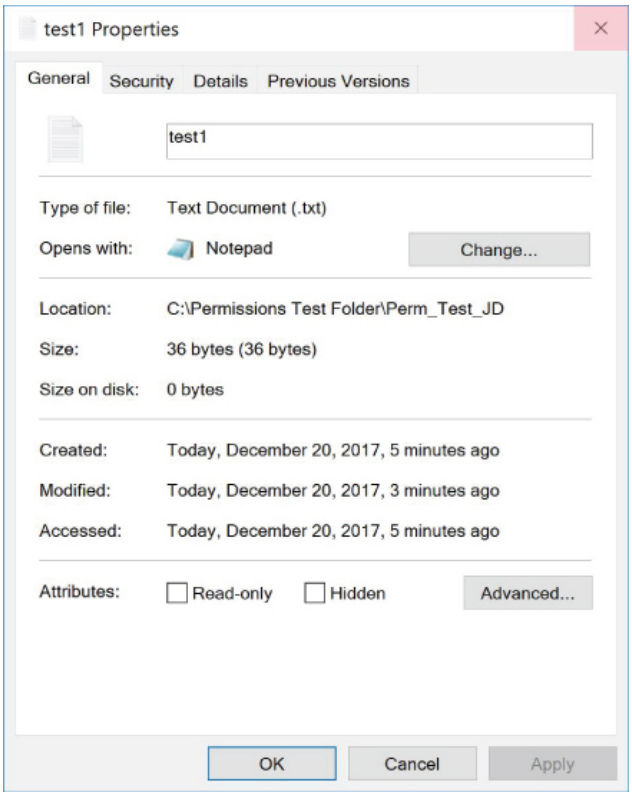


FIGURE 8.21 File `test1` Properties window

The Properties window may not have all of the tabs listed in the example. At this point, the only necessary tab you will be working with is the Security tab.

2. Click the Security tab. Note the types of permissions available and record them in Table 8.2. This window is the file's associated access control list.

TABLE 8.2 Permissions Available in `test1` ACL

Currently, the only permissions granted or denied on this object are those associated with the group the user became a member of at its creation. To limit specific users' access to this file, you must add them to the ACL and select the permission level you want them to have.

3. Click Edit to open the `test1` Permissions window.

4. Click Add to navigate to the Select Users Or Groups window.
5. Under Enter The Object Names To Select (Example):, enter **TestUser2**. Click Check Names to confirm the user account. Click OK to continue.

This is the same window in which you can add groups to grant or deny access to anyone associated with a known group. Groups are better utilized within a networked environment; therefore, you will not set or test group permissions in this lab.

Notice that the user TestUser2 is now included in the ACL. Here you can fine-tune the permissions for this user on the file you created. The default permissions given are to allow Read and Read & Execute.

6. Under the Deny column head, click the Write check box. Figure 8.22 shows the Permissions allocated to TestUser2.

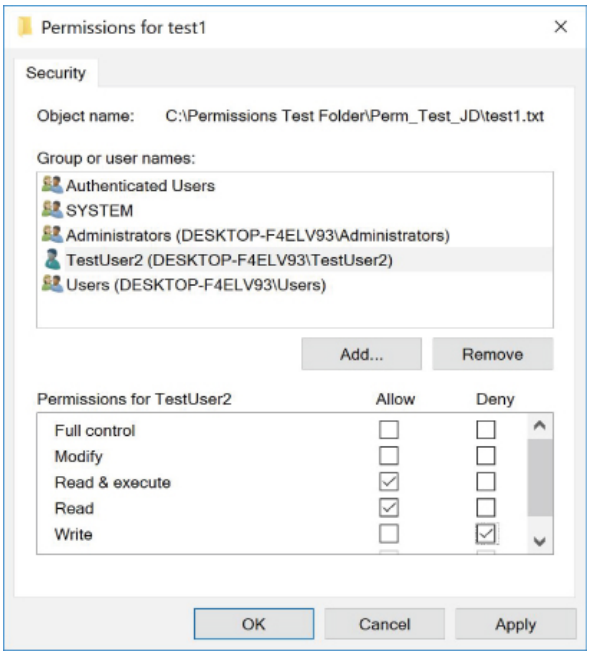


FIGURE 8.22 Permissions for `Test1` Given to TestUser2

7. Click the Apply button. Read the Windows Security prompt, and then click Yes. You are directed back to the `test1` Properties window. Click OK to exit this window.

In regard to permissions, there are a number of rules that apply:

- *Deny permissions* take precedence over *allow permissions* in most scenarios. When a deny permission is applied to an object, in this case a `.txt` document, it is called an *explicit deny*.
- *Explicit permissions* are those applied directly to an object, and they take precedence over permissions that have been inherited. This will be discussed in later labs.
- Permissions are cumulative among users and groups. Permissions will be combined to achieve what is called the *effective permissions* for that object.

8. Right-click `test2` and click Properties.
9. Click the Security tab and click Edit.

10. As done previously, add TestUser2 to the ACL of `test2`.
11. For `test2`, under the Allow column heading, click the check boxes for Read and Read & Execute to remove all listed permissions. No check boxes should be marked.
12. Click OK twice. You should be returned to the folder with your test files.
13. Access the ACL for `test3`. Review the previous steps if you need help navigating to this location.
14. Under the Deny column heading, click the Full Control check box. Notice that all the check boxes, other than Special Permissions, were automatically marked, while under the Allow column heading, the Read and Read & Execute permissions were removed.
15. Click OK and view the Windows Security prompt. Click Yes, and then click OK again. You should be returned to the folder that contains your test files.

Applying File-Level Encryption

In this procedure, you will be using freeware by the name of AxCrypt. AxCrypt is an open-source file-encryption program that can be integrated with Windows Explorer. This feature makes it easy to use and convenient. It also password-protects the encrypted files, giving another layer of security.

1. Right-click on the file `test4`. Locate and hover the mouse cursor over AxCrypt. There are a few options, but for now you will just click the bold Encrypt.
2. To encrypt the file, you must passphrase-protect it as well. Enter the passphrase **marcraft** and verify the passphrase by entering it again.
3. Click on both check boxes to mark Remember This For Decryption and Use As Default For Encryption. The window should look the same as Figure 8.23.

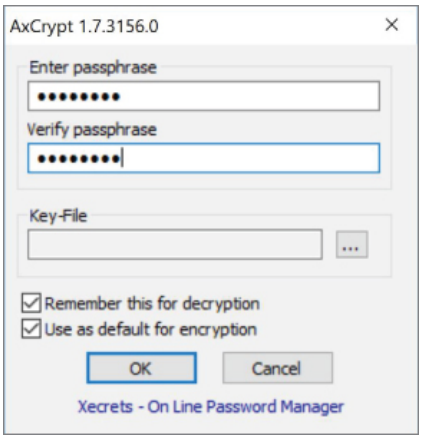


FIGURE 8.23 Using AxCrypt to Encrypt the `test4` File

4. Click OK. You will notice the icon next to `test4` has changed, as well as the name and extension of the file. If you double-click it though, the file will open as normal in Notepad, with the same data inside.

Setting Folder Permissions

Folder permissions provide the same basic permission choices as file permissions. This can be deceiving, as the meaning of each Allow or Deny is slightly different. For instance, the Allow –

Read option on a file permits the opening and viewing of its contents. On the other hand, the Allow – Read option on a folder will only let the specified user list the contents of the folder. The latter can be used when a user needs to be able to access a folder, but not all of the files within the folder.

1. Click the Back button, or Permissions Test in the address bar, to see the folder you created named `Perm_Test_(your initials here)`.
2. Right-click the folder and click Properties.

   Notice the options for permissions. They are the same as file permissions, with the inclusion of one more option: List Folder Contents.
3. Click Edit.
4. Click Add and add TestUser2 to the folder's ACL. This process is the same as you performed before with individual files. Return to the "Creating File Permissions" section if you need to review how this is done.
5. The default permissions for the folder are Allow – Read & Execute, List Folder Contents, and Read. Under the Deny column heading, click the Read & Execute check box. You will notice that all of the Allow permissions have been removed, and the subsequent Deny permissions replace all three.
6. Click the check box to select Allow – Write.
7. Click OK, acknowledge the Windows Security prompt, and click Yes. Click OK to close the Properties window.

Testing Folder Permissions

Now it is time to test all of the options you have put into place. You will need to close all open windows and log onto TestUser2. Choose to Switch User, rather than the Log Off option.

1. Close all open windows and select Switch Users. (Logging off completely would serve the same function; however, it would take much longer.)
2. After selecting the Switch User option, type in the username **TestUser2**. Enter the password **testuser2**.
3. Navigate to the location of the folder you created at the beginning of this lab: Permissions Test. Your personal testing folder will be there.
4. Double-click your folder. Were you able to access the contents?

   Input your findings into Table 8.3.

TABLE 8.3 TestUser2 Access Levels

File/Folder	Permissions for Testuser2	Access?
Perm_Test_folder access		
test1		
test2		
test3		
test4		

5. Right-click the folder and click Properties to try to access the ACL. Click the Security tab. What are the results?

The Deny – Read & Execute, List Folder Contents, and Read permissions override any group permissions that may have previously allowed this. This is an easy way to keep certain users out of important information that they should not access.

6. Leave the Permissions Test window open and switch users. You will need to access TestUser1 again.
7. After entering the username and password, you should be back to the desktop. Once again, navigate to the Permissions Test folder.
8. Right-click the `Perm_Test_(your initials here)` folder and click Properties. In order to grant access to TestUser2, you will need to remove the Deny options.
9. Click the Security tab. Click TestUser2 under Group Or User Names.

When you click on the username, you will notice the check marks for permissions are black. If you click on another user or group, you will notice the check marks for permissions are gray. This means you are unable to change them. Only those check marks that are black can be modified.

In this lab, you are dealing with the DACL (Discretionary Access Control List). This means when a user creates a file, they are considered the owner and have the right to grant or deny permissions as they so choose. However, users with administrative privileges have the right to change the ownership and permissions of a file or folder.

10. Click Edit. The Permissions window loads. Click TestUser2 in the top panel. Change the permissions by clicking the Allow – Read & Execute permissions. This will remove all Deny permissions previously in place and fill in the three Allow permissions as they were originally.
11. Click the OK button to save the permissions.
12. Close all windows and switch users. Log into TestUser2 by supplying the username and password.
13. The desktop will load with the window of the Permissions Test folder still open. Attempt to read the contents by double-clicking the `Perm_Test_(your initials here)` folder. Were you able to access it this time?

Testing File Permissions

1. Within this folder, you should see the four text documents that you created as TestUser1. Double-click `test1` to attempt opening it. Were you allowed?

If you recall from earlier, `test1` was given a Deny – Write permission.

2. Adjust the text in the file by deleting it all and typing **This is no longer a test.** Click File and then click Save. You are asked to confirm the name; click Save. You are asked to Confirm the Save As to replace the file; click Yes.
3. A prompt appears. Was this the expected outcome? List your findings in Table 8.3. Click OK to accept the Access Is Denied prompt.

4. Click the X in the upper-right corner of the file window to close the window. You are asked if you want to save changes, but you already know that you do not have the proper permissions to accomplish this. Click Don't Save. You are now back to the contents of the folder.
5. Double-click `test2` to attempt to open it. Were you allowed?
6. Adjust the text in the file by deleting it all and typing **This is no longer a test.** Click File, and then click Save. Were you prompted for any reason? Record your results in Table 8.3.

You previously removed all permissions for TestUser2 on `test2`. No permissions were granted or denied; however, you are still able to read, modify, and write to this file. Why is that?

TestUser2 is also part of the group Users, which is granted Read & Execute, Read, and Write permissions by default. As mentioned earlier, permissions are cumulative, and the result is the Effective Permissions. Only in the case of a Deny, will an Allow be overridden.

7. Close the `test2` file by clicking the X in the upper-right corner.
8. Double-click `test3` to attempt to open it. Were you allowed? Note the results in Table 8.3.

Deny – Full Control was issued for this particular file. Therefore, TestUser2 is not allowed to access it in any way.

Testing File Encryption

You no doubt have noticed that `test4` has a green shield next to it. The filename and extension are still in their changed format. All indications are that this file is encrypted. You will now try to access the information.

1. Double-click `test4` to attempt to open. Were you allowed?

As a different user, you must supply a password to decrypt the file for access. Assuming the password is not known to another user, this is a good preventative measure.

2. Click Cancel.
3. You will now attempt to view the encrypted text. Right-click `test4`. Hover the cursor over Open With.
4. Click Choose Default Program. The window suggests you open the file with AxCrypt; however, you are unable to access it in this way. Under Other Programs, find and select Notepad.
5. Before clicking OK, look to be sure Always Use The Selected Program To Open This Kind Of File is unchecked. Now click OK.
6. The test document opens. Can you read it? It should look something like Figure 8.24.

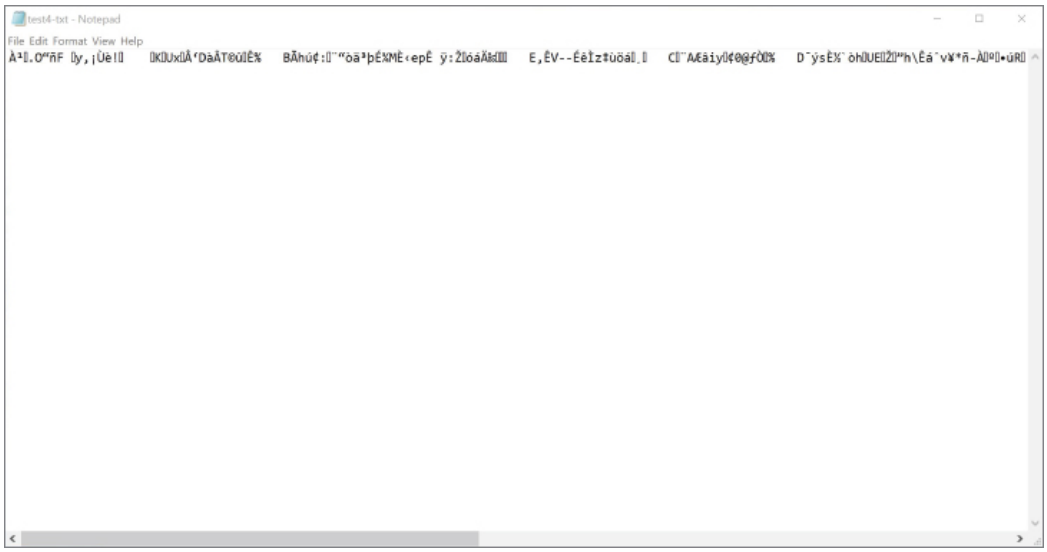


FIGURE 8.24 Encrypted Data in `.txt` Document

7. Adjust the text by deleting and adding random characters to it. Click File, and then click Save. Were you able to save? Record your results in Table 8.3.
8. If you haven't received an error yet, try to access `test4` by double-clicking the file. An error has occurred.

Although encrypting safeguards the information from TestUser2, the permissions were unchanged. This allowed TestUser2 to open the file, change its contents, and finally save it. The result is a corrupted file, which can no longer be read. So even though encryption can hide the contents, permissions still need to be set in order to truly protect the data.

9. Close all the windows and log off as user TestUser2.
10. Log onto TestUser1.
11. Navigate to the Permissions Test folder and access your `Perm_Test_(your initials here)` folder. Attempt to open the `test4` AxCrypt file. Were you able to open it?

Unfortunately, this information is lost.

12. Close all the windows and shut down the computer.

Tables

TABLE 8.2 Permissions Available in `test1` ACL

Full Control	**Modify**	**Read & Execute**
Read	**Write**	**Special Permissions**

TABLE 8.3 TestUser2 Access Levels

File/Folder	Permissions for TestUser2	Access?
`Perm_Test_` folder access	Allow – Write Deny – Read & Execute, List Folder Contents, Read	No access to contents of folder or the ACL
`test1`	Allow – Read & Execute, Read Deny – Write	Can access file but cannot change/save file
`test2`	No explicit permissions given	Can access, change, and save file
`test3`	Deny – Full Control	Denied any access
`test4`	Allow – Read & Execute, Read, Write.	Can access, change, and save file

Lab Questions

1. **Which permission do folders have that files do not?**

   Answer: Folder permissions include List folder contents. File permissions only have Read and Read & Execute.

2. **What are effective permissions?**

   Answer: Effective permissions are the cumulative permissions granted by all sources. Individual and group sources are combined to give an overall permission within an ACL**.**

3. **Does encryption alone make your data safe?**

   Answer: No. As shown in the lab, the information may be protected, but it is not untouchable. Without setting proper permissions, a malicious person might choose to corrupt your information. Even worse, another person might not know exactly what they are doing and accidentally affect the data in an irreversible way.

4. **If a User tries to access a file that has an Allow – Read & Execute permission, and a Deny – Read & Execute permission assigned to them from different sources, will they be able to access the file?**

   Answer: No. In most cases, a Deny permission overrides the Allow permission. The Allow permission granted is voided, and the User will not have access.

5. **If you remove all permissions, Allow and Deny, from a specific user will they be able to access the file or folder?**

   Answer: Depending on the group or groups they are associated with, yes. Users are generally added to the Users groups, and as such they are given the default Allow – Read & Execute, Read, and Write on most files.

6. **As a basic user, can you change the permissions on any file or object?**

   Answer: No. A user without administrative properties cannot change any file or folders permissions. A user is allowed to change only the permissions of files to which they are considered the owner.

CHAPTER 9
Protecting Remote Access

As you learned earlier in Part II, computers do not have to be connected to other computers to be at risk. Although many computers might not be part of a corporate network, almost all modern personal computers at least occasionally get attached to the largest data network in the world: the Internet. As such, these standalone computing and control devices are exposed to corruption and exploitation from remote sources.

- **Analyze and Differentiate Between Anti-Virus/Anti-Malware Products.**
- **Secure the Web Browser of a Standalone Computing Device.**
- **Configure and Test a Local Firewall Installation.**
- **Explain the Importance of Application Security.**
- **Audit Local Operating System Services and Events.**
- **Establish a Local Security Policy on a Standalone Host Device.**
- **Describe the Importance of Conducting Local Updates and Patch Maintenance Activities.**

Protecting Local Computing Devices

There are nine basic steps for protecting local computing devices from Internet-based threats:

1. Use a secure connection.

2. Establish and configure a firewall to control the flow of information between the computing device and the Internet.
3. Install and use anti-malware on the local computer.
4. Remove unnecessary software from the computer.
5. Disable any nonessential services running on the computer.
6. Disable unnecessary OS default features.
7. Secure the web browser.
8. Apply operating system and application software updates and patches.
9. Require strong passwords.

Using a Secure Connection

One of first steps in securing an Internet connection is to implement security options on the local router. If a particular connection does not include a router, you may want to consider installing one, as well-configured routers offer one of the best initial lines of defense. Routers and other network connectivity devices are covered in detail in Part III.

Some basic items to consider when configuring a router's security features include:

- Change the login username and default password. (The defaults are published in the user's setup instructions and, therefore, are known to everyone.)
- For wireless network connections, change the default SSID setting.
- Configure the wireless network with the highest level of encryption available—preferably WPA2-AES for maximum data confidentiality.
- Identify trusted wireless connections by conducting MAC address filtering.

Establishing and Using a Firewall

You should always establish and configure a firewall to control the flow of information between the computing device and the Internet. For standalone or local computers, this can be addressed through the local software firewall available with the operating system and/or through the protective router. Local firewall configurations are discussed later in this chapter.

Installing and Using Anti-Malware Software

Anti-malware software can be installed using an inclusive malware-prevention product or by combining different types of specific prevention programs, such as antivirus and antispyware products from different vendors. Different malware types and prevention methods are discussed in detail at the end of this chapter.

Removing Unnecessary Software

Keeping unused software products on a computer provides additional avenues of possible attack and exploitation. If you don't know what a suspected software program does, research it and get rid of it if it is not important to the operation of that system.

Disabling Nonessential Services

Some viruses are designed to exploit nonessential services in order to migrate from device to device. In particular, disengage any file-sharing or device-sharing services that are running, unless they are somehow required for proper operation of the system (this is almost never the case in nonconsumer usage).

Photo-sharing and music-sharing services should always be disabled, while file and printer should be disabled unless required to pass information from one device to another to perform work tasks. (This would pertain to a networked computer, which is discussed in detail in Part IV.)

Disabling Unnecessary OS Default Features

As mentioned earlier, Autorun is a highly exploitable feature of the Microsoft line of operating systems. When this feature is enabled, the OS will detect the presence of the removable media and execute its contents. If the SD card or CD/DVD contains a virus, it will automatically be executed and infect the host computer.

Securing the Web Browser

The web-browsing class of application software has attracted an increasing number of attacks. Initial browser configurations may not offer much in the way of security. As such, it is usually necessary to configure a new browser's security options to safeguard the system from attack through this portal. Steps for securing different web browsers are discussed later in this chapter.

Applying Updates and Patches

People and groups that produce malware are always busy designing the next exploit. For this reason, operating systems and applications must constantly be updated to counteract these efforts. This requires a planned methodology for obtaining and applying the latest upgrades and security patches for each software product on the system.

Requiring Strong Passwords

The main user authentication tool used with personal computing devices is the *username and password login*. In general, there are three types of user-related logons with which to contend:

- Logons to the local machine
- Logons to a specific software application
- Network logons

For a password to be effective, it must possess a certain amount of *complexity*. Its length, width, and depth must be designed to thwart the efforts of the previously mentioned password-cracking techniques. Refer back to Chapter 8 for an in-depth discussion of passwords.

Implementing Local Protection Tools

Five common tools are used at the local level to protect computing devices from exploitation through the Internet world:

- Local firewalls
- Host-based intrusion-detection systems
- Browser security options
- Antivirus/anti-malware tools
- Software updates and patches

Each topic is discussed in greater detail later in this book. The materials presented in this chapter are specific to local host security. However, each topic expands in scope as the local hosts are attached to larger networks and Internet systems.

Software-Based Local Firewalls

Computers connected directly to the Internet are vulnerable to attacks from outsiders. One way to protect standalone computers from outside attacks is to install a local firewall. A *firewall* is a device or a program that is placed between a local device and an outside network such as the Internet.

Local software-based firewalls can be installed on an individual computer to protect it from malicious activities introduced through the Internet connection. In some cases, the operating system provides a built-in firewall option that can be used to protect the local computer.

A WORD ABOUT FIREWALLS

Local software firewalls are designed to provide protection from outside attacks by preventing unwanted connections from Internet devices. Software-based firewall services are designed to protect individual computers that are directly connected to the Internet through dial-up, LAN, or high-speed Internet connections.

The firewall inspects all traffic going to and coming from the outside connection and can be configured to control traffic flow between the Internet and the local device based on desirable properties, as illustrated in Figure 9.1. Firewalls are configured so they will only pass data to and from designated IP addresses and TCP/UDP ports.

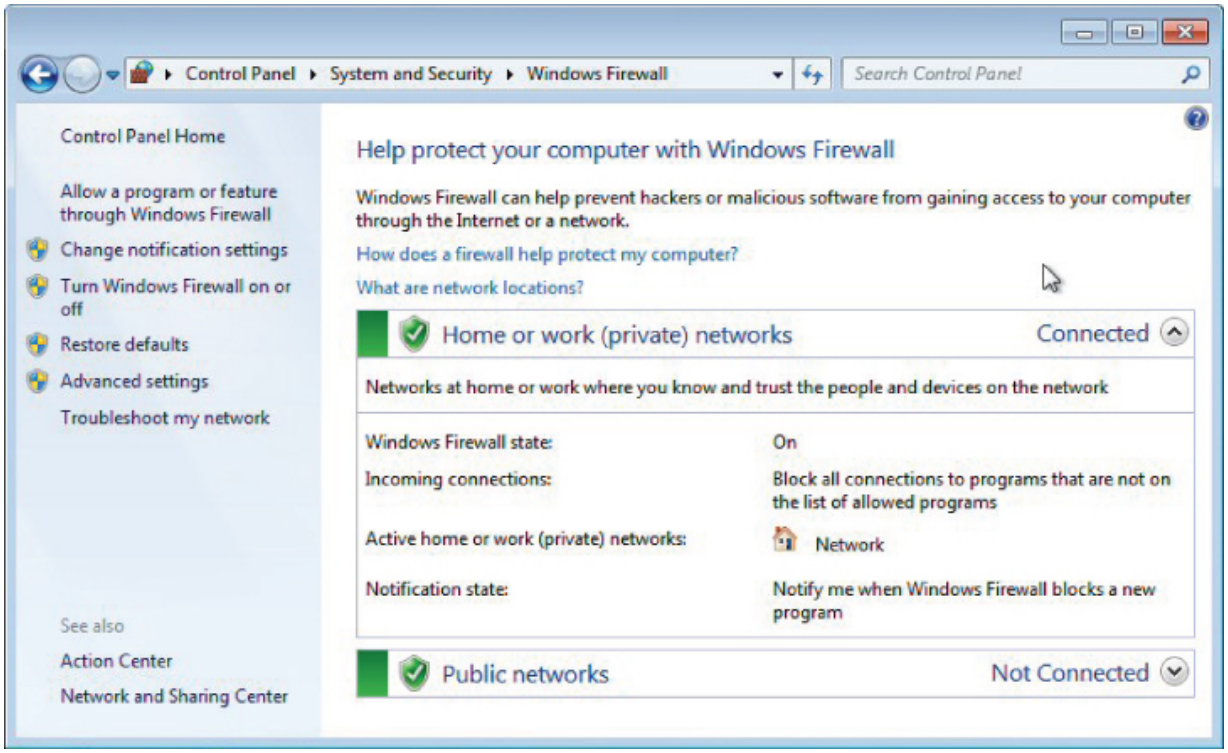


FIGURE 9.1 Firewall Operation

Normally, firewall filters are configured around services recognized by the TCP and UDP networking protocols. These protocols use port numbers to identify specific processes such as HTTP or FTP and are used to refer incoming packets to a software application that will process them. Many of the port numbers are standardized and are referred to as *well-known ports*. Similarly, their associated applications are called *well-known services*.

Table 9.1 lists several well-known port numbers and their associated services. The Internet Assigned Numbers Authority (IANA) has assigned standard port numbers ranging from 0 to 1023 to specific services. Port numbers from 1024 through 49151 are called *registered ports* and are used in vendor applications. Ports 49152 through 65535 are *dynamic,* or ephemeral, ports and are used by computer applications to communicate with other applications.

TABLE 9.1 Typical I/O Ports

Service	Well-Known Port Number
FTP	20, 21
Telnet	23
SMTP Mail	25
HTTP (WWW)	80
POP3 (Mail)	110
News	144
HTTPS	443
PPTP	1723
IRC	6667

When the firewall examines the incoming packet, it can read the source and destination IP addresses of the packet and any TCP/UDP port numbers, as shown in Figure 9.2. It will use the IP address and port information in the packet headers to determine if an incoming packet should be routed into the internal network.

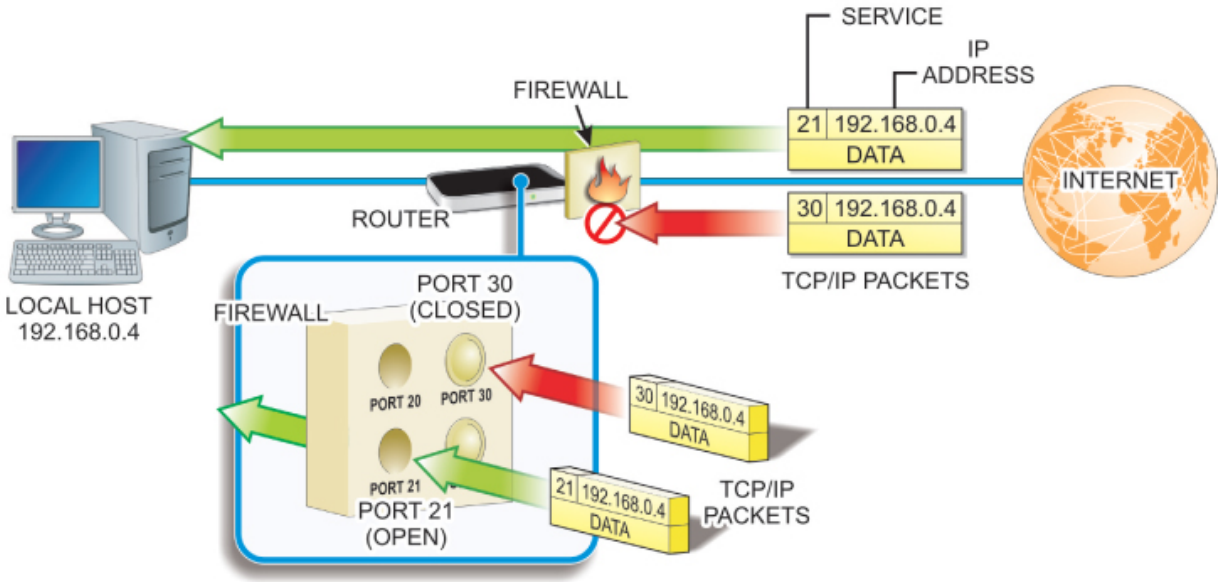


FIGURE 9.2 Firewall Functionality

If you have configured the firewall with the IP address of an internal computer that provides FTP services and opened ports 20 and 21, the firewall will recognize the IP address and port numbers in the incoming header as valid and route the packet to that computer. However, all other incoming requests will still be blocked.

Using Local Intrusion-Detection Tools

As with physical security efforts, preventing unauthorized access is the first line of security at the local computing and control-device level. However, it is just as important at this level to be able to detect the occurrence of an intrusion and notify the proper authorities of its nature.

Computer-based Intrusion Detection Systems (IDS) can be implemented in two ways: as network-based IDS (NIDS) or as host-based IDS (HIDS). In both cases, the system is designed primarily to monitor the system (local computer or network environment), log key events and policy violations, and report them as directed.

Intrusion Prevention Systems (IPS), also referred to as Intrusion Detection and Prevention Systems (IDPS), provide an additional level of protection aimed at preventing the detected threat from succeeding.

As their definitions imply, HIDS and NIDS operate in different areas of the computer/network environment. For now, we will hold off on the discussion of NIDS. Instead, we will focus on HIDS tools that run on individual hosts or devices.

All IDS devices are based on one of two strategies:

- Signature analysis – Incoming and outgoing traffic is compared to a database of stored specific code patterns that have been identified as malicious threats.

- Anomaly analysis – Incoming and outgoing traffic is compared to an established baseline of normal traffic for the system.

The baseline is "learned" (generated) by applying mathematical algorithms to data the system obtains from the traffic flow.

Signature-based IDS/IDPS products generally work by looking for specific patterns in content, known as *signatures*. If a "known bad" pattern is detected, the appropriate actions can be taken to protect the host. However, because of the dynamic nature of programming languages, scripting in web pages can be used to evade such protective systems.

The signature-based IDS database is typically generated and distributed by its manufacturer in response to observed malicious signatures. Therefore, the malicious code is already in existence before a signature can be identified and added to the database to be acted on. The time delay between the release of the malicious code and the issuing of its signature presents its own security issue.

Anomaly-based IDS/IDPS systems apply statistical analysis techniques to the data stream to determine whether it is "normal" or "anomalous" at any given time. There are two common methods of implementing statistical anomaly detection:

- Profile-based anomaly-detection systems
- Threshold-based anomaly-detection systems

Profile-Based Anomaly-Detection Systems

These systems use mathematical algorithms to monitor normal data traffic and develop a "profile" of rules that describe what normal traffic for that system looks like. The profile developed reflects evaluations of users' past behaviors and is configured to signal when deviations from these behaviors reach a certain level (or *threshold*).

- Rule-based anomaly detection – This detection method analyzes audit records to generate rules based on past usage patterns to generate the "rules" set. The system then monitors the traffic looking for patterns that don't match the rules.
- Penetration detection – These systems generate rules based on known penetration occurrences, system weaknesses, or behavior patterns. For this reason, they are normally specific to a given host system. They also typically include rules generated by security experts that are current with security activities.

Threshold-Based Anomaly-Detection Systems

These IDS systems are designed to track the number of occurrences of specific events over time and generate an intrusion warning if the number of events exceeds a predetermined number.

Most commonly available IDS systems are designed for use on local host systems. However, there is an increasing effort in producing network-based IDS systems to provide a more effective intrusion-detection-and-prevention arsenal. Network-Based Distributed Intrusion Systems are described in Part IV.

IDS NOTIFICATIONS

In all IDS types, the administrator is notified when a potential attack is detected.

Configuring Browser Security Options

Web browsers are designed to be highly flexible to offer users as many usage options as possible. They are also designed to appeal to users who by and large are nontechnical. Coupled together with the abundance of people connected to the Internet who use their access

to the web for less-than-honorable purposes and you have a huge security window into your local system.

For example, Figure 9.3 shows a sample of the Internet options available with the Windows Internet Explorer (IE) web browser. As you can see, some of these options are personal preferences, such as colors, fonts, and toolbars. However, there are a variety of security-related activities that involve the browser and searching the Internet.

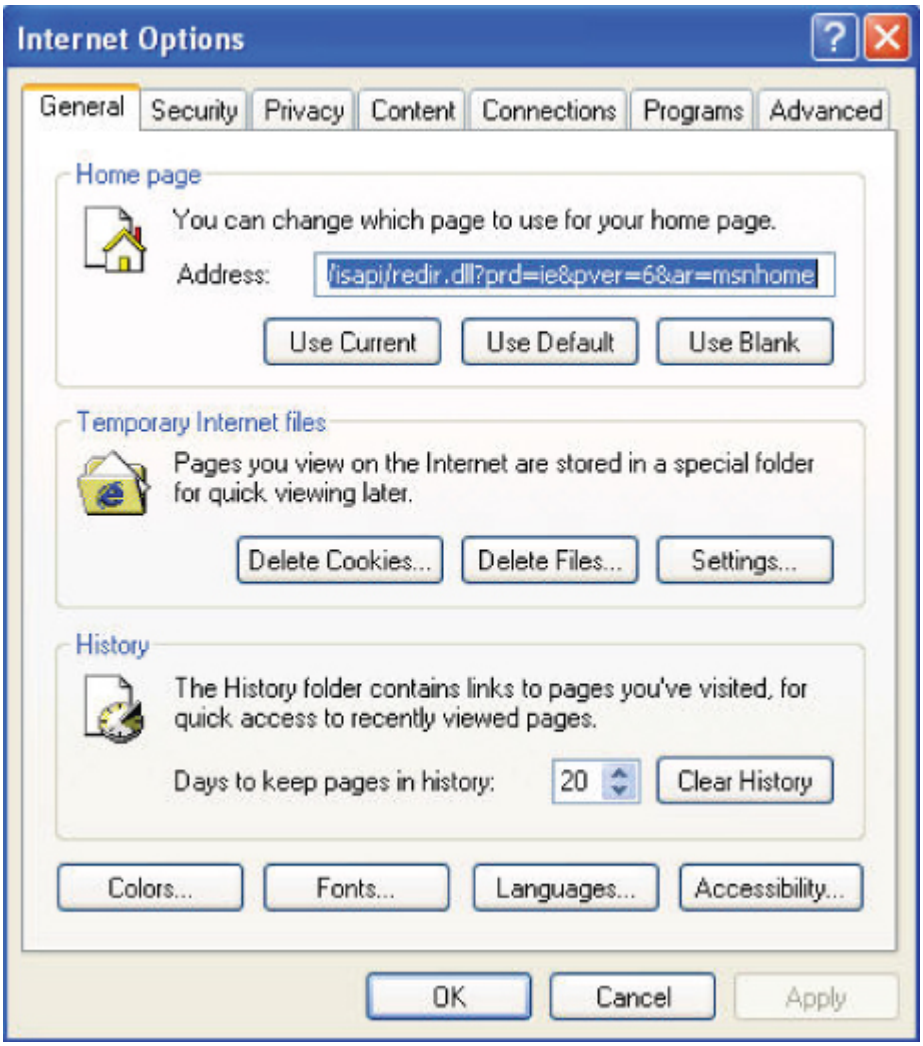


FIGURE 9.3 Internet Options

As the figure illustrates, web browsers routinely offer a variety of user-selectable security options that can be established to

compensate for the added vulnerability Internet browsing and searching brings to the system. These options include:

- Configuring security levels
- Configuring scripting
- Configuring proxies
- Controlling cookies

Although each browser is designed differently, they all tend to provide similar web security options. The user may have to search for specific tools to configure their browser for secure operation, but the same basic configuration techniques apply to all browsers.

Configuring Security Levels

Because the browser is the portal to the wider outside world, its security settings are very important. In addition, other Internet tools on the machine may rely on components of the browser to perform their functions. These applications may bring with them enhancements that create additional vulnerabilities. These features should be evaluated and turned off if they do not contribute to the operation of the system.

As with other applications, browsers come with a preconfigured set of security levels. In Microsoft IE, these functions are located on the Security tab depicted in Figure 9.4.

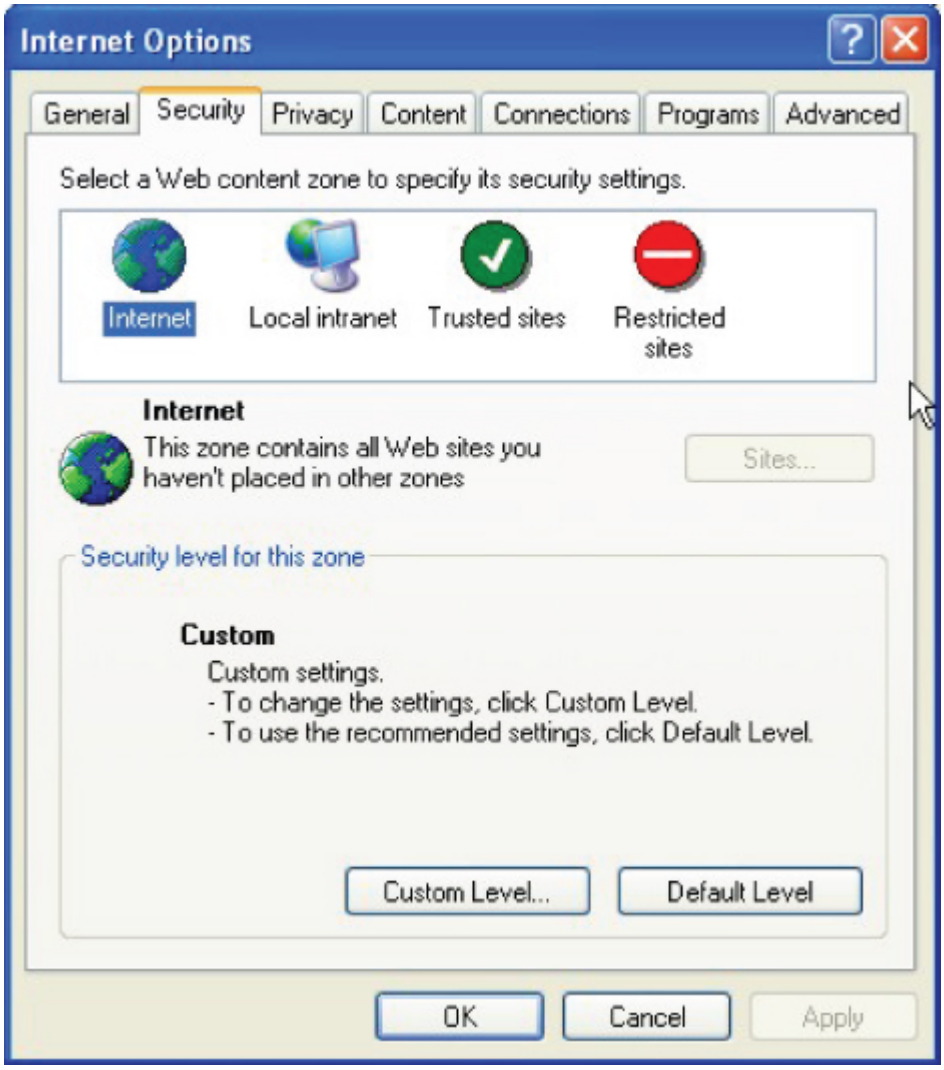


FIGURE 9.4 IE Security Tab

In this browser example, Internet sites may be categorized under different Internet security *zones* that enable sites listed in each zone to be governed by security restrictions that apply to that group (Internet, Local Intranet, Trusted Sites, and Restricted Sites).

This allows different websites to be accessed with different security restrictions. Trusted Sites could be established to work with less security overhead, while Restricted Sites can be assigned heightened security settings. The Internet zone option is the default zone for all sites not assigned to one of the other zone options.

The best option for configuring security levels is to set them as high as possible without restricting the browser to the point where sites do not load or function correctly.

Configuring Script Support

Scripts are executable applications that provide interactive content on websites. They are also capable of retrieving information in response to user selections. However, the user may not have to do anything to run a script program; they are simply embedded in the website being accessed.

Scripts encountered on websites should be controlled because they are one of the main sources of virus infections. Attackers reconfigure scripts to contain viruses that clients may download unwittingly. They also facilitate automatic pop-up windows that appear without warning on the client's browser. These windows normally contain unrequested advertisements that tend to annoy users.

The capability to load and run scripts in a browser can be controlled through the browser's Security feature. The list of individual web page components that you can control includes different script types, such as ActiveX and JavaScript.

ActiveX is a Microsoft utility that enables web applications to build extended, interactive features, and functionality around the presence of the ActiveX framework in the browser. When the ActiveX-enabled browser encounters a web page calling for an ActiveX control function, it automatically downloads without involving the user. Of course, this creates a potential security vulnerability that can be used by crackers to embed malicious code in hacked websites.

A similar scripting language called JavaScript is often used in web browsers to make websites more interactive. It is particularly interesting for developing interactive content in games and other audio/video-rich web pages. However, it is also widely used to

transmit information about remote activities, such as browsing and reading habits for use in advertisement tracking and analysis. It does this without reloading the page where the information was gathered and without notifying the reader. This again creates a potential portal for malicious (or at least unwanted) activities.

A WORD ABOUT VBSCRIPT

VBScript is another scripting language that is unique to Microsoft Windows Internet Explorer. VBScript is similar to JavaScript, but it is not as widely used in websites because of limited compatibility with other browsers.

Another area of concern in the interaction between websites and browsers is the use of plug-ins to add new features to existing software applications, such as search engines and antivirus functions. These script controls are similar to ActiveX controls but cannot be executed outside of a web browser. Adobe Flash and QuickTime Player are the most recognized examples of web browser plug-ins.

Most browsers support various plug-ins by default and rely on them for some portion of their operation. Along with the automatic nature of these components comes an increasing vulnerability both in terms of design deficiencies and as potential hacking targets. Historically, ActiveX controls, Adobe's PDF Reader and Flash products, as well as Apple's QuickTime product have represented the highest number of documented vulnerabilities among script products.

As with the other security objects, the browser can typically be configured to Enable, Disable, or present a user prompt whenever it encounters these scripted items on a page. As a rule of thumb, all

add-ons (including Java, JavaScript, Flash, and ActiveX) should be disabled on websites unless you know that they can be trusted.

Controlling Cookies

Cookies are small files that web servers send to web browsers when their pages are accessed. The legitimate use of these files is to enable the server to automatically recognize the client browser any time it connects to the server. The basic HTTP page transfer process is described in Figure 9.5.

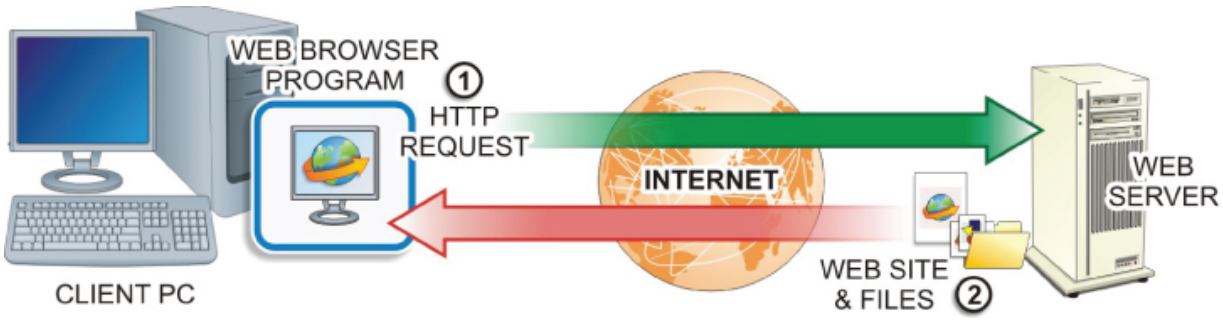


FIGURE 9.5 HTTP Transfer Operations

Web page transfers are initiated on the client side through the local web browser. The browser sends an HTTP request to the designated web server, which in turn sends back the requested page along with an HTTP response message. One piece of information in the message may be a request for the browser to set (accept and store) cookies, so that a more efficient, automated page transfer process can be carried out.

The cookie may also contain several pieces of configuration information known as *cookie attributes*. One key security-related attribute is the setting for when the cookie expires. There are basically two varieties of cookies to be concerned with: session cookies and persistent cookies. *Session cookies* are cleared when the browser is closed, and *persistent cookies* will remain on the computer until the specified expiration date is reached. Persistent cookies pose a higher risk than session cookies because they remain on the client computer for a longer period of time.

Cookies were originally developed to keep users logged into online shopping environments while they moved from page to page and placed items in online shopping baskets. However, the use of cookies has expanded to include a lot more than just shopping baskets. They may be designed to gather and track any information that a website is designed to place in it—for example, they may track information about the sites the user visited or credentials used to access the site. Cookies designed to perform these types of functions are called *tracking cookies*.

This is the type of information that makes cookies attractive to crackers. If a website uses cookies for authentication, then an attacker may be able to acquire unauthorized access to that site by obtaining the cookie. This is referred to as *cookie theft*.

The attacker only needs to employ a packet sniffer utility to monitor the network traffic and capture the cookie in order to gain access to their credentials (username, passwords, network address, and so on). With this information in hand, the attacker has the ability to pretend to be the original user when they access other sites.

The attacker can also use a technique called *cross-site scripting*, or XSS, to cause the returning cookie to be redirected to a third-party server operated by the attacker. The attacker can then use the stolen cookie to spoof the original site posing as the original user. The redirection is typically accomplished by simply hiding the script on the site and using social engineering techniques to trick the user into clicking on the code. When they do, their cookie is transmitted to the third-party location specified by the attacker.

In addition, the attacker may simply alter the contents of a stolen cookie to perform an attack on the original web server. For example, if the cookie was the product of an ecommerce sales site, it might include pricing information about products in a shopping cart. The attacker could alter that information and send it back to the original server, causing it to charge the customer a lower price for the item. This type of attack, as depicted in Figure 9.6, is a form of a man-in-the-middle (MITM) attack referred to as *cookie poisoning*.

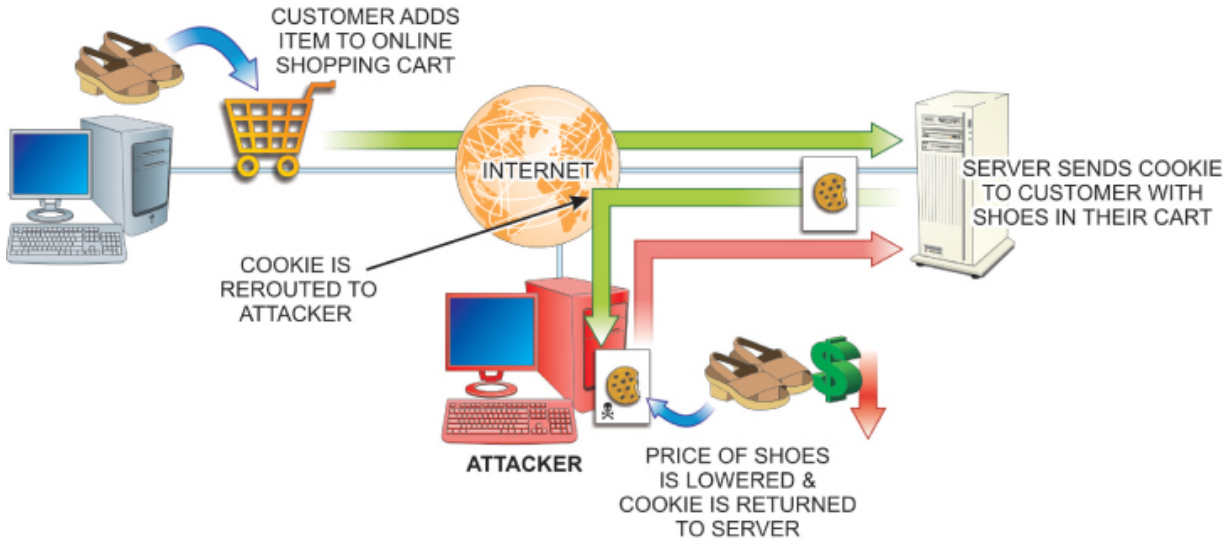


FIGURE 9.6 Cookie Poisoning

Virtually all browsers support cookies by default. Some offer the user the option to completely enable or completely disable cookies, while others provide a more robust cookie manager that enables the user to view and select individual cookies to remove from the system.

For security purposes, the best recommendation for handling cookies is to disable the option to Always Set Cookies. In addition, use transmission encryption to prevent third parties from being able to read the cookies if they are intercepted along the way. This is particularly important when using Wi-Fi communications. If the wireless link is not encrypted, attackers can easily intercept and then read the data including the cookies sent.

The use of secure socket layer (SSL) links provides data encryption security for the transmitted data (including the cookies) and prevents unauthorized access to the data as it moves across the communication link. SSL links are always identified as `HTTPS://` sites instead of simply `HTTP://`.

Defending Against Malicious Software

Increased connectivity through networks and the Internet have made personal computers vulnerable to an array of different types of malware and grayware. *Malware* is the term used to describe programs designed to be malicious in nature. The term *grayware* describes programs that have behavior that is undisclosed or that is undesirable.

New malware threats are constantly emerging, and successful cybersecurity personnel must stay abreast of them. The following list identifies some of the more advanced malware threats being produced. Some of these have been around for many years but have continued to be very dangerous and continue to be modified and difficult to detect:

- *Viruses* are destructive programs designed to replicate and spread on their own. Viruses are designed to replicate themselves within a local computer environment. This most often happens when users download programs from the Internet or open email attachments. Many “free” products obtained from the Internet have something attached to them—a virus, spyware, or some other form of malware.
- *Worms* (sometimes referred to as network viruses) are circulated through a network connection. Unlike a virus, worms do not need a host program in order to infect your computer. Worms search for vulnerabilities to exploit in an application. Once the worm has taken advantage of the vulnerability, it seeks to replicate to another computer on the network. While initially intended to slow down network environments, worms often leave payloads on systems to cause further malicious activity.
- *Trojans* appear to be a legitimate program that might be found on any system. They are made to appear to be actual applications so that users will be tricked into using them. Although they function and work properly, they have malicious code that initiates when the application is launched.

- *Rootkits* are a type of software designed to gain administrative control of a computer system while remaining undetected. Normally, the purpose is to enable malicious operations to occur on a target computer without the knowledge of its users or system administrators. Rootkits can occur in hardware or software by going after the BIOS, boot loader, OS kernel, and sometimes applications or libraries.

  Rootkits are designed to operate at the root level of the operating system and appear as a benign entity at that level. After the rootkit has been installed in a system, it will take measures to hide itself from detection. They modify the behavior of the operating system's core components by altering drivers or kernel modules. These programs have the ability to steal PINs, account passwords, credit cards, and other sensitive information. They can infect nearly any operating system type.

- *Ransomware* is software designed to keep the user from their data and hold it hostage for payment. Spam email is the most common delivery vehicle for spreading the malware. It is then activated by the user clicking an attachment or a link in the email message. It then disables essential system services or even locks the computer so that the user cannot gain access to it.

  Hackers can encrypt personal files on the computer keeping the user from gaining access to their data. The hacker will normally prompt the user to enter a code that can be attained only after wiring payment through cryptic means such as Bitcoin cryptocurrency. They will also typically try to get the user to purchase a legal decryption or removal tool. The author (hacker) is the only person(s) who knows the required private decryption key.

- *Spyware* programs are generally introduced to the system through Internet downloads that appear to be useful programs. Unlike viruses and Trojans, spyware typically does not self-replicate. Once spyware is installed on a system, it monitors the

system's operation and collects information such as usernames, passwords, credit card numbers, and other PII.

- *Adware* programs introduce unwanted, unsolicited advertising displays to web browsers. They can also be designed to gather user selection information from the browser, constructing a more personalized advertising scheme. Adware is typically introduced to the system through downloads such as free software (freeware).
- *Logic bombs* are a type of malware typically used to delete data. A logic bomb is computer code that, much like other malware, is attached to a legitimate program. The code sits idle until a specific logical event is concluded. This includes a number of days passing, a number of programs being opened, or executing a program in a specific manner. Logic bombs are hard to detect because they are often included in large programs with thousands of lines of code.
- *Zombies* are infected computers that can be placed under the remote control of a malicious user. Zombies can be used to create Denial of Service (DoS) attacks that flood targeted networks to slow down and sometimes stop servers completely. Computers are often infected and become zombies by way of viruses, worms, and Trojans.
- *Botnets* are a large collection of zombies, or bots, controlled by a bot herder. This type of network can consist of literally millions of unsuspecting computers. Botnets can be used to send out spam (usually through email lists) originating from unsuspecting users' computers. It is estimated that 50 to 80 percent of spam worldwide is created by zombie computers.

It is common to install a number of different defensive products to protect PCs and their data from unauthorized access and malicious interference. Most products these days include protections against multiple fronts. The products most widely used for these purposes include:

- Antivirus programs
- Antispyware programs
- Spam blockers
- Pop-up blockers

Using Antivirus Programs

Every computer should have some means of protecting itself against computer viruses. The most common means of virus protection involve installing a virus-scanning (antivirus) program that checks disks and files before using them in the computer. Several companies offer third-party virus-protection software that can be configured to operate in various ways.

If the computer is a standalone unit, it might be nonproductive to have the antivirus software run each time the system is booted up. It would be much more practical to have the program check any removable media attached to the system, only because this is the only possible non-network entryway into the computer.

All computers with connections to the Internet should be protected by an antivirus solution before they are ever attached to the Internet. In these cases, setting the software to run at each bootup is more desirable. In addition, most antivirus software includes utilities to check email and files downloaded to the computer through network or Internet connections.

As indicated earlier, when an antivirus application is installed on the system, it can be configured to provide different levels of virus protection. You will need to configure when and under what circumstances you want the virus software to run.

Using Antispyware

As shown in Figure 9.7, there are basically two types of antispyware products available: those that find and remove spyware after it has been installed and those that block spyware when it is trying to

install itself. Both of these methods stand a better chance of keeping computers free from spyware when they are combined with user information about how to avoid spyware.

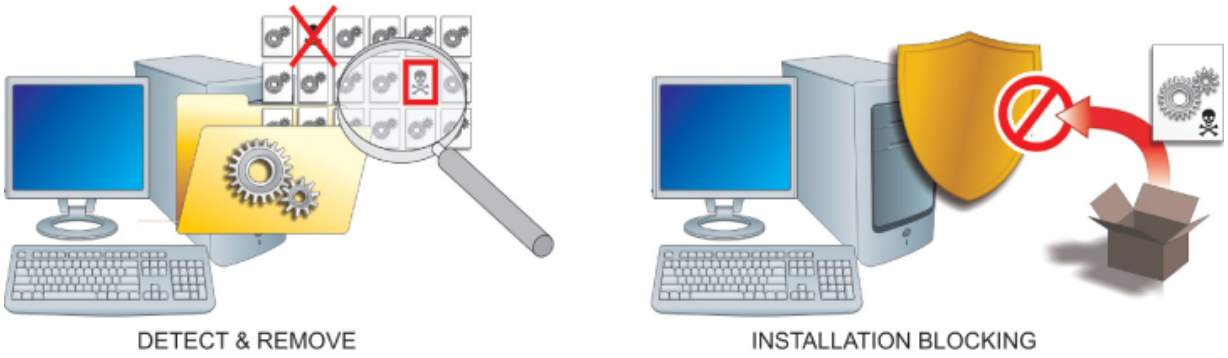


FIGURE 9.7 Antispyware Product Types

The detect-and-remove method is by far the simpler type of antispyware product to write. Therefore, there are several commercially available products that use this method. Like antivirus software packages, this type of antispyware product relies on databases of existing definitions to recognize spyware threats. These databases must be updated frequently to recognize new spyware versions that have been identified.

The real-time-prevention type of antispyware product does not rely on historical data to identify spyware. Instead, it monitors certain configuration parameters and notifies the user when suspicious installation activity occurs. The user then has the option to allow or block the installation effort. Some antispyware products incorporate both methods of dealing with spyware.

In addition to installing antispyware applications, users can fight spyware in a number of other ways:

- Install a web browser other than Internet Explorer (for example, Chrome or Firefox).
- Download the newest browser version that offers better security features.

- Work with an ISP that uses their firewalls and proxies to block sites that are known to distribute spyware.
- Download only software from reputable sites to prevent spyware that comes attached to other programs.

Hardening Operating Systems

As noted earlier, the second level of hardening local computer systems against attacks is to secure their operating systems. This involves updating vulnerable code segments of the OS as they become known. OS hardening occurs through the application of new programming in the form of:

- Service packs
- Patches
- Updates

Service Packs

After an operating system has been in the field for some time, vendors may combine several product improvements and distribute a numbered *service pack* for the specific operating system being upgraded. Critical files should always be backed up in the event that the service pack or OS fails to work after installing the service pack.

Patches

Patches are general improvements to a given operating system that have been released for distribution. Many patches and updates are purely cosmetic and convenient add-on features, while others are critical security upgrades designed to respond to a particular virus, discovered threat, or weakness found in the operating system.

Updates

An *update* is a service pack or patch that improves the reliability, security, or attractiveness of an operating system. The most reliable source of operating system updates is the OS manufacturer. These organizations are always seeking ways to improve their products. Some updates may make the OS more convenient but may not necessarily make it more secure. Therefore, they should be tested before implementing. Consider backing up critical files in the event that the patch or OS fails to work after installation.

Overseeing Application Software Security

Software application packages operate as extensions of the operating system. Depending on the type of operating system being used, an application program may directly control some system resources, such as printers and network interfaces, while the operating system lends fundamental support in the background. In more advanced systems, the operating system supplies common input, output, and disk management functions for all applications in the system.

Some applications include built-in security tools that control access to the application beyond the levels presented by the operating system. However, many applications are written with very little concern for security issues. The focus of such programs is functionality and sharing, leaving security issues to the operating system and security utilities.

Software Exploitation

The term *software exploitation* is used to describe cyber attacks designed to take advantage of vulnerabilities or weaknesses in software products—operating systems and applications. These vulnerabilities may be the result of software that is created with little or no thought for security issues, or they may be the product of software that has been inadequately tested before being released for use.

There are two very conflicting objectives in the computer software industry:

- Make the product as open and easy to use as possible so that otherwise nontechnical users will be able to work with it.
- Make the application bullet proof so that nothing bad can happen to it—ever.

Software programmers are asked to meet both of these objectives in the same product.

In some cases, the programmers may be trying to create a truly open product without concerns about how it might be exploited by malicious people. In other cases, they may not be experienced enough to envision how their product might be exploited. With the worldwide pool of programmers continuously growing, there are many individuals with a significant knowledge base of how to test, manipulate, and modify programming. This includes black hat hackers.

A WORD ABOUT BLACK HAT HACKERS

A *black hat hacker* is an individual who possesses extensive programming skills and uses them to breach or bypass network security structures for malicious or criminal purposes. People in this category of hacker are also known as *crackers* or *dark-side hackers*.

There are also *white hat* and *gray hat hackers* who also seek to exploit Internet security vulnerabilities and weaknesses, but not for malicious reasons (for example, to perform security system analysis checks).

Modern operating system and application programming is very complex. When programmers initially develop a product, they may

make coding mistakes or create portions of a product that do not work well with elements created by other programmers in the development team. Attackers will often use software vulnerabilities to insert and hide malicious code that can be used to disrupt services or operations.

In particular, the attacker may alter the existing code to create a condition in the computer's memory known as a *buffer overflow,* which results in erratic behavior, memory access errors, and/or system crashes. The system is effectively disabled to the point where the user cannot use it. This kind of attack is a type of Denial of Service (DOS) attack.

Applying Software Updates and Patches

From the previous section, you can see that due to the nature of product development and the pressures on software producers to bring new products to the market, new software releases never seem to be complete or perfect. As security issues are revealed with software products, their producers are forced to issue security patches for their product that correct the weakness.

Security patches are updates issued for the specific purpose of correcting an observed weakness to prevent exploitation of the vulnerability. Microsoft issues security patches for its products once a month. Other software developers use dedicated security teams to develop and issue security patches as soon as possible after a vulnerability has been discovered.

For security and stability reasons, you should always patch operating systems on computing devices that are connected to the Internet. However, this is not the case with all PCs. Stable PC systems that are not connected to the Internet should not be patched unless doing so resolves some sort of existing problem.

Hands-On Exercises

Objectives

- Manage the local firewall configuration.
- Explore Windows Firewall with Advanced Security.
- Recognize the need for outbound filtering.
- Create a port filtering rule.
- Create an ICMP filtering rule.

Resources

- PC-compatible desktop/tower computer system
- Windows 10 Professional installed
- User account with Administrative access
- Internet access from a network connection

Discussion

Computers connected directly to the Internet are vulnerable to attacks from outsiders. One way to protect standalone computers from outside attacks is to install a local firewall.

Local software-based firewalls can be installed on an individual computer to protect it from malicious activities introduced through their Internet connection. In some cases, the operating system provides a built-in firewall option that can be used to protect the local computer.

In this lab, you will explore the options associated with Windows Firewall to apply the local (software) firewall. You will also recognize the need for inbound and outbound filtering and testing various security options. In some scenarios, you may want to download a software-based firewall, but Microsoft includes Windows Firewall, as well as Windows Firewall with Advanced Security, with their operating system.

Procedures

Accessing Windows Firewall Basic Settings

To access the basic Windows Firewall settings, follow these steps:

1. Power on the computer, and choose Windows 10 Professional if a given a choice.
2. Log on to your administrative account.
3. Click on the embedded search bar on your taskbar, type **Control Panel**, and then click on Control Panel in the menu presented.
4. If necessary, switch to viewing the Control Panel with the View by: Small Icons, locate and click Windows Firewall. Figure 9.8 shows the basic Windows Firewall settings.

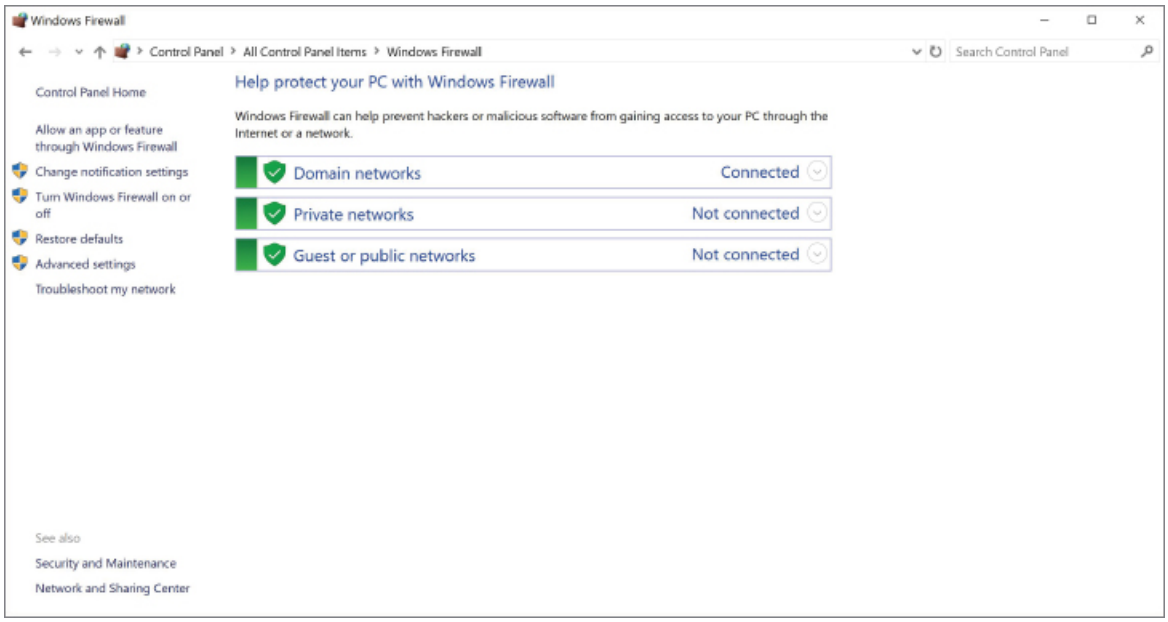


FIGURE 9.8 Basic Windows Firewall Settings

In this window, you can see the current firewall states for each type of network.

5. Expand each network type by clicking the down arrows located in the top-right of each network. Examine the current states and

the rules associated with each. List the three types of networks in Table 9.2.

TABLE 9.2 Types of Networks

Domain networks	Home or work (private) networks	Public networks

6. In the left pane, click Turn Windows Firewall On Or Off, located next to a Windows Defender Shield indicating Administrative access is required.

In the left pane, Turn Windows Firewall On Or Off and Change Notifications lead to the same window. Figure 9.9 depicts the Customize Settings window.

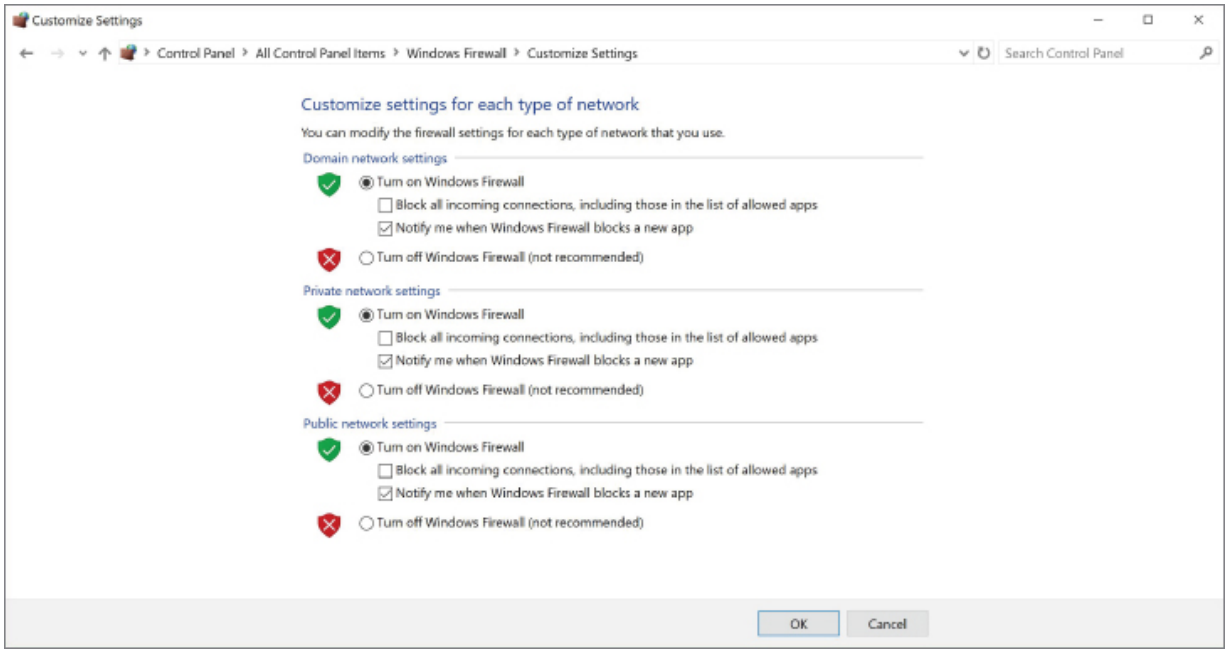


FIGURE 9.9 Customize Settings Window for Windows Firewall

This window shows the basic options associated with each type of network. You turn on or off the firewall. If the firewall is turned on (recommended), you can decide if you want to block all incoming traffic and if you want to be notified if and when a program is blocked.

The firewall inspects all traffic going to and coming from the outside connection and can be configured to control traffic flow between the Internet and the local device based on desirable properties. Firewalls are configured so they will only pass data to and from designated IP addresses and TCP/UDP ports.

There are very few reasons to turn off Windows Firewall (not recommended).

7. If any network type has Turn Off Windows Firewall selected, click Turn On Windows Firewall. Click OK to exit the Windows Firewall Customize Settings.

Examining Windows Firewall with Advanced Security

To examine Windows Firewall with Advanced Security, follow these steps:

1. In the left pane, click Advanced Settings, next to a Windows Defender Shield, to launch the Windows Firewall with Advanced Security console. (See Figure 9.10.)

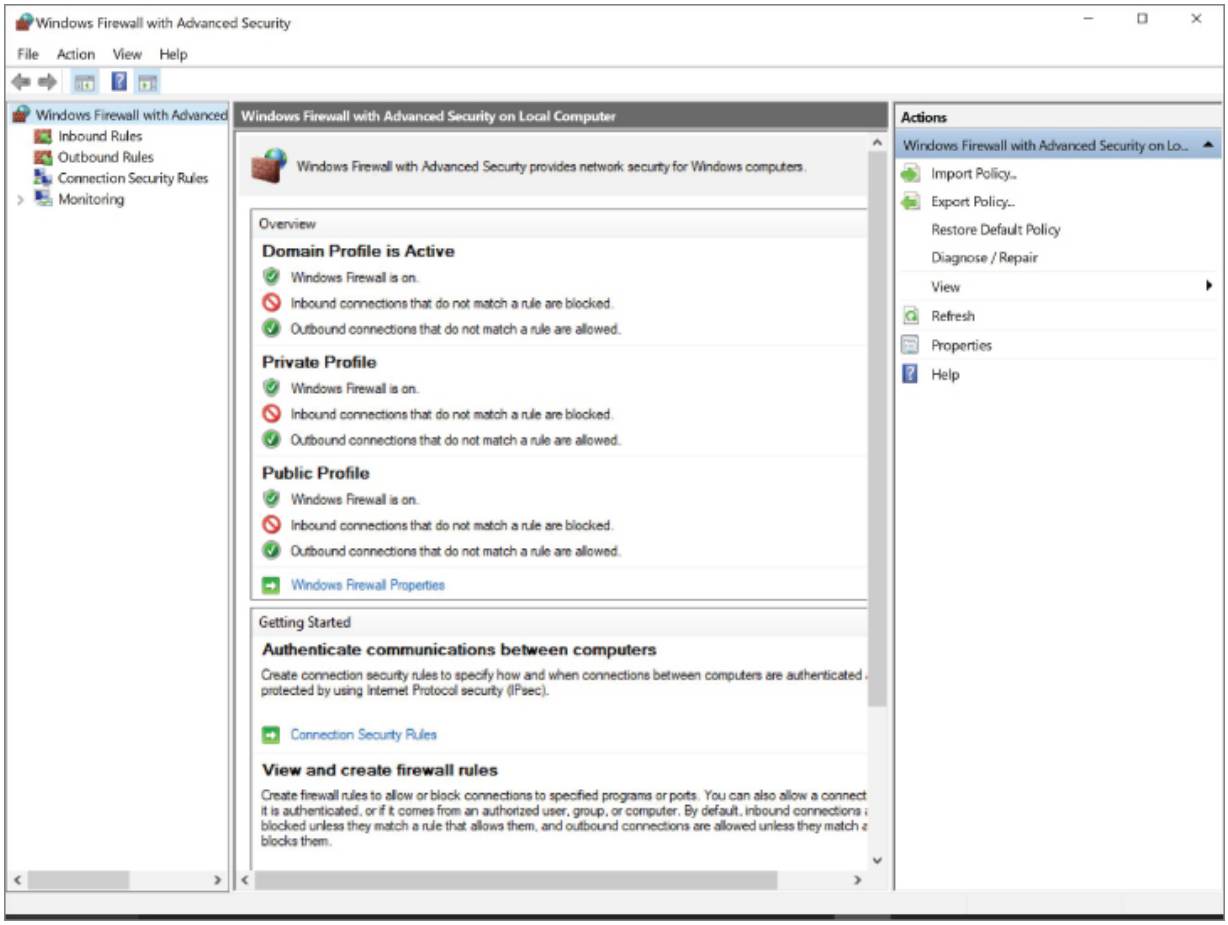


FIGURE 9.10 Windows Firewall with Advanced Security Console

This opening view in the console shows an overview of the current state of the firewall, along with a basic Getting Started tutorial that includes:

- Authenticate communications between computers
- View and create firewall rules
- View current firewall and IPsec policy and activity

2. At the bottom of the Overview section, select Windows Firewall Properties to launch the Windows Firewall with Advanced Security on Local Computer Properties window, as shown in Figure 9.11.

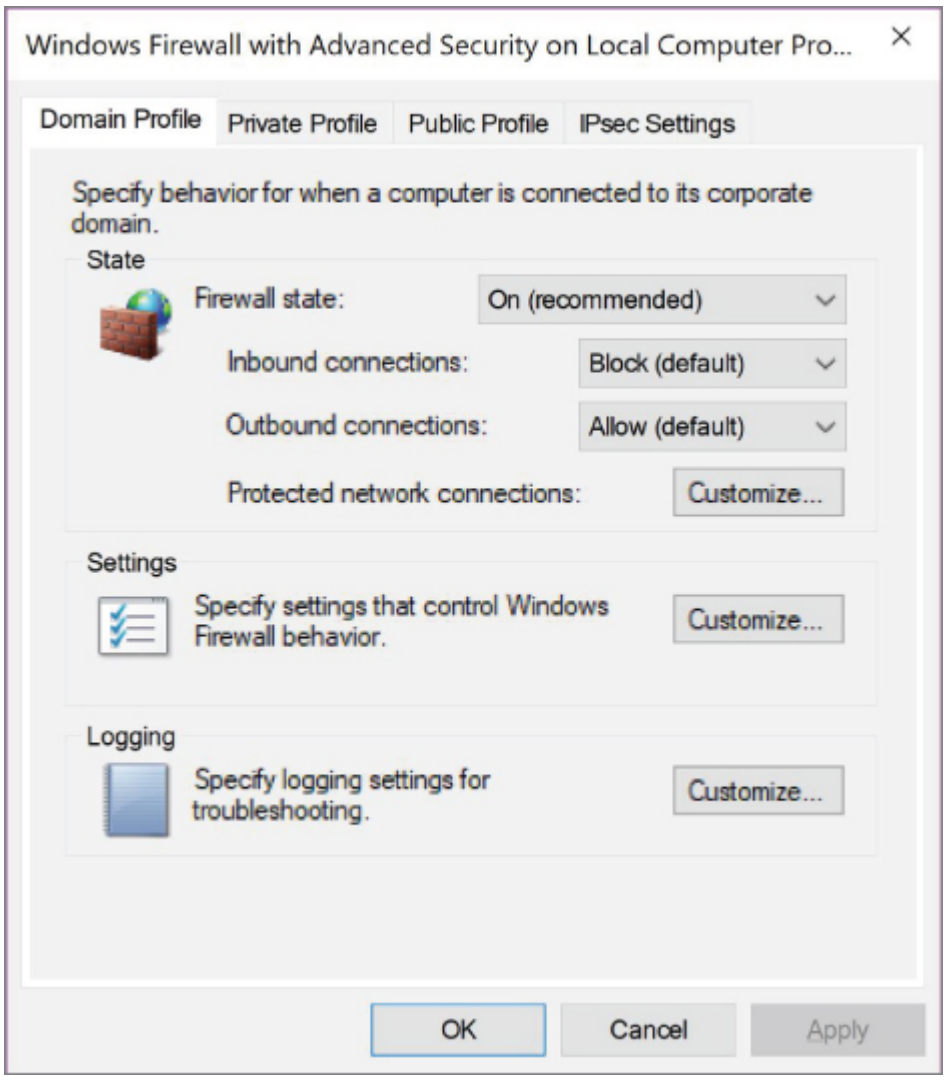


FIGURE 9.11 Windows Firewall with Advanced Security on Local Computer Properties

This window gives you another option to control settings for each of the three types of networks. You can also customize the various settings and set rules for logging.

3. Explore the tabs without changing the configurations and then click Cancel to close out this window.
4. In the left pane, select Outbound Rules. The central and right panes will be similar to Figure 9.12.

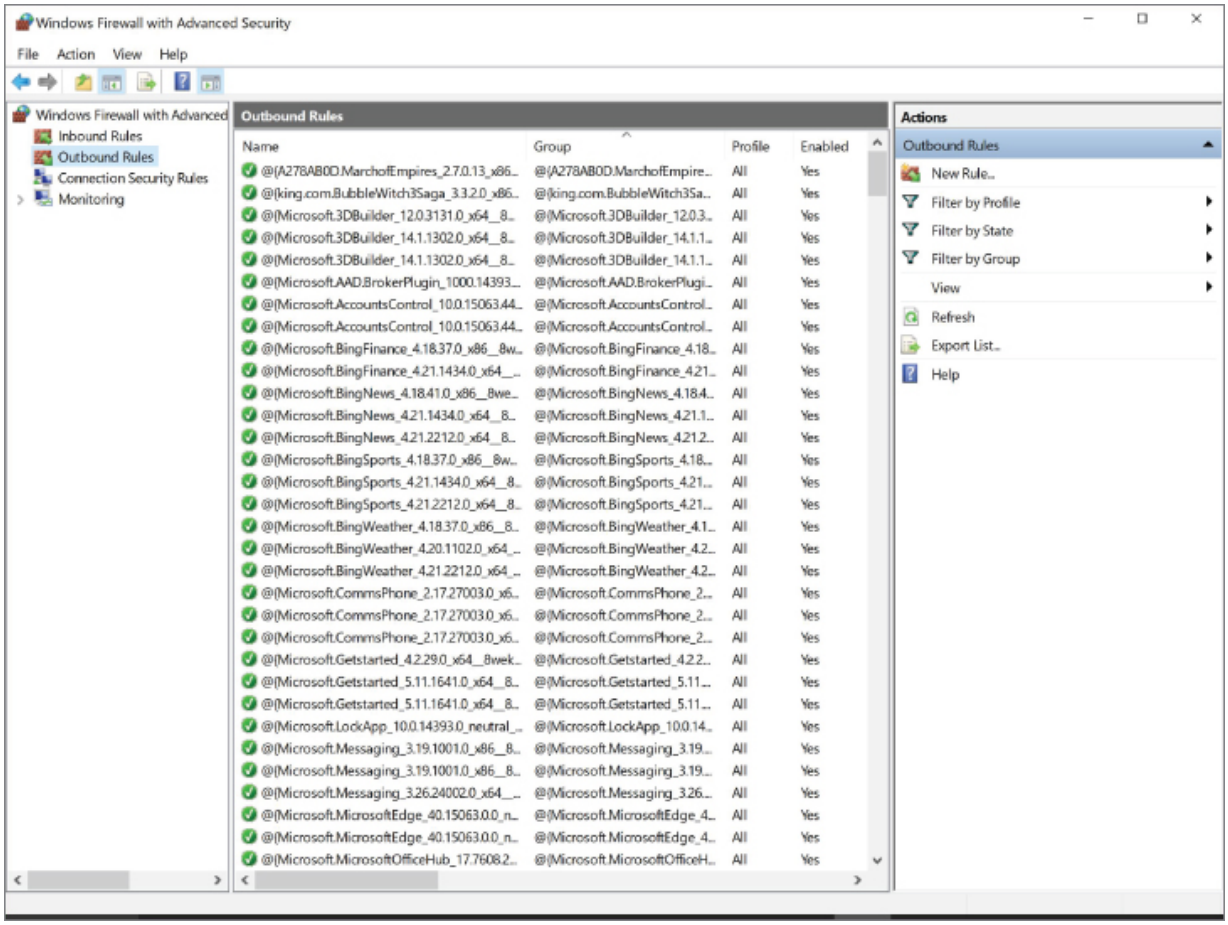


FIGURE 9.12 Outbound Rules in Windows Firewall with Advanced Security

Creating a TCP Outbound Rule

To create a TCP outbound rule, follow these steps:

1. In the right pane, click New Rule. The New Outbound Rule Wizard will appear, as shown in Figure 9.13.

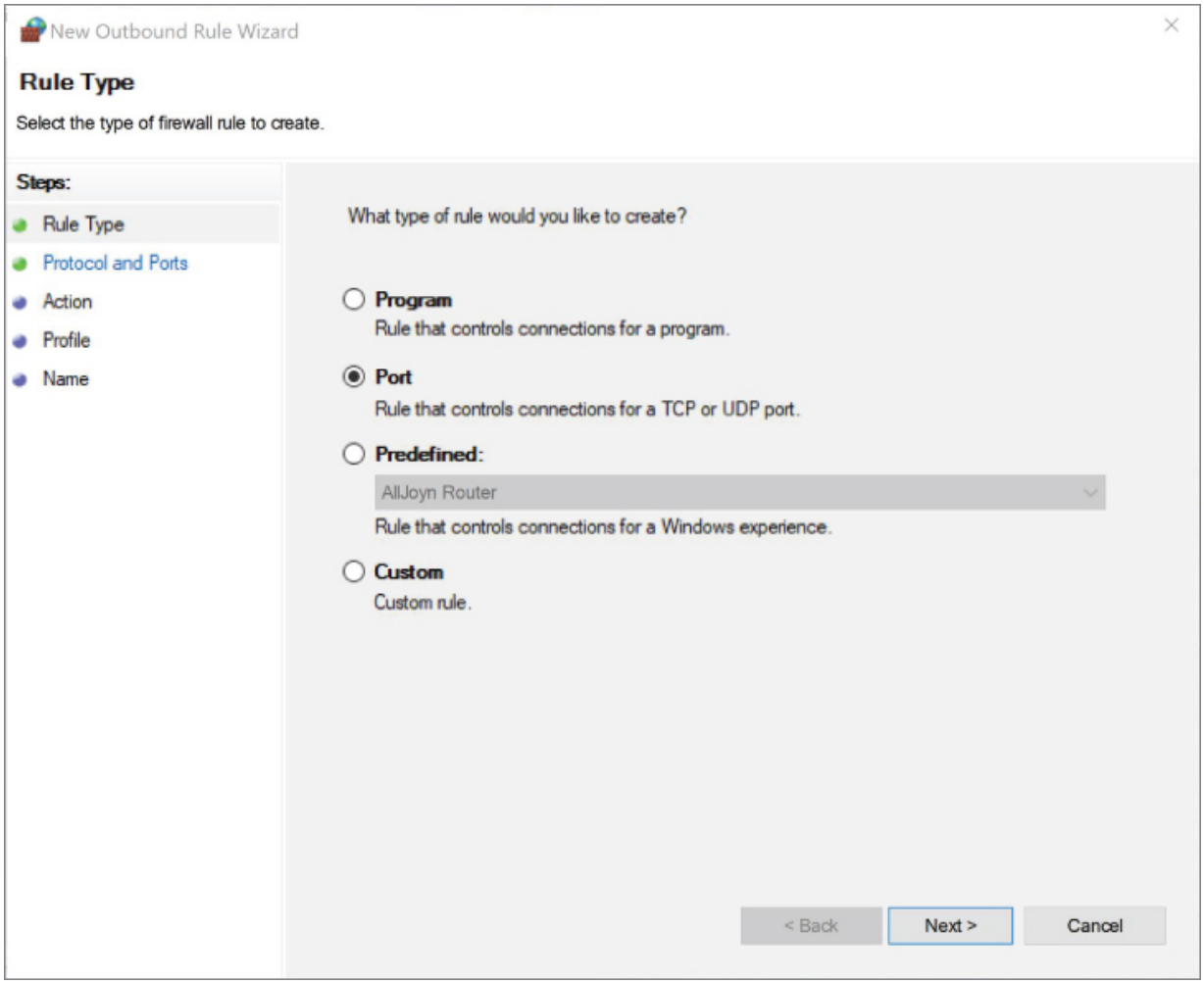


FIGURE 9.13 New Outbound Rule Wizard

On any page within the New Outbound Rule Wizard, you can learn more about the options by selecting the Learn More About (Subject) link located near the bottom of each page.

2. Select the Port radio button, and then click on the Next button to continue the steps in the left pane, as shown in Figure 9.14.

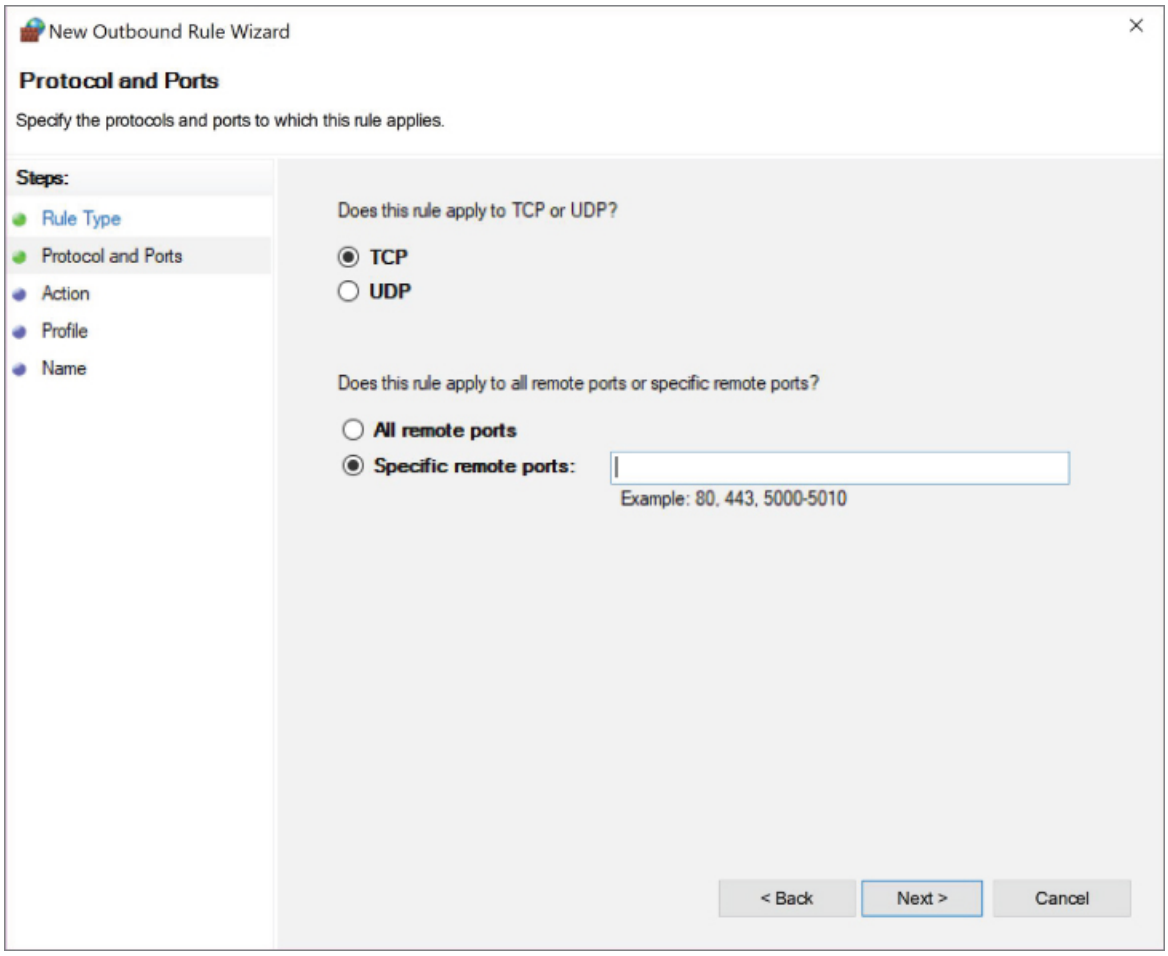


FIGURE 9.14 New Outbound Rule Wizard Steps: Protocol and Ports

3. In the Protocol and Ports window that appears, make sure the TCP radio button is selected along with the Specific Remote Ports radio button. Input **135** into the text field.

TCP port 135 is one of many ports through which malware often attempts to initiate network requests via `NetBIOS/SMB/RPC`. Creating an outbound block rule will prevent your system from connecting to malicious external hosts.

4. Click the Next button to proceed to the Steps: Action page.
5. Examine the options, but leave the Block The Connection radio button selected. Click the Next button to continue onto the Steps: Profile page.

6. Here you will decide the type of network to which your rule should apply. Leave all three check boxes marked to apply the rule to all networks. Click Next to continue to the Steps: Name page.
7. On the Name page, enter **My First TCP Rule** into the Name text box. Type **This is my first TCP outbound rule** into the Description (Optional): field box. Figure 9.15 shows the Steps: Name page with the information entered.

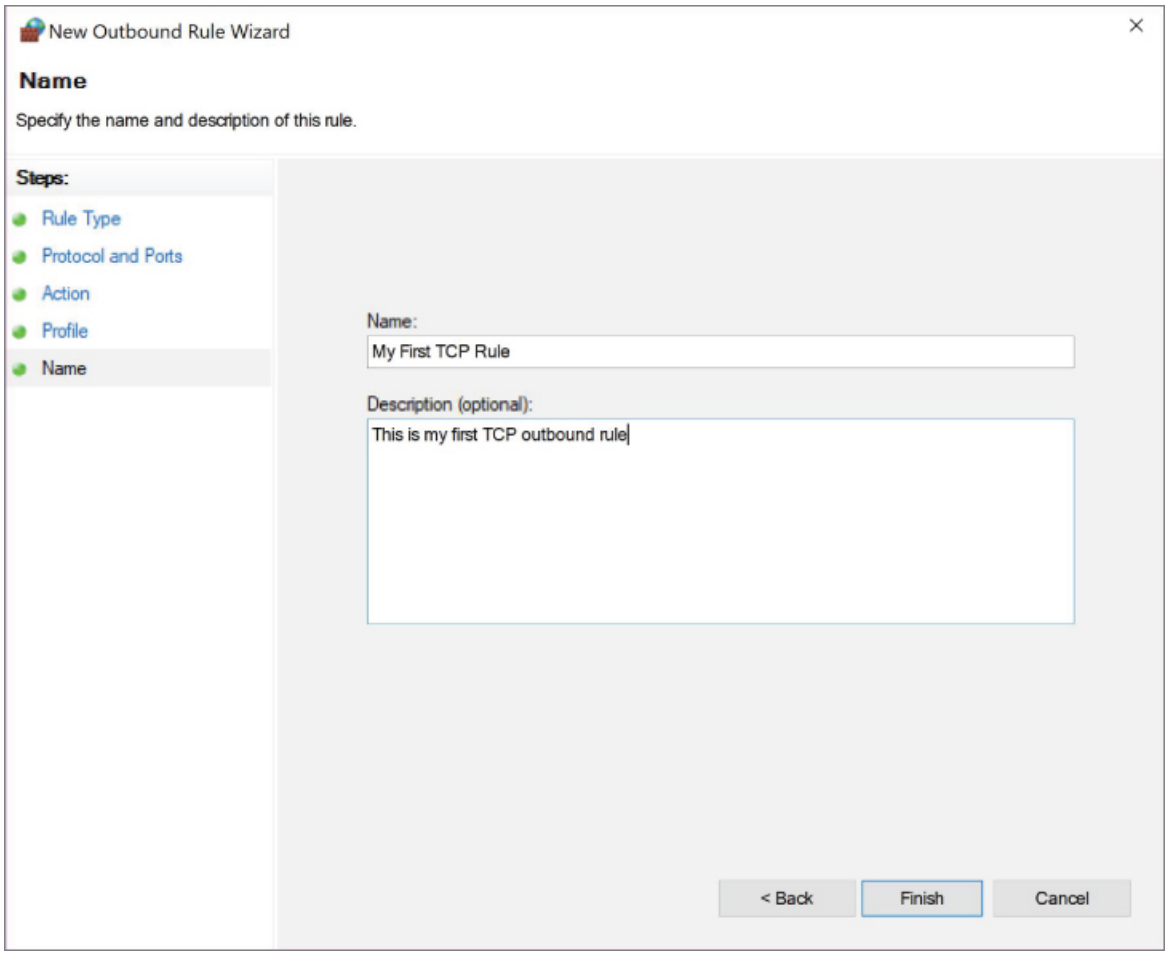


FIGURE 9.15 New Outbound Rule Wizard Steps: Name Page

8. Click Finish. You should see your rule in the Rules list in the center pane, as shown in Figure 9.16.

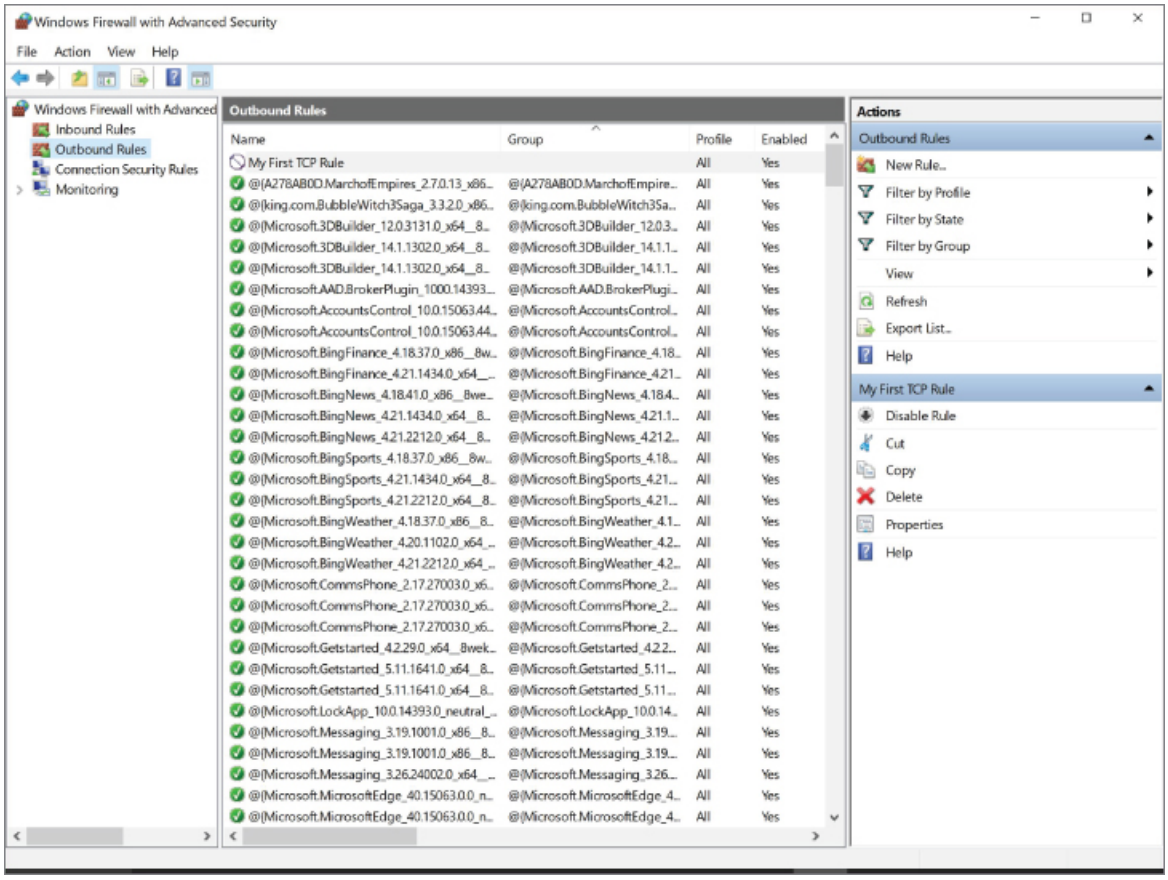


FIGURE 9.16 Windows Firewall with Advanced Security New Outbound Rule

Creating an ICMP Outbound Rule

Outbound communications can be in the form of ICMP types or codes in addition to TCP/UDP ports. The following steps will show you how to block outgoing ICMP communications.

1. Click on New Rule in the right pane. The New Outbound Rule Wizard will appear.
2. Select the Custom radio button. Notice that the Steps located in the left pane have grown in numbers. Click Next to continue.
3. Leave the All Programs radio button selected, as shown in Figure 9.17.

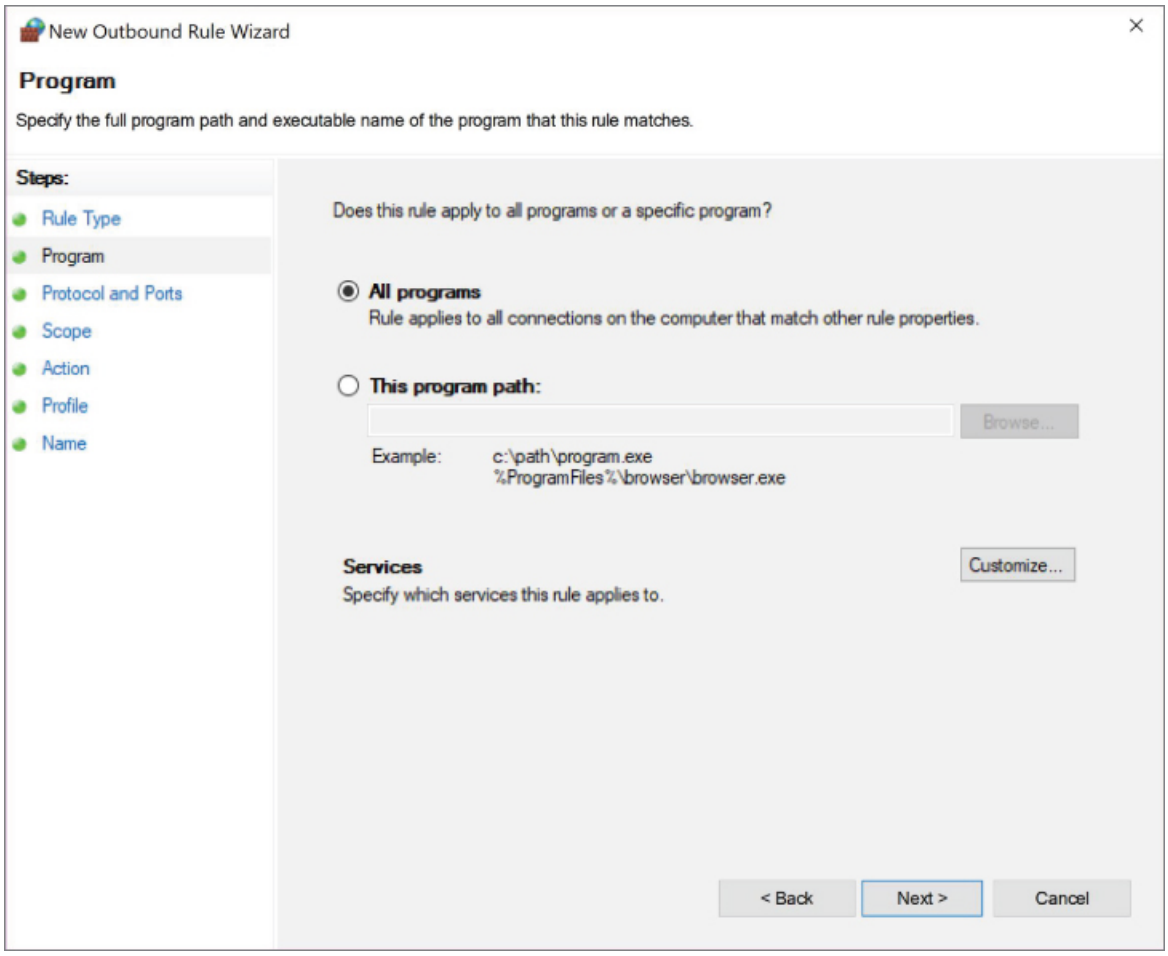


FIGURE 9.17 New Outbound Rule Wizard Steps: Program Page

4. Click Next to continue to the Steps: Protocol and Ports page.
5. Select ICMPv4 from the Protocol Type drop-down menu. Click on the Customize button to access the Customize ICMP Settings, as shown in Figure 9.18.

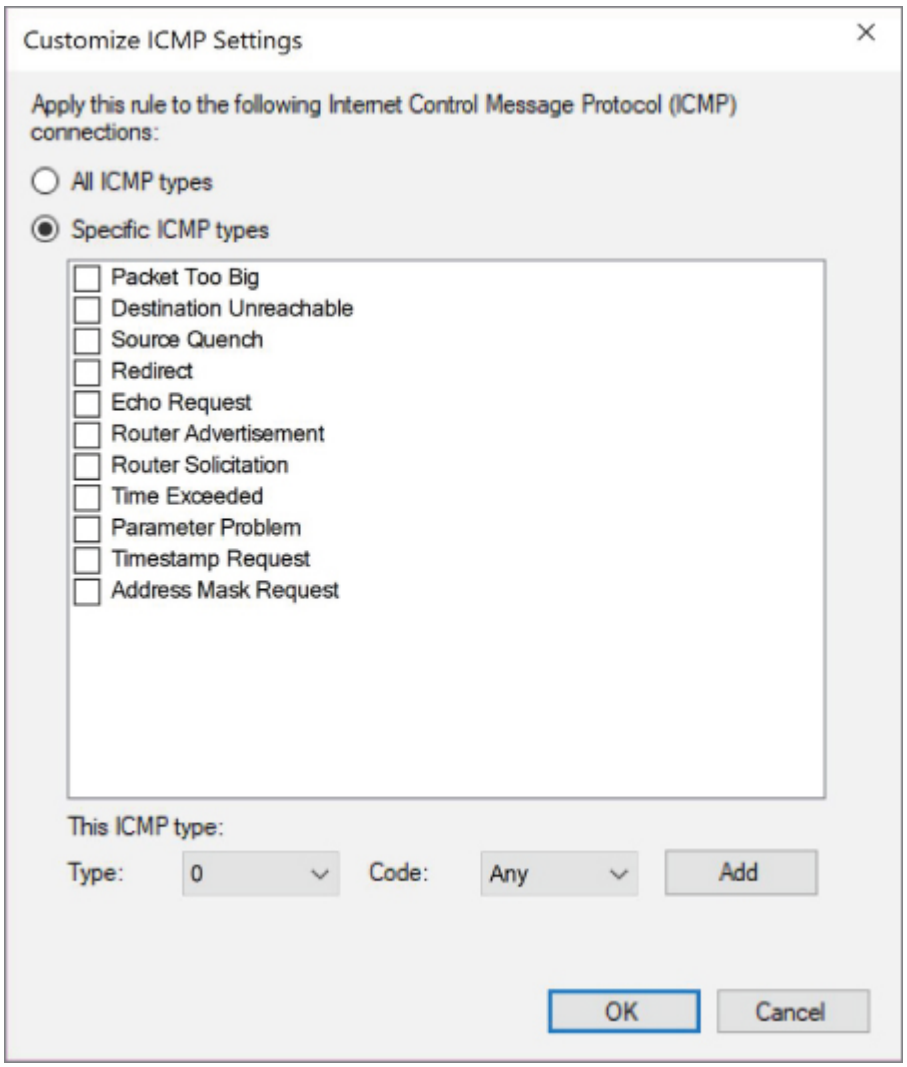


FIGURE 9.18 Customize ICMP Settings

6. In the Customize ICMP Settings window, select the Specific ICMP Types radio button. Click the check box next to Echo Request.

   You can block outbound ICMP echo requests, also known as `pings`, when your machine has been affected by malware and is now part of a botnet. In this instance, the botnet may be sending ICMP requests to create a `ping` flood (DoS attack).

7. Select OK to return to the Steps: Protocol and Ports page.
8. Click Next to continue to the Steps: Scope page, as shown in Figure 9.19.

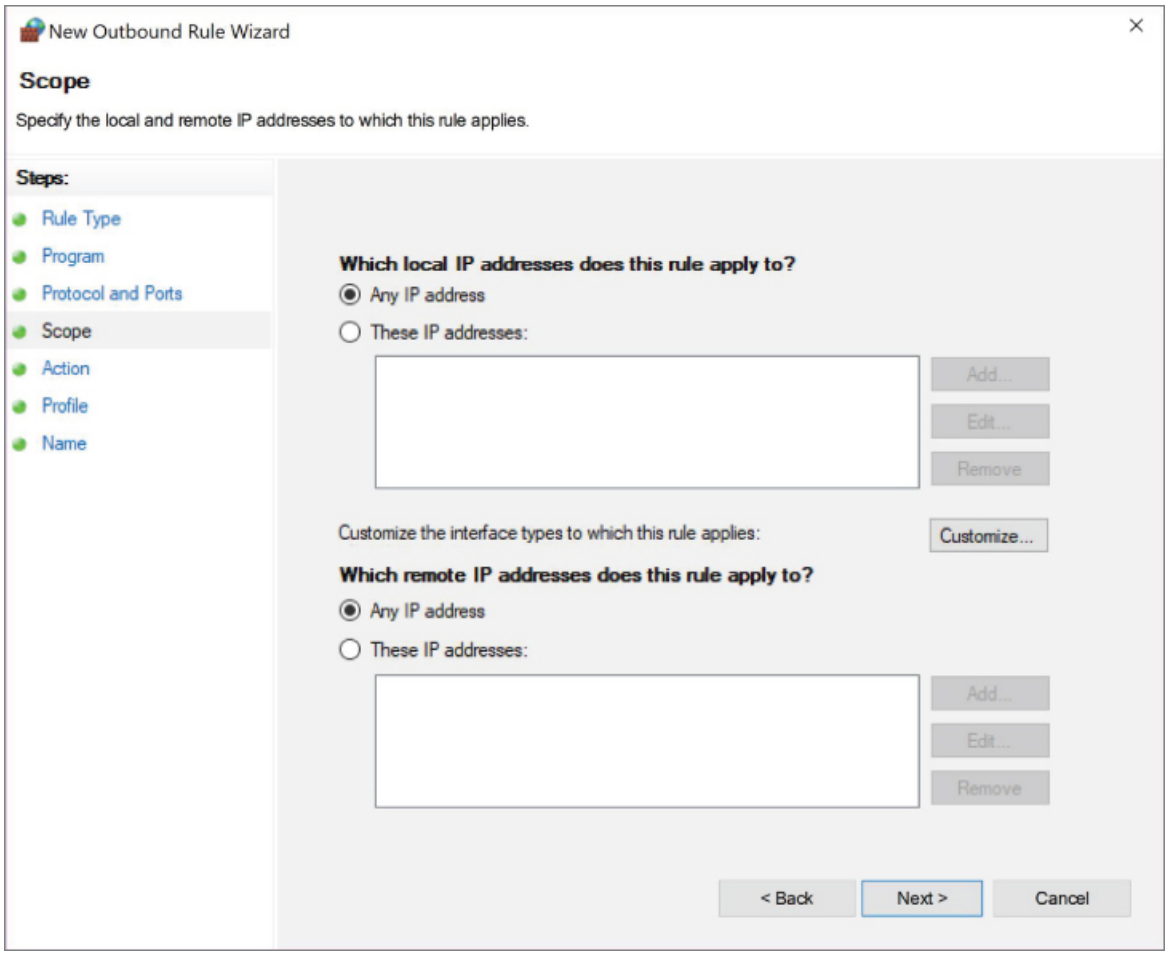


FIGURE 9.19 New Outbound Rule Steps: Scope Page

9. Leave the Any IP Address radio buttons selected and then click Next to continue to the Steps: Action page.
10. Leave the Block The Connection radio button selected, and then click Next to continue to the Steps: Profile page.
11. Leave all the profile check boxes marked, and then click Next to continue to the Steps: Name page.
12. In the Name text box that appears, enter **My First ICMP Rule**. Enter **ICMP Echo Requests** into the Description (Optional) text box. Figure 9.20 shows the completed Steps: Name page.